**Міністерство освіти і науки України**
**Тернопільський національний технічний університет імені Івана Пулюя**
Факультет комп'ютерно-інформаційних систем і програмної інженерії
Кафедра кібербезпеки

# КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр

на тему: «Використання біометричної автентифікації в системах керування доступу на основі технології SSO»».

Виконав студент 4 курсу, групи СБ - 41
Копач Максим Андрійович

125 кібербезпека
( шифр, спеціальність)

| | | |
|---|---|---|
| Керівник | (підпис) | Кульчицький Т.Р. (прізвище та ініціали) |
| Нормоконтроль | (підпис) | Лобур Т.Б. (прізвище та ініціали) |
| Завідувач кафедри | (підпис) | Загородна Н.В. (прізвище та ініціали) |
| Рецензент | (підпис) | (прізвище та ініціали) |

**Тернопіль 2023 р.**

Міністерство освіти і науки України
**Тернопільський національний технічний університет імені Івана Пулюя**

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Загородна Н. В
(підпис) (прізвище та ініціали)

« » 2023 р.

# З А В Д А Н Н Я
## НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня
Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студенту Копача Максима Андрійовича
(прізвище, ім'я, по батькові)

1. Тема роботи «Використання біометричної автентифікації в системах керування доступу на основі технології SSO».

Керівник роботи Кульчицький Тарас Русланович Ph.D в галузі права
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «___»_____2023 року №_____

2. Термін подання студентом завершеної роботи _____

3. Вихідні дані до роботи Технічна документація, інтернет-джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. Розділ 1. Інформаційні системи авторизація та автентифікація у таких автоматизованих системах . 1.1.Поняття інформаційних систем. 1.2. Поняття автентифікації ,авторизації та її види 1.3. Поняття SSO та застосування системи в сучасних інформаційних системах Розділ 2 SSO технології, як система усунення 2.1. Аналіз безпеки SSO та її ризик . 2.2. Біометричні характеристики які використовуються в системі SSO. Розділ 3 Візуалізація об'єктів біометричних даних та методи використання правоохоронними органами таких даних . 3.1. Візуалізація об'єктів біометричних даних. 3.2. Алгоритм фреймворку.Розділ 4 Безпека життєдіяльності, основи охорони праці . Висновки, Список Використаних Джерел, Додатки .

5. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Безпека життєдіяльності і основи охорони праці | Пилипець М.І. д.т.н. професор кафедри МТ | 22.05.23 | 26.05.23 |

6. Дата видачі завдання _____ _____

**КАЛЕНДАРНИЙ ПЛАН**

| № з/п | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Ознайомлення з завданням до кваліфікаційної роботи | | **Виконано** |
| 2. | Підбір джерел про аудит інформаційної безпеки | | **Виконано** |
| 3. | Опрацювання джерел про аудит інформаційної безпеки | | **Виконано** |
| 4. | Підбір джерел про існуючі засоби проведення аудиту | | **Виконано** |
| 5. | Опрацювання джерел про існуючі засоби проведення аудиту | | **Виконано** |
| 6. | Аналіз роботи SSO систем | | **Виконано** |
| 7. | Оформлення першого розділу | | **Виконано** |
| 8. | Оформлення другого розділу | | **Виконано** |
| 9. | Оформлення третього розділу | | **Виконано** |
| 10. | Оформлення розділу «Безпека життєдіяльності і основи охорони праці» | | **Виконано** |
| 11. | Оформлення кваліфікаційної роботи | | **Виконано** |
| 12. | Нормконтроль | | **Виконано** |
| 13. | Перевірка на плагіат | | **Виконано** |
| 14. | Захист кваліфікаційної роботи | | **Виконано** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Студент _____ ___ Копач .М.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ ___ Кульчицький Т.Р.
(підпис) (прізвище та ініціали)

# АНОТАЦІЯ

«Використання біометричної автентифікації в системах керування доступом на основі технології SSO» // Кваліфікаційна робота освітнього рівня «Бакалавр» // Копач Максим Андрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки,група СБс-41 // Тернопіль 2023 // С.57 , рис. - 7, додат. – , бібліогр. – 20.

Ключові слова: Технологія SSO, АВТЕНТИФІКАЦІЯ , ІДЕНТИФІКАЦІЯ БІОМЕТРИЧНІ ДАНІ, ПІДСИСТЕМА.

У роботі досліджено питання використання біометричної автентифікації в системи на основі SSO, які стали невід'ємною частиною сучасних управлінських процесів у багатьох організаціях та державних установах.

Однак, використання цих систем також створює нові виклики та загрози інформаційній безпеці. У цій роботі проаналізовано позитивні та негативні сторони, які можуть вплинути на системи інформаційну безпеку використання біометричних даних. Також будуть розглянуті сучасні методи та технології, що використовуються для захисту систем на основі технології Single Sing-On від цих загроз.

Основна увага присвячена використанню біометрії в таких підсистемах, які використовуються в державних установах для обробки та обміну конфіденційною інформацією. Будуть проаналізовані їхні функціональні можливості та засоби безпеки.

Результати цієї роботи допоможуть підвищити розуміння процесів інформаційної безпеки в при використані систем на основі технологій єдиного входу і розробити рекомендації щодо поліпшення систем електронної взаємодії, автентифікації та авторизації . Дана кваліфікаційна робота може бути корисною для організацій, які використовують або планують використовувати такі системи на основі технологій єдиного входу.

# ANNOTATION

The use of biometric authentication in access management systems based on Single Sign-On(SSO) technology // Thesis of educational level “Bachelor” // Kopach Andrii // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, group SBs-42 // Ternopil 2022 // P.57, fig. - 7, add. - 0, bibliogr. - 20.

Keywords: SSO Technology, AUTHENTICATION, IDENTIFICATION, BIOMETRIC DATA, SYDSUSTEM.

The study examines the use of biometric authentication in SSO-based systems, which have become an integral part of modern management processes in numerous organizations and government institutions.

However, the use of these systems also presents new challenges and threats to information security. This research analyzes the positive and negative aspects that can impact the information security of utilizing biometric data. Additionally, it explores contemporary methods and technologies employed to safeguard SSO-based systems from these risks.

The primary focus is on the utilization of biometrics in subsystems employed by governmental institutions for the processing and exchange of confidential information. Their functional capabilities and security measures are thoroughly analyzed.

The findings of this research will contribute to a better understanding of information security processes in the implementation of SSO-based technologies and aid in the development of recommendations for enhancing electronic interaction, authentication, and authorization systems. This thesis can be of value to organizations currently employing or planning to adopt such SSO-based systems.

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

SSO - Single Sing-On

СЗ системи захисту інформації

ПЗ –Програмне забезпечення

СУБД – Система управління базами даних

ДСТУ –Державні стандарти України

ЕЦП –Електроно-цифровий підпис

PKL – Інфраструктура відкрити ключів

# ВСТУП

В Україні, як і в світі в цілому стрімко розповсюджуєтеся використання різних за своєю сутністю систем та підсистем це є фактом розвитку громадськості та суспільства в цілому , яке передбачає за собою розвиток технологічних процесів, саме тому керування доступом шляхом використання біометричних даних на основі SSO являєтеся такою великою необхідністю.

Сьогодні платформою де ми часто використовується біометричні даній на основі SSO в Україні є саме проект Державного підприємства «ДІЯ», а саме в автоматизованій системі ДІЯ, адже створення таких автоматизованих систем, що дозволяють можливість звертатись до суб'єктів владних повноважень органів влади та адміністрування та інших уповноважених осіб за наданням, як адміністративних та соціальних послуг не можливе без використання компонентів підтвердження особи її автентифікації і верифікації в системі, а розвиток сучасних гаджетів дозволяє ще більше спростити ці методи входу в систему чи застосунок. Це можна спостерігати кожен, адже для пришвидшення процесів входу використовується технології зчитування біометрії пальця Face-ID, а також інші варіації входу, проте саме авторизація за допомогою біометричних даних набирає найбільшої популярності адже автоматизація таких процесів є набагато зручнішої, а також дозволяє пришвидшувати роботу, чи виконання запиту.

Розвиток таких технологій і керування доступом на основі технологій SSO також забезпечує додаткові рівні безпеки збереження інформації, що є дуже необхідною річчю на сьогоднішній день так і в майбутньому, адже із розвитком технологій завжди і зростає рівень можливостей цифрового шахрайства, це пояснюється тим, що у випадку стрімкого розвитку програмного забезпечення можливості захисту даних такого програмного забезпечення є обмеженні, адже пришвидшення випуску продукту на ринок передбачає собою пропуск тестування систем захисту від кібератак, а також інших варіацій злому, що в подальшому слугує використанням біометричними даними осіб у шахрайських цілях.

Тому саме постійне проведення аналізу безпеки програм, які використовую технології на основі варіацій єдиного входу на сьогоднішній день

є пріоритетом багатьох засновників різного програмного забезпечення, для захисту персональних данних

Метою роботи є проведення аналізу системи керування доступом шляхом використання біометричних даних на основі технології SSO.

– Відповідно до встановленої мети було вирішено такі завдання
– Здійснити всебічне аналізування біометричної автентифікації та проаналізувати варіативність застосування їх в системах керування доступом на основі технології SSO;
– створити процес ініціалізації до підсистеми на основі технології SSO з використанням біометричної автентифікації;

Об'єктами дослідження роботи є : автентифікація, реалізація авторизації, формування доступу до систем з використанням технології SSO при використанні біометричних даних.

Предметом дослідження дипломної роботи : методика формування авторизації за допомогою біометричних даних та керування доступом за допомогою технології Single Sign-On.

Актуальність роботи полягає в проведеному аналізі технології SSO, перегляду її переваг та недоліків, а також написанні фреймворку на основі C + дляавтентифікації по розпізнаванню відбитків пальців.

Практична цінність роботи: аналіз використання біометричних даних доступом, що базується на технології SSO, аналіз біометричних даних та автентифікації за відбитком пальця. Доведення факту що система дозволяє користувачам отримати санкціонований доступ одночасно до різних ресурсів системи з використанням технології єдиного входу.

Методами дослідження є: створення бази даних , що створюються на підґрунті фреймворку C+ і використовує бібліотеки .NET Framework для ефективної автентифікації з використанням відбитка пальця. Встановлено що процеси що створюються суспільство пришвидшують таку роботу в декілька сотень разів. На сьогоднішній день перспективним рішенням для захисту даних від несанкціонованого доступу є використання біометричних параметрів користувачів для автентифікації. Цей підхід базується на використанні біометричних характеристик

користувача, щоб уникнути проблем, пов'язаних з приватністю та конфіденційністю.

Головною вимогою є забезпечення безпечного зберігання унікальних і незаперечних біометричних даних. Саме ця проблема ускладнює використання криптографічних хеш-функцій для безпечного зберігання біометричної інформації. З розвитком технологій забезпечення збереження простих біометричних даних полегшилось проте саме цей розвиток і створює найбільший ризик спроби злому таких даних, або дешифровці збереження персональних даних є надзвичайно важливим, і одним з ефективних підходів до забезпечення безпеки є процес знеособлення. Знеособлення дозволяє знизити ризики недозволеного використання та заподіяння шкоди у разі витоку даних. Біометрична інформація також відносяться до персональних даних, яких необхідно надійно захищати від незаконного використання. Проте, звичайні методи знеособлення не є ефективними для інформаційних систем, що обробляють біометричні дані. Тому виникає актуальне завдання розробки спеціальних методів знеособлення, які враховують унікальні особливості біометричних даних та систем, що їх використовують.

Вирішенням такої проблематики стало необхідним кроком сьогодні, саме тому створення програмних забезпечень таких, як Single Sign-On призвело до закріплення її у використанні масовістю.

Це технологія разової автентифікації єдиного входу що англійською мовою несе найменування - «Single Sign-On», «SSO» - технологія авторизації (формування єдиного входу) до спеціальних програмних забезпечень за допомогою єдиного процесу автентифікації.

Розв’язання проблематики варіацій входу в систему за допомогою програмних комплексів на основі технологій єдиного входу дає інформаційним компаніям значну перевагу на ринку, що в подальшому допомагає залучити все більше інвестицій в компанію та розвивати таку продукцію чи створювати нову.

# РОЗДІЛ 1. АВТОРИЗАЦІЯ ТА АВТЕНТИФІКАЦІЯ В АТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

## 1.1 Поняття інформаційних систем

Інформаційні системи - це комплексні системи, які забезпечують збір, обробку, зберігання і передачу інформації з метою підтримки прийняття рішень і виконання різних функцій в організаціях або у особистому житті. Їх основна мета полягає в забезпеченні доступу до відповідних даних, їх обробці і аналізі для підтримки прийняття ефективних рішень.

Інформаційні системи можуть включати в себе різні компоненти, такі як внутрішнє програмне забезпечення , бази даних, мережі зв'язку та людський фактор. Вони забезпечують можливість збирати дані з різних джерел, обробляти їх за допомогою спеціальних алгоритмів і аналітичних інструментів, а також забезпечують зручні інтерфейси для користувачів для взаємодії з системою, складаються з різних частин, які працюють разом, щоб обробляти та передавати інформацію. Основні складові цих систем включають комп'ютери, сервери та різні модулі, які забезпечують обчислювальну потужність і зберігання даних. Програмне забезпечення, таке як операційна система та програми, дозволяє управляти цими пристроями та виконувати завдання обробки даних. Бази даних забезпечують зберігання і організацію інформації, а мережі зв'язку дозволяють передавати дані між різними компонентами системи. Алгоритми і програми визначають, як система повинна обробляти дані, а інтерфейси користувача надають зручний спосіб взаємодії з системою для користувачів. Всі ці частини разом створюють інформаційну систему, яка може збирати, обробляти, зберігати і передавати інформацію з метою підтримки різних функцій та прийняття рішень. Визначення даних їх обробка та зберігання є невід’ємною складовою становлення системи функціювання більшості програмних забезпечень, а також систем бази даних які використовую систему авторизації, автентифікації особи за допомогою невід’ємного на сьогоднішній час алгоритму обробки персональних даних.

Використання інформаційних систем на базі звичайного користувача ПЗ є невід'ємною частиною життєдіяльності людини на сьогоднішній час.

Основною метою створення інформаційних систем являєтеся комплексний підхід до формування, обробки та зберігання інформації, яка створюється в процесі життєдіяльності людини. Важливість також можна підкреслити наступними факторами Підтримка прийняття рішень: Інформаційні системи надають доступ до актуальних та точних даних, що допомагають в процесі прийняття рішень. Вони можуть забезпечити аналітичні інструменти, здатні проводити комплексний аналіз даних та надавати цінні висновки та рекомендації для структурним підрозділам, фізичним особам зайнятими із систематичною обробкою даних.

Інформаційні системи, що покращують комунікацію, надають зручні засоби для обміну інформацією та спілкування між різними особами та відділами в організації. Вони спрощують спільну роботу над проектами, спільний доступ до документів і обмін повідомленнями, що сприяє поліпшенню комунікації та співпраці.

Підвищення конкурентоспроможності: Завдяки ефективній обробці та використанню інформації, організації можуть збільшити свою конкурентоспроможність. Інформаційні системи допомагають виявляти нові можливості, вдосконалювати продукти та послуги, а також оптимізувати виробничі процеси, що дозволяє досягти більшої ефективності на ринку.

На сьогоднішній день використання даних інформаційних систем забезпечує основині потреби обробки даних, які використовуються у в органах державної влади, в органах місцевого самоврядування та інших верствах, для забезпечення життєдіяльності суспільства, та систематизації даних, які створюються в процесі життєдіяльності людини.

Зараз авторизація є важливим аспектом через зростання впливу людського фактору на роботу автоматизованих систем та популярність надання послуг віддалено через Інтернет. Це вимагає ідентифікації користувача, який планує скористатися відповідними послугами.

Авторизація - це процес перевірки прав доступу до виконання певних

операцій. зміни даних. Це необхідно для забезпечення безпеки під час виконання різних дій, для розмежування прав користувачів та для захисту від зловмисників. Механізм авторизації застосовується на веб-сайтах, в банкоматах, інтернет-магазинах та державних установах. Зазвичай користувачеві потрібно ввести свій логін та пароль. Якщо введені дані є правильними, користувачу надається доступ до системи та можливість виконувати дозволені операції. У разі помилки вхід до системи не дозволяється. При виникненні помилки авторизації, яка включає неправильне введення логіну, паролю та інших даних, система може застосовувати наступні дії:

Блокування доступу користувача: Система може тимчасово або постійно на регулярній основ і здійснити блокування усіх прав користувача системи, який допустив помилку авторизації.

Повідомлення про помилку: Система може відображати повідомлення про помилку авторизації, яке повідомляє користувача про невірність введених даних.

Забезпечення додаткових заходів безпеки: В разі повторних помилкових спроб авторизації система може вимагати виконання додаткових заходів безпеки, таких як введення капчі або відправку коду перевірки на зареєстрований номер телефону або електронну пошту.

Такі заходи допомагають захистити обліковий запис користувача від несанкціонованого доступу та підвищують безпеку системи авторизації.

- формування реєстру не задекларованого доступу;
- встановлення спеціального музичного або світлового сигналу, повідомлень на екрані;
- обмеження варіацій входу на встановлений період
- необхідність повторної ініціалізації
- відновлення паролю;
- обмеження облікового профілю-запису.

Інформацій код найпростіший варіант входу, який зберігається в локальній пам’яті, а також використовується для ідентифікації можливостей та прав користувача. Зазвичай це комбінації з 3 до 12 символів, таких як букви,

цифри та знаки, які вводяться у визначеному порядку. Ключі генерації входу під час реєстрації користувача і може бути змінений власником облікового запису або за необхідності з міркувань безпеки. Часто існує обмеження на кількість змін комбінацій протягом певного періоду часу. Для безпечного використання сервісу користувачу необхідно тримати код авторизації в недоступному місці від інших та не розповсюджувати його. Використання входу за допомогою авторизації  надає користувачу можливість отримати доступ до різних функцій, таких як зміна варіацій власного облікового запису взаємодія з інтерфейсом системи, зміна паролю, керування рахунком та внесення змін у систему. . При вході в підсистему шляхом авторизації в ній, підсистема може створювати нові шари захисту, або  використовуються інші варіації захисту та формування інших варіацій за допомогою sms підтвердження чи підтвердження додаткового паролю.

При вході в підсистему, є велика ймовірність, що авторизація буде недоступна для користувача. У таких випадках потрібно повторно авторизуватись, дотримуючись ряду вимог: створення нового (запасного) паролю або логіну. Це можна буде зробити самостійно, використовуючи електронну пошту або зателефонувавши до служби технічної підтримки. Користувачу сервісу може появитись повідомлення “Авторизація недоступна” у кількох випадках, наведених на рисунку 1.1


Рисунок 1.1 - випадки видачі повідомлення “Авторизація недоступна”

Дані авторизації включають інформацію, яку користувач системи повинен надати для підтвердження свого права доступу до виконання операцій. Зазвичай це включає логін та пароль. Є також такі ситуації, що використовується індивідуальні дані (прізвище, ім’я, по батькові, посаду і т.д.). Будь-які дані, що використовується для авторизації, повинні зберігатися в системі і при потребі міняються службою безпеки чи навіть самим користувачем. Якщо сталось так, що користувач сервісу втратив дані для доступу в систему, він зобов’язаний розпочати процедуру відновлення, яка може включити повторну ідентифікацію за допомогою SMS або електронної пошти, або шляхом звернення до служби технічної підтримки. Щоб гарантувати комфортність користувачів, застосування наявного програмного забезпечення, та виконання умов заходів безпеки, запровадженні різноманітні режими доступу. Часто використовується комбінація декількох таких режимів.

Авторизація існує двох видів:

- онлайн – здійснюється тільки завдяки активного підключення до інтернет-мережі;
- офлайн – це вхід в систему без доступу до інтернет-мережі.

В свою чергу процеси авторизації групуються на три класи:

Доступ до об’єктів, даних або функцій можуть отримати лише визначені суб’єкти, користувачі або групи користувачів із дискреційним контролем доступу. Власники об’єктів відповідають за встановлення прав доступу, тому користувач_1 може читати файл_1, але не змінювати його. Також є супер користувач, який може регулювати права доступу для всіх, а звичайні користувачі можуть передавати свої права іншим. Кожен об’єкт закріплений визначеного суб'єкта, свого власника, закріпленого за ним. У цю епоху технологій авторизація надається через впровадження списків контролю доступу (ACL) і прав у поточних операційних системах. Відповідно до принципів обов'язкового контролю доступу інформація розподіляється за рівнем конфіденційності та відповідно до цього користувачам призначаються рівні доступу до цієї інформації. Найвигіднішим аспектом цього підходу є те, що він обмежує привілеї користувача призначеним об'єктом. Права власності

на об’єкти для користувачів визначатимуться на основі їх позиції серед визначених рівнів доступу. Відповідно вони не зможуть випадково або спеціально видати їх неавторизованим користувачам.

Формування політик користування доступом на основі ролей є розширенням політики вибіркового доступу, де доступ до об'єктів системи формується, враховуючи конкретні ролі суб'єктів в кожний момент часу на правах адміністратора чи користувача. Ролі дозволяють встановлювати зрозумілі правила розмежування доступу для користувачів. Роль поєднує в собі аспекти окремого керування на основі наданих прав та можливостей , встановлюючи відповідні об'єкти для суб'єктів. При зміні ролей змінюється доступ до групи файлів. Цей тип доступу є більш гнучким у порівнянні з попередніми моделями та дозволяє їх ефективне моделювання.

## 1.2 Поняття автентифікації авторизації та її види

Автентифікацією – називається процедура верифікації належності суб’єкта інформації його авторизацію у підвідомчих системах та основний ланцюг процедури ідентифікації суб’єкта у підвідомчих системах.

Автентифікація здійснюється на основі багатьох різних елементів на вибір користувача підвідомчих систем, а також на виконання функціоналу системи яка може обмежувати тип та порядок входу до комплексу програмних забезпечень інформаційної системи.

Автентифікація здійснюється шляхом перевірки певного визначеного елемента (автентифікатора), який наявний як у суб'єкта, так і в інформаційній системі. Зазвичай система має доступ не до самого елемента, а до відповідної інформації про нього, на основі якої приймається рішення щодо відповідності ідентифікатора суб'єкта. [2 с.3].

Прикладом може слугувати система взаємодії електронних сертифікатів засвідчуваного органу та підпису, де операційна система взаємодіє із верствою бази даних, сервером на якому розміщуєтеся дана інформація, а також із хмарним сховищем таких сертифікатів. Операційна система зазвичай зберігає

не сам пароль, а його хеш–функцію, чи сертифікат виданий особі як додатковий захист перевірки даних, чи системи взаємодії ЕЦП із верифікатором даних. Існують різні методи автентифікації, які зображені на рисунку 1.2.

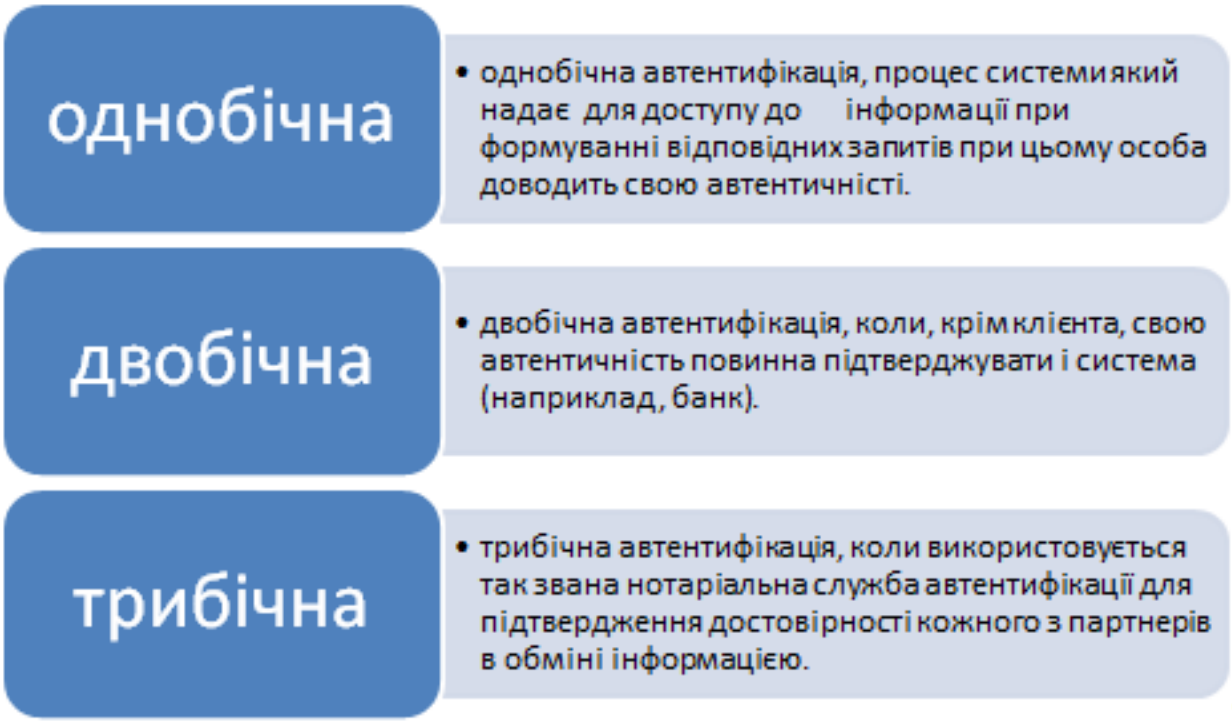


Рисунок 1.2 - методи автентифікації

Методи автентифікації в свою чергу поділяються на однофакторні та двофакторні.

Однофакторними методами є логічні (паролі, ключові фрази, що вносяться безпосередньо користувачем за допомогою клавіатури); ідентифікаційні - носієм, який файлове повідомлення збережене в системі чи іншому носію інформації, чи інша смарт-карта яка несе в собі записану інформацію для підтвердження особи та авторизовує осіб у системі.

На сьогоднішній день в України найпопулярнішим способом та найбільш розповсюдженіший варіантом входу являється саме однобічна одно факторна автентифікація , адже методологія випуску ЕЦП я найбільш доступною послугою, а захист таких персональних даних забезпечується можливістю створення одно-екземплярного ідентифікаторів.

Також із основних можливих варіанті слід відзначити біометричні способи серед який є як і розпізнавання голосу так і розпізнавання відбитку

долоні руки чи окремо пальця особи яка володіє парольною інформацію та під яку власне прописувався алгоритм автоматизації входу то підсистеми, а також варіація голосу, тембру та поведінкові варіації біометричного входу. тому забезпечення таких варіантів ідентифікації, обов'язковому порядку повинно забезпечуватись іншими додатковими видами ідентифікації, у зв'язку із можливістю втрати природи даних необхідних для біометричної ідентифікації, що трапляється доволі часто, а заміна біометричних даних супроводжується доволі затратними процедурами та складністю ведення таких відомостей ідентифікаторів у підвідомчу систему. [1 ст.18]

У майбутньому вхід у підсистеми програмних забезпечень за допомогою варіації розпізнавання біометричних матеріалів носіїв інформації таких як видбиток долоні чи пальця стане найпопулярнішою біометричною технологією. Його переваги включають швидку ідентифікацію, яка не вимагає від користувачів особливих зусиль, що робить його дуже зручним і надійним. Крім того, частота помилок ідентифікації користувача значно нижча якщо порівнювати такі варіації входу тому вона набуде масової популяризації у майбутньому Прикладом може бути саме використання геометрії відбитку долоні чи іншого зчитуваного біометричного матеріалу. Даний метод застосовується сьогодні у багатьох державах та багатьох організація установах та закладах світу що начислю уже на сьогоднішній день цифру більше семи тисяч серед яких є міжнародно-правові організації уряди та інші установи а найпопулярнішим з успішних практиків використання таких варіантів входу являється уряд Республіки Колумбія, Міжнародний Аеропорт Сан-Франциско, лікарні і імміграційні служби. Серед переваг ідентифікації по геометрії долоні у порівнянні з автентифікацією по відбитку пальця слугує саме питання надійності автентифікації таких аспектів інформації та авторизації згідно окремого біо-матеріалу дуплікація якого стає практично неможлива, хоча пристрій для читання відбитків долонь є більш габаритним та ускладнює облаштування такого у багатьох установах де існує необхідність в облаштуванні такого варіанту автентифікації. Серед таких пристрої слід відзначити саме найбільш досконалий пристрій в системі автентифікації згідно

біологічного матеріалу (долоні) “Handkey”, котрий сканує як внутрішню, так і бічну сторону руки.

Ще одним із найбільш розповсюджених варіантів автентифікація за скануванням окремої частини людського ока, який авторизує вхід у підвідомчу систему за допомогою розпізнавання райдужної оболонки ока, адже даний біометричний матеріал несе більше окремих об’єктів, котрі можна перетворити у дані, для більш надійнішого захисту даних, чи відокремлення можливості злому підсистеми оброблення інформації це надає великі переваги.

Цей прогрес пояснюється розквітом мультимедійних відео технологій. Незважаючи на це, розробники намагаються досягти оптимальної продуктивності цих пристроїв. Тим не менш, ми очікуємо появи спеціалізованих систем розпізнавання обличчя в терміналах аеропорту для забезпечення міжнародного захисту та захисту суверенітету та цілісності а також для безпеки громадян.

Найпоширеним варіантом для забезпечення додаткового ступеню захисту використання аспектів авторизації є двофакторний метод, який в свою чергу базується на програмі використання двох чи більше простіших варіації входу та авторизації пов’язаних із використанням простих але послідовних методів однофакторної авторизації, що збільшує в свою чергу рівень безпеки в цілому у двічі, це показово наведено на рисунку 1.3.

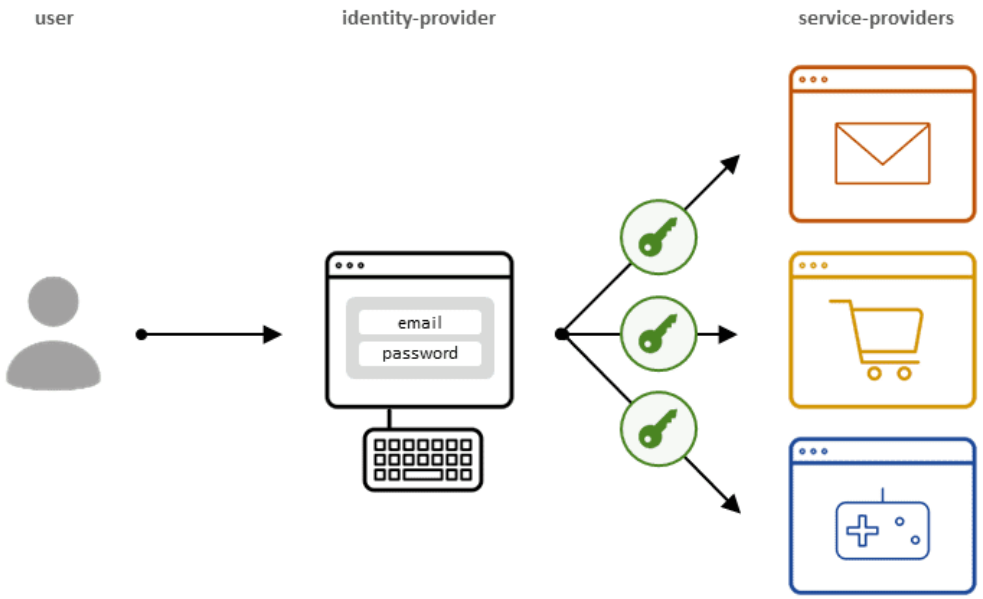

Рисунок 1.3 - Двофакторний метод автентифікації.

Найпоширенішим мабуть серед таких використання саме логін та паролю, або паролю і та ключа і особистим цифровим підписом, чи іншим обов'язковим модулем як наприклад дискетою, чи токеном що відображений на рисунку 1.4.


Рисунок 1.4 - Токен

Насправді кожен метод чи кожна варіація такого входу в підсистему за допомогою авторизації за тим чи іншим методом має свої переваги та недоліки, серед яких найбільшим недоліком невиправленим на сьогоднішній день є те, що підсистемі не потрібно, що даний суб'єкт, об'єкт чи носій інформації був відповідним користувачем під якого саме писався скрип чи модуль, а лише потрібно відповідати встановленим вимогам інформації, що в свою чергу дозволяє зловмисникам здійснювати вхід до систем не витрачаючи додаткових зусиль особливо коли це однофакторний метод.[2 ст.16]

Серед найбільш розповсюджених варіації автентифікації особи в системі мабуть є саме вхід за допомогою паролю, що даний метод є спрощеним в порівнянні із всіма іншими методами авторизації він є одним чи не найменш незахищеним у свої групі, адже пароль є слабкою системою захисту яка легко може забутись самим користувачем, так і може бути отримана в процесі за спостерігання за особою за динамікою пальців набору чисел яких вона часто використовую, а на професійному рівні може легко обходитись шляхом комбінатора який записує код підбирає усі можливі варіанти паролю та запускає програму ініціалізації таких цифр та символів.

З метою створити саме запам'ятовувальний пароль для особи часто використовується саме найбільш притаманні особі об'єкти та джерела, які нею

часто використовуються серед яких можуть бути, як імена близьких родичів чи їх рік народження, власні паспортні данні, імена домашніх улюбленці та інше що робить саме авторизацію за допомогою паролю дуже вразливою, хоча комбінування неприродніх наборів чисел може додати додаткового рівня захисту такої авторизації, хоча в цьому аспектів найбільш вразливою деталлю, є саме людський фактор

Проте саме ведення паролю і саме пароль можна з легкістю переглянути за допомогою брандмауера та з'ясувати ключ ідентифікатор, що робить це вразливим до різних видів витоку такої інформації що містить предмет ідентифікації.

### 1.3 Поняття та застосування SSO в сучасних інформаційних системах

Станом на сьогоднішній день безпосередній користувач та клієнт такої системи зіштовхуєтеся саме із проблематикою постійного входу з використанням неоднорідних паролей, облікових записів. Якщо вони працюють із розширеними платформами та додатками, їм потрібно постійно вводити свої дані для авторизації у систему

Технологія єдиного входу (SSO) являється мультифункціональним помічником, а також вирішенням цих проблем, що виникають у багатьох користувачів відповідних підсистем.

Механізм єдиного входу (SSO) є системою перевірки сеансу, яка дозволяє клієнтам використовувати один набір облікових даних, таких як ім'я користувача та пароль, щоб отримати доступ до необхідного програмного забезпечення. Даний механізм здійснює автоматичну перевірку клієнта для кожної програми та забезпечує необхідну повторну автентифікацію при перемиканні користувачів між іншими програмами протягом одного сеансу.

Механізм єдиного входу можна розглядати як програмний підхід, що спрямований на задоволення потреб користувача, незалежно від угод, укладених на серверній стороні. Наразі існує такі найпоширеніші механізми єдиного входу:

єдиний вхід в систему підприємства, Kerberos (автентифікація витків/токенів), відкритий ідентифікатор або зібрана інформація.

SSO (одночасна автентифікація) не є окремим поняттям, а скоріше терміном, який використовується для всіх методів, комбінацій або пристроїв, спрямованих на зменшення завантаження на кілька загальних точок входу в течії сеансу. Це означає, що користувачі можуть отримати погоду, яка є доступною для них і забезпечує безперешкодний доступ до їх ресурсів. Водночас це надає додаткові переваги підприємствам, які піклуються про безпеку та послідовність. Виконання цих заходів включає основи механізму єдиного входу.

Головною перевагою технології єдиного входу (SSO) є здатність користувача отримувати доступ до різноманітних систем без необхідності входу в кожну з них окремо. Це відображено на рисунку 1.5.

Рисунок 1.5 - Основна перевага SSO

Основними недоліками технології SSO є:

- Порушені дані входу користувача можуть призвести до доступу до багатьох додатків.
- Виробник може не використовувати загальноприйнятий стандарт або використовувати стандарти, які несумісні з іншими додатками.

Початкова реалізація ускладнюється залежно від кількості наявних непорівнянних систем. Хоча біометричні системи вважаються надійними,

дослідники активно працюють над виявленням потенційних вразливостей цієї технології та розробкою заходів для їх запобігання. Біометричні системи використовуються для ідентифікації особи на основі її анатомічних особливостей, таких як відбитки пальців, образ обличчя, малюнок ліній долоні, райдужна оболонка ока та голос, або особистого підпису. Так, як перелічені риси унікальні для кожної особи і пов'язані з їх фізичними характеристиками, біометричне розпізнавання виконує роль механізму, який гарантує, що лише особи з необхідними повноваженнями мають доступ до будівель, комп'ютерних систем або можуть перетнути кордони держави. Унікальність біометричних систем має свої переваги, такі як здатність виявляти суб’єкт входу в систему. [16 ст.12]

Отже, застосування системи SSO в сучасних інформаційних системах відіграє дуже важливу роль, адже майже вдесятеро раз покращує авторизацію та ідентифікацію особи в  підсистемах, а авторизація за біометричними даними, а також двоетапна формує захищену ресурсну базу інформації необхідної для авторизації. Використання даної системи  входу допомагає спрощувати та пришвидшувати процеси пов’язанні із забезпеченням обробки даних, а у майбутньому автентифікація за відбитками пальців стане найпопулярнішою біометричною технологією. Його переваги включають швидку ідентифікацію, яка не вимагає від користувачів особливих зусиль, що робить його дуже зручним і надійним, що допоможе подолати низьку соціальних проблем пов’язаних саме із встановленням особи, пришвидшення впровадження та стрімкий розвиток таких технологій забезпечить не тільки вирішення громадських проблем, трудових проблем що виникають на робочому місці, а також забезпечить, захист інформації від можливого дешифрування, адже станом на сьогоднішній день практично усі підсистеми використовують процедуру двоетапної перевірки особи, а також зменшить надання деяких адміністративних та соціальних послуг населенню.

Отже, Проблемним питанням на сьогоднішній день являєтеся саме передача паролів третім особам, щоб на деякий час здійснити заміну власника пароля у своїй роботі. В теорії найкращим варіантом в таких ситуаціях

являєтеся саме генерація нового сертифікату входу, окремого ключа, чи інших засобів авторизації із використанням власних даних авторизації, але на практиці такі дії не виконуються, а безпека захисту даних порушуєтеся, як третьою особою так і самим користувачем підвідомчої системи SSO.

Проблематикою також являєтеся систематичні помилки власників авторифікаторів засобів авторизації, адже при генерації таких засобів, особи створюють паролі до підсистем користувача, які не потребують додаткових зусиль для генерації потрібних чисел, запрограмувавши повний перебір (передбачається, що алгоритм шифрування відомий) можна з легкістю здійснити генерацію потрібного паролю.

Однак важливі заходи дозволяють значно підвищити надійність захисту паролем:

– накладати технічні обмеження (паролі не повинні бути надто короткими, містити букви та цифри);

– управління терміном дії пароля: регулярно змінюйте; – обмежити доступ до файлів паролів;

– скоротити кількість невдалих спроб авторизації, що ускладнить використання «грубої сили»;

– навчання користувачів;

–використовуйте програмний генератор паролів (такі програми, засновані на простих правилах, можуть генерувати лише паролі, що добре звучать, а отже, такі, що запам’ятовуються).

Ідентифікація – це процедура авторизації за допомогою визначення такого користувача програми чи адміністратора програми відповідно до завданих програмним забезпеченням характеристик (ідентифікатора) або іншої прошитої інформації про нього, яка сприймається системою.

Ідентифікація об'єкта означає його розпізнавання і встановлення зв'язку з чим-небудь. У контексті інформаційних технологій, цей термін відноситься до процесу визначення особистості користувача. Цей процес необхідний для того, щоб система могла приймати рішення щодо надання людині дозволу на роботу з комп'ютером, доступ до конфіденційної інформації та інше. Таким чином, ідентифікація є одним з ключових понять в інформаційній безпеці

# РОЗДІЛ 2. SSO ТЕХНОЛОГІЇ, ЯК СИСТЕМА УСУНЕННЯ ЗАПИТІВ НА АВТЕНТИФІКАЦІЮ ОСОБИ ТА БЕЗПЕКА ЇЇ ВИКОРИСТАННЯ

## 2.1. Аналіз безпеки SSO та її ризики

Протягом останніх сто років правоохоронні органи успішно завершили біометричну автентифікацію з використанням сформованого об’єкту біометричного матеріалу а саме дактилоскопії (відбитку пальця-долоні) у своїх розслідуваннях, а в останнє десятиліття стало швидке поширення системи біометричного розпізнавання в урядових і комерційних організаціях по всьому світу. Багато з цих впроваджень випущено дуже успішно, проте підтримує певні непорозуміння щодо безпеки біометричних систем та можливе порушення конфіденційності через несанкціоновану публікацію користувачів сформованих біометричних даних. Як і в разі будь-якого іншого автентифікаційного механізму, біометричну систему можна зламати, а досвідченим програмістом-шахраєм, який має достатній час та ресурси можуть бути завданні серйозні витрати компанії володільцем системи взаємодії SSO. Важливо розвивати ці оброблення, щоб заслужити довіру суспільства до біометричних технологій.

У сьогоденні спостерігаються дві виражені тенденції розвитку систем та заходів захисту персональних даних та інформації в цілому.

- масове використання асиметричної криптографії (пари з відкритого і закритого ключа-доступу );
- посилення процедур ідентифікації та авторизації за допомогою біометричних технологій.

Згідно з експертами зі сфери безпеки як українських, так і зарубіжних, можна підвищити безпеку використання асиметричної криптографії шляхом пов'язування відкритих і закритих ключів з біометричними даними їх власника. Під час авторизації особи для управління закритим криптографічним ключем важливо забезпечити конфіденційність закритого біометричного образу. Відкритий ключ може бути пов'язаний з публічним біометричним

характеристиками особи, наприклад, з тривимірною маскою обличчя. Закритий ключ обов'язково повинен бути пов'язаний з приватним (таємним) образом особи, наприклад, з його рукописним паролем. [3 ст.12]

У процесі реєстрації біометричний образ зчитується спеціальним пристроєм для збору біометричних даних. Після цього параметри користувача виокремлюються, і на їх основі формується біометричний шаблон. Цей шаблон разом з унікальним ідентифікатором, який користувач має або отримує під час реєстрації, зберігаються в базі даних. Ідентифікатор користувача та біометричний шаблон можуть бути збережені на смарт-картці або токені.

Під час верифікації користувач пред’являє системний ідентифікатор та біометричні дані. Після цього значення параметрів користувача обчислюються і порівнюються з параметрами біометричного шаблону, який витягується з бази даних для відповідного ідентифікатора. На основі цього порівняння приймається рішення і дається відповідь на питання "Чи ця особа є тим, за кого вона себе видає?" результатом може бути "Так" або "Ні".

Біометрична система також може виконувати ідентифікацію особи, відповідаючи на питання, чи належать біометричні дані комусь з користувачів системи.

Під час порівняння біометричних параметрів, обчислюється міра подібності S, яка потім порівнюється з граничним значенням T. Якщо значення S більше або дорівнює T, тоді приймається рішення, що біометричні параметри та параметри біометричного шаблону належать одній людині. З іншого боку, якщо значення S менше T, приймається висновок, що параметри належать різним людям.

SSO (Single Sign-On) спрощує складність різнорідної архітектури безпеки шляхом використання єдиного входу. Система, яка використовує SSO, має здатність керувати ресурсами, інформаційними послугами та управлінням даними. Крім того, безпека повинна бути забезпечена на всіх рівнях архітектури безпеки.

Для досягнення цієї вимоги щодо наскрізної безпеки використовуються різні методи та підходи асоціацій безпеки (SA). Кожна асоціація безпеки

визначає протоколи, ключі та алгоритми шифрування, які необхідно використовувати. Порушення у створенні асоціацій безпеки можуть призвести до проблем у функціонуванні відповідної частини організаційної системи.

Ефективність асоціацій безпеки (SA) залежить від використовуваних алгоритмів шифрування та хешування. Деякі алгоритми, зокрема алгоритми шифрування відкритих ключів, є обчислювальними витратами через великі розміри криптографічних ключів, вимоги до використання двох криптографічних ключів замість одного, а також необхідно введення органу сертифікації, додатково також системи пошуку доменних імен та перевірки сертифікатів. Використання інфраструктури відкритих ключів (PKI) забезпечує рівень безпеки, прете існує імовірність того, що це  призведе до збільшення часу перегляду сервера через вищевказані обмеження.

Веб-система SSO, або система єдиного входу, пропонує веб-архітектуру, де клієнти можуть мати потребу входити в різні веб-системи, але їм потрібно це зробити лише один раз. Основна мета такої системи полягає у тому, щоб кожен користувач увійшов лише один раз за сеанс. Хоча ця система може бути внутрішньою для мережі, її головне призначення - забезпечити єдиний вхід для кожного користувача.

З метою забезпечення безпеки, SSO використовує маркери або файли cookie, а також протокол обміну метаданими заявок про твердження (SAML). Маркери перевірки передаються через захищений канал, зазвичай за допомогою протоколу SSL (Secure Sockets Layer). Для SSL використовуються серверні сертифікати, а криптографічні функції SSL надаються клієнтам через веб-браузери.

Після успішної процедури автентифікації, ці об’єкти ідентифікації надсилаються захищеними каналами до інших систем безпеки для перевірки ідентичності користувача. Після цього маркери видаляються, а ідентифікаційні підписи передаються системі, що почала транзакцію. Це дає клієнтській системі можливість отримати доступ до даних або інших ресурсів. [5 ст.33]

SSO (Single Sign-On) дійсно може бути корисним для компаній, які працюють через COVID-19. Його головна перевага проблема в тому, що він

надає безпечну та зручну автентифікацію для віддаленого входу. Замість того, щоб користувачам доводитися запам’ятовувати багато різних паролів для різних систем, SSO дозволяє їм використовувати один раз і мати доступ до багатьох ресурсів без необхідності повторної автентифікації.

Крім того, використання SSO може бути частиною системи керування доступом, що дозволяє швидше надавати та скасовувати доступ користувачів до різних ресурсів. Це полегшує процес управління користувачами, особливо великими організаціями з багатьма співробітниками.

Однак SSO також має свої ризики. Оскільки він створює єдину точку збою, якщо зловмисник отримує доступ до цієї точки, він може отримати доступ до всіх пов’язаних із нею програмою. Тому важливо приділяти достатню увагу безпеці впровадження SSO, зокрема застосуванню надійних механізмів автентифікації та моніторингу діяльності користувачів.

Також важливо враховувати, що впровадження та конфігурація SSO можуть бути складними і вимагати додаткових зусиль та витрат. Це може бути особливо проблематичним для малого та середнього бізнесу з обмеженими ресурсами.

Додатковою негативною стороною SSO є те, що багато постачальників системи єдиного входу стягують плату за кожну функцію окремо. Це означає, що комісія  за обслуговування такої системи може швидко зрости в ціновій політиці.

## 2.2 Біометричні характеристики які використовуються в системі sso

Біометричні характеристики людини можна поділити на дві категорії: статичні та динамічні характеристики. Аспектичні біометричні показники представляють собою фізіологічні особливості, які залишаються незмінними протягом життя особи. До цих Фізичних показників та аспектів належать:

- геометрія обличчя ;
- відбитки пальців руки;
- райдужна сітківка очного тіла ;
- геометрія долоні чи руки

Фізичні аспекти зчитування інформації можуть бути утраченими через захворювання або внаслідок фізичного (хірургічного) втручання в органи людини.

Щодо рухомих характеристик, які використовуються в біометричних авторизація відносяться:

- формування динаміки почерку людини ;
- голос;
- властивість ходи та її поведінка.

Не існує універсальної біометричної характеристики, котра би задовольняла заявлені потреби. Кожна біометрична характеристика має свої переваги і недоліки. Процес отримання біологічних характеристик повинен бути най більш швидким і простим, не спричиняючи жодних незручностей для фізичної особи.

У сучасний час Використання біометричних даних особи складає більше обов'язок ніж новостворена можливість, якою варто скористатись, такий обов'язком навіть закріплюєтеся на державному рівні багатьох країн. Проте із розвитком таких технологій і навіть за допомогою обміну інформації із різними країнами найпоширеніша варіації входу часто моделюють погане 2D[7 ст.12]

Двоетапний аналіз прямого зображення полягає саме у визначенні на ньому характерних абрисів і обчисленні геометрії, а саме відстаней між очними яблуками(райдужними оболонками в цілому), між лінією ока та закінченням

носа та інші.

Двоетапний аналіз прямого зображення людського обличчя встановлює не та і багато окремих об’єктів інформації.

Відбиток пальця, який представляє папілярний візерунок, зараз широко використовується в дактилоскопії, що є важливою складовою криміналістики та детективної роботи. Завдяки мініатюрним сканерам для зчитування папілярних відбитків, стало можливим використання цього біометричного показника для підтвердження особистості в підсистемах керування, адміністрування та управління доступом. Також важливо зазначити, що використання відбитків пальців є необхідним у паспортній, візовій та імміграційній політиці а також криміналістиці у багатьох країнах.

Райдужна форма сітківки людського є своєю надприродною формою унікальності фізіологічною характеристикою людини. Процес сканування обґрунтовується на використанні інфрачервоного випромінювання, яке поглинається меланіном, відповідальним за формування окремих елементів пігменту ока при х хворобі. Вимір параметрів базується на отриманому зображенні.

На сьогоднішній день є два основних підходи до ідентифікації геометрії рук людини. Перший підхід базується на геометричних характеристиках кісти. Другий підхід є сучасним, крім геометричних параметрів, корисною інформацією про розташування кровоносних судин рук.

Рукописний почерк є динамічною характеристикою, яка відображає особливості поведінки людини. Вимірюванням параметрів є залежності координат руху пера від часу, які зазвичай отримуються за допомогою графічного планшета.

Голосовий почерк також володіє певним ступенем унікальності. Використання голосових біометричних характеристик включає в себе визначення літературно-мовних фраз одній культурі особи та ідентифікацію особистості за допомогою голосу, що застосовується в криміналістиці. Автоматичні системи розпізнавання можуть вимірювати показники при врахуванні основи первинних характеристик сигналів, що виникають при

вимові мови і  мають як свій власний тембр так форми подачі голосового об’єкту, який пізніше зчитуєтеся як інформація, тоді як інші є шиплячими і не мають  такого періодичного характеру.

Відображення сітківки чи райдужної оболонки людського ока є унікальним для кожної особи. У цьому методі важним є не лише спеціальна камера, але й надійне програмне забезпечення. Саме завдяки програмному забезпеченню з отриманого зображення виокремлюється малюнок потрібної райдужної оболонки. Цей метод вважається одним з найточніших серед усіх біометричних методів.

Також слід зазначити, що на сучасному ринку біометричних рішень розпізнавання голосу стає все більш розширеною цією технологією. Раніше такі системи майже не зустрічалися, але зі зростанням кількості постачальників вони набирають популярність завдяки своїй простоті розгортання та іншим перевагам. Крім того, фінансова сфера є одним з основних напрямків застосування цієї технології. Наприклад, багато брокерських установ пропонують своїм клієнтам розпізнавання голосу як засіб швидкої верифікації. Замість введення PIN-коду та номера соціального страхування клієнт може швидко ідентифікуватися за допомогою розпізнавання голосу. Це дозволяє значно прискорити фінансові операції для клієнтів. Крім того, розпізнавання голосу можна використовувати на смартфонах як засоби замість введення перевіреного цифрового пароля.

Ці  та інші технології найбільш використовуються підсистемою MegaMatcher

Технологія MegaMatcher для великомасштабних автоматизованих систем біометричної ідентифікації була представлена в 2005 році. З того часу технологія постійно вдосконалювалася, на сьогодні випущено понад 10 основних і додаткових версій.

Технологія MegaMatcher доступна як багато платформний SDK, який включає механізми розпізнавання відбитків пальців, обличчя, динаміка, райдужної оболонки ока та долоні, а також об’єднаний алгоритм для швидкої та надійної ідентифікації у великих системах. Біометричні програмні механізми

базуються на глибоких нейронних мережах і містять багато власних алгоритмічних рішень, які особливо корисні для великомасштабних проблем ідентифікації. Деякі з цих рішень наведено в описі системи біометричної ідентифікації відбитків пальців, обличчя, голосу та райдужної оболонки ока нижче.

Повна відповідність MINEX. NIST визнав алгоритм відбитків пальців MegaMatcher сумісним з MINEX і є придатним для використання в програмі перевірки особи (PIV).

Відбитки згорнутих і плоских пальців збігаються. Механізм відбитків пальців MegaMatcher зіставляє згорнуті та плоскі відбитки пальців між собою. Як правило, звичайні «плоскі» алгоритми ідентифікації відбитків пальців виконують порівняння між плоскими та згорнутими відбитками менш надійно через специфічні деформації згорнутих відбитків пальців. MegaMatcher дозволяє зіставляти відбитки пальців від плоского до плоского, від плоского до згорнутого або згорнутого до згорнутого з високим ступенем надійності та точності. Алгоритм зіставляє до 200 000 плоских записів відбитків пальців на секунду на одному ПК.

MegaMatcher містить функцію визначення якості зображення відбитка пальця, яку можна використовувати під час реєстрації, щоб переконатися, що в базі даних зберігатиметься лише шаблон відбитка пальця найкращої якості. Визначення якості зображення може визначити, чи палець занадто вологий, занадто сухий, натиснутий занадто сильно чи недостатньо, чи присутні лише кінчики пальців.

Підробка виявлення відбитків пальців. Класифікація відсканованих зображень відбитків пальців на основі глибокого навчання використовується для розділення живих і неживих відбитків пальців для виявлення атаки презентації пальців. Ця функція охоплює спроби спуфінгу, здійснені за допомогою ecoflex, клею для дерева, латексу та желатину, і корисна для виявлення шахрайства.

Узагальнення шаблону використовується для створення якіснішого шаблону з кількох відбитків пальців. Краща якість шаблонів забезпечує вищий

рівень точності ідентифікації.

MegaMatcher стійкий до перекладу відбитків пальців, обертання та деформації. Він використовує власний алгоритм зіставлення відбитків пальців, який ідентифікує відбитки пальців, навіть якщо вони повернуті, перекладені або мають деформацію. Крім того, алгоритм зіставлення має спеціальний режим для зіставлення різномасштабних записів відбитків пальців, а також опціональне зіставлення дзеркальних відбитків пальців.

Адаптивний алгоритм фільтрації зображення усуває шуми, розриви та застряглі виступи та надійно виділяє дрібниці навіть із найнижчої якості відбитків менш ніж за 1 секунду.

Механізм вилучення шаблонів обличчя та зіставлення MegaMatcher.

Толерантність до положення обличчям забезпечує рівень зручності реєстрації. MegaMatcher дозволяє повертати голову на 360 градусів. Нахил голови може бути до 15 градусів у кожному напрямку від фронтального положення. Кут повороту голови може становити до 45 градусів у кожному напрямку від фронтального положення.

Надійне розпізнавання обличчя забезпечує точну реєстрацію з камер, веб-камер і різноманітних відсканованих документів; обличчя можуть бути зареєстровані зі сканованих сторінок паспорта чи інших видів документів. Якщо у відео або на зображенні є кілька обличь, їх можна зареєструвати та обробляти одночасно. За бажанням можна визначити стать людини, риси обличчя та основні емоції. Крім того, частково закриті обличчя (тобто особи в масках або респіраторах) можна розпізнати без окремої реєстрації.

Розпізнавання ознак обличчя. MegaMatcher можна налаштувати для виявлення певних атрибутів під час виділення обличчя – посмішки, відкритого рота, закритих очей, окулярів, темних окулярів, бороди та вусів.

Оцінка віку.MegaMatcher може додатково оцінити вік людини, аналізуючи виявлене обличчя на зображенні.

Виявлення живості обличчя.Звичайну систему ідентифікації обличчя можна обдурити, розмістивши фотографію перед камерою. MegaMatcher

здатний запобігти таким порушенням безпеки, визначаючи, чи є обличчя у відео потоці чи окремому кадрі «живим» чи фотографією. Виявлення живості може виконуватися в пасивному режимі, коли механізм оцінює певні риси обличчя, і в активному режимі, коли механізм оцінює реакцію користувача на виконання дій, таких як моргання або рухи головою. Щоб отримати докладніші відомості, перегляньте рекомендації щодо визначення живості обличчя.

Запис біометричного шаблону може містити кілька зразків обличчя однієї особи. Ці зразки можуть бути зареєстровані з різних джерел і в різний час, що дозволяє покращити роботу користувача під час зіставлення. Наприклад, особа може бути зареєстрована з окулярами та без них або з окулярами різних типів; з бородою чи вусами та без них тощо.

Залежна від тексту система підбору голосу визначає, чи відповідає зразок голосу шаблону, витягнутому з певної фрази. Під час реєстрації від особи, яка реєструється, запитується одна або кілька фраз. Пізніше цю людину можуть попросити вимовити певну фразу для перевірки. Цей метод забезпечує захист від використання таємно записаної випадкової фрази цієї особи.

Двофакторна автентифікація за допомогою фрази-паролю виконується, коли людину просять сказати унікальну фразу (наприклад, фразу-пароль або відповідь на «секретне запитання», яке знає лише зареєстрована особа). Загальна безпека системи підвищується, оскільки перевіряються автентичність голосу та пароль.

Незалежний від тексту механізм відповідності голосу використовує різні фрази для реєстрації та розпізнавання користувачів. Цей спосіб більш зручний, оскільки не вимагає від кожного користувача запам'ятовувати парольну фразу. Його можна поєднати з текст залежним алгоритмом для швидшого незалежного від тексту пошуку з подальшою перевіркою фрази за допомогою більш надійного текст залежного алгоритму.

Автоматичне визначення голосової активності. Механізм здатний визначити, коли користувачі починають і закінчують говорити.

Виявлення живості. Система може вимагати від кожного користувача зареєструвати набір унікальних фраз. Пізніше користувачеві буде

запропоновано вимовити певну фразу із зареєстрованого набору. Таким чином система може гарантувати перевірку живої людини (на відміну від самозванця, який використовує запис голосу).

Кілька голосових записів з тією самою фразою можуть зберігатися для підвищення надійності розпізнавання мовця. Певні природні варіації голосу (наприклад, хрипкий голос) або зміни навколишнього середовища (наприклад, в офісі та на природі) можна зберегти в одному шаблоні.

Механізм вилучення шаблону обрису MegaMatcher і відповідності.

Перевірена надійність NIST IREX. Механізм зіставлення райдужної оболонки MegaMatcher заснований на VeriEye, визнаному NIST одним із найнадійніших доступних алгоритмів розпізнавання райдужної оболонки.

Швидке зіставлення. Швидкість зіставлення райдужної оболонки становить до 200 000 порівнянь за секунду на одному ПК.

Надійне виявлення райдужної оболонки. Райдужка виявляється навіть за наявності перешкод для зображення, візуального шуму та/або різного рівня освітлення. Усуваються відблиски світла, засмічення повік і вій. Також приймаються зображення зі звуженими повіками або очима, які дивляться вбік.

Автоматичне виявлення та корекція чергування забезпечує максимальну якість шаблонів характеристик райдужної оболонки із рухомих зображень райдужної оболонки.

Правильна сегментація райдужної оболонки досягається, навіть якщо ідеальні кола не вдаються, центри внутрішніх і зовнішніх меж райдужної оболонки відрізняються, межі райдужної оболонки точно не є колами і навіть не еліпсами або межі райдужної оболонки здаються ідеальними колами.

Визначення якості зображення райдужної оболонки. Оцінку якості зображення можна використовувати під час реєстрації райдужної оболонки, щоб переконатися, що лише шаблон райдужної оболонки найкращої якості зберігатиметься в базі даних. Кут повороту можна визначити за зображенням райдужної оболонки для прийняття подальших рішень щодо прийняття зображення для реєстрації. Також до зарахування можуть бути відхилені райдужні оболонки, закриті косметичними (декоративними) контактними

лінзами з художніми зображеннями або зміною кольору.

Виявлення живості. Захоплену райдужну оболонку можна проаналізувати, чи є вона «живою» чи підробкою, щоб запобігти порушенню безпеки, якщо розмістити фотографію перед камерою або надіти контактні лінзи з підробленою текстурою райдужної оболонки.

Автоматичне визначення положення діафрагми. Алгоритм здатний розділяти зображення лівої та правої райдужки.

Розпізнавання ходи: розпізнавання автентифікується за допомогою способу ходьби, щоб ідентифікувати його. Кожна людина ходить по-різному, тому те, як людина ставить одну ногу перед іншою, є ефективним способом перевірити свою особу. Наразі це не поширена форма автентифікації, але очікується, що вона стане більш поширеною, оскільки майбутні форми автентифікації стануть більш популярними.

Розпізнавання вен: розпізнавання вен використовує схему кровоносних судин на руці чи пальці людини, щоб ідентифікувати їх. Цей тип біометричної автентифікації використовує інфрачервоне світло для картування вен під шкірою на руках або пальцях. Розпізнавання вен надзвичайно точне, ніж розпізнавання сітківки/райдужки.

Страхування особи: біометрична ідентифікація дає відповіді на питання «щось є в людини та є» та допомагає підтвердити особу. Біометрична автентифікація забезпечує підвищений рівень надійності для кінцевих користувачів. Його складне програмне забезпечення дозволяє постачальникам знати, що людина є тим, ким вони себе видають, через відчутну рису реального світу. Навіть якби кіберзловмисник знав пароль користувача чи відповідь на його таємне запитання, він не міг би скопіювати відбиток пальця чи сканування райдужної оболонки ока.

Простота використання: хоча біометрична автентифікація є скоріше технічною стороною щодо внутрішнього процесу, загалом вона проста та швидка з точки зору користувача. Використовуючи або сканер відбитків пальців для розблокування облікового запису, або розпізнавання обличчя, ви зменшуєте кількість разів, коли вам доведеться входити за допомогою довгого

пароля, який містить кілька спеціальних символів, які ви, швидше за все, збудете. Серед відомих продуктів на базі SSO Є CAME  Apple, який  чудово справляється з біометричною автентифікацією на своїх пристроях як за відбитками пальців, так і за обличчям.

Виявлення шахрайства: біометричні дані майже неможливо відтворити. Їх важко відтворити та вкрасти, і ймовірність того, що ваш відбиток точно збігатиметься з чужим, становить лише 1 із 64 мільярдів. Дуже малоймовірно, що хакер зможе отримати доступ до чогось, що захищено біометричними даними.

Проте такі ризик існують адже можливості і варіації злому розвиваються із розвитком таких технологій  а шахрайство у біометричних даних ускладняєтеся не залишенням цифрового сліду.

Можливість злому: біометрику все ще можна зламати. Компанії та уряди, які збирають і зберігають особисті дані користувачів, знаходяться під постійною загрозою з боку хакерів. Проте, якщо вони стали жертвою витоку даних, біометричні дані незамінні, і організаціям потрібно дбайливо й обережно ставитися до біометричних даних користувачів.

Часткові збіги: більшість поширених методів біометричної автентифікації покладаються на часткову інформацію для автентифікації особи користувача. Наприклад, під час реєстрації вашого відбитка пальця він візьме дані з усього вашого відбитка та перетворить їх у дані. Однак під час майбутньої автентифікації для підтвердження вашої особи знадобляться лише часткові дані відбитків пальців, тому це буде швидше й швидше.

Не вдається розпізнати дійсного користувача: коли ви реєструєтеся для розпізнавання обличчя, ви реєструєте певний кут і вираз свого обличчя. Однак, оскільки система має лише дані з процесу реєстрації, щоразу, коли користувач носить окуляри, макіяж або навіть посміхається, системі розпізнавання обличчя важко розпізнати користувача, що може ускладнити процес входу.

Упередженість: системи розпізнавання обличчя можуть не так точно розпізнавати кольорових або негендерних людей. Багато біометричних систем були навчені в основному за допомогою фотографій білих або білих

чоловіків. Це включає в себе внутрішню упередженість, яка призводить до труднощів у розпізнаванні жінок і кольорових людей. Погане впровадження технології або навмисне неправильне використання може призвести до дискримінації та відчуження. Без перевіреного рішення для перевірки ідентифікаційної інформації крос-демографічна ефективність може бути ненадійною.

Побоювання передати біометричні дані: чи прийнятно для компаній продавати чи надавати свої біометричні дані іншим особам, наприклад правоохоронним органам, імміграційним службам або репресивним іноземним урядам. Ці проблеми щодо конфіденційності змусили багато штатів США прийняти закони про конфіденційність біометричної інформації. Коли біометричні дані перетворюються на дані та зберігаються, особливо в місцях або країнах, де є потужні заходи спостереження, користувач ризикує залишити постійний цифровий запис, який потенційно може бути відстежений зловмисниками.

Дуже важливо, щоб всі біометричні дані надійно зберігалися. Біометричні дані не можна скинути, як пароль. Якщо б вони втратились, то користувач насправді нічого не зможе зробити, оскільки він не зможе змінити райдужну оболонку ока чи відбиток пальця.

Отже, SSO як система усунення запитів на автентифікацію особи за допомогою використання біометричних даних, є чи не найбільш популяризована система у світі, її роль і складність дозволяє використовувати увесь набутий людством досвід у ідентифікації особи за допомогою окремих частин інформації за допомогою біометричних ідентифікаторів, і хоча такі ідентифікатори є однойменні у своїй природі та не повторюються, проте заходи безпеки підсистеми SSO нажаль не опереджають саме розвитку такої системи.

Саме розвиток формування нових варіацій входу у системи нових варіації автентифікації та ідентифікації пришвидшує ризики та загрози втрати інформації чи відомостей про біометричні данні особи і хоча існує багато захищених веб ресурсів, серверів, та хмарних сховищ де зберігаються такі відомості, вони можуть бути опрацьовані, як професійними шахраями у сфері

кібербезпеки та і простими людьми, які просто проводять ідентифікацію за допомогою простого програмного забезпечення, як приклад генератор паролю.

Також існує ряд інших форм проблематики безпеки, одним із найпростіших яких являєтеся саме втрата фізичною особою кореневих ключів авторизації паролю, токену, чи іншого, що безпосередньо створює більший ризик цілій системі загалом, Проте такі ризики є оправданні за рахунок різкого розвитку системи автентифікації

Що дозволяє пришвидшувати взаємодію різних інстанцій суспільного життя, взаємодію органів державної влади та органів місцевого самоврядування, пришвидшує роботу державних реєстрів та здійснює прогрес у сфері інформаційних технологій та розвиток економічних процесів на рівні держави, Вдосконалення цієї системи є необхідним для спрощення користування продуктом та налагодження реалізації проектів електронного урядування, та спрощення автентифікації, що в подальшому дозволить аналізувати недоліки системи та забезпечити більш ефективне використання біометричних даних використовуючи підсистему SSO.

# РОЗДІЛ 3. ВІЗУАЛІЗАЦІЯ ОБЄКТІВ БІОМЕТРИЧНИХ ДАНИХ ТА МЕДОТИ ВИКОРИСТАННЯ ПРАВООХОРОНИМИ ОРГАНАМИ ТАКИХ ДАНИХ

## 3.1. Візуалізація об’єктів біометричних даних

При розслідуванні кримінальних правопорушень органи досудового розслідування аналізують сліди, залишені на місці події та обладнанні, на тілі і одязі потерпілих та злочинців. Це вимагає залучення експертів та спеціалістів, а також використання інформації з баз біометричних даних, зокрема з інформаційно-пошукових систем Експертної служби МВС України. Отже, важливо визначити поняття, види та роль таких баз у діяльності органів досудового розслідування.

Безпосередньо так відповідно до встановлених норм прецесії та процесуального кодексу являєтеся факт використання в криміналістиці окремих процесуальних та інших дій пов’язаних із опрацюванням біометричних данних та інформації людини-злочинця. Без належної організації та планування діяльності органів досудового розслідування неможливо отримати повну доказову базу та встановити всі обставини, які підлягають доказуванню в кримінальному провадженні. Для цього потрібно забезпечити суб'єктів розслідування необхідними ресурсами, інформацією про криміналістично важливі ознаки та оперативний інтерес. [10 ст. 98–101]. Слідчо-пошукові дії як і розслідування кримінального правопорушення в цілому не можливе без визначення певної ролі об’єкту, суб’єкту та іншого.

Насамперед варто відмітити, що в криміналістичній науці можна зустріти вживання різної термінології для позначення інформаційно- довідкового забезпечення досудового розслідування. Зокрема, використовуються терміни «кримінальна реєстрація», «криміналістична реєстрація», «інформаційне забезпечення», «інформаційно-аналітичне забезпечення» тощо. Враховуючи вище наведене можна говорити про те що основним об’єктом та увага зосереджується на ролі криміналістичного, значущого факту подібності

перспективності та використання біометричних даних в процесі кримінального правопорушення та використання, як працівниками правоохоронних органів так і працівниками науково дослідницьких центрів експертиз значущою інформацією, щодо можливості ідентифікації за біометричними даними.

Тому проведення інших слідчо-оперативних дій та експертизи не можливо проводити без врахування окремих біометричних улаштувань людини, що в свою чергу тягне за собою зниження показників розкриття.

Саме тому визначення біопроцесій - ідентифікації особи за окремими характерезуючими згідно біоматеріалів процесій є необхідною процедурою слідства.

### 3.2. Алгоритм роботи та цілі розробки фреймворку SSO.

У наш час вивчення розпізнавання відбитків пальців є активною областю досліджень. Важливою складовою системи розпізнавання є правильне застосування алгоритмів. У зв'язку з особливостями цієї галузі, алгоритми розпізнавання відбитків пальців можна розділити на дві категорії:

– алгоритм перевірки;

– алгоритм ідентифікації.

Мету Алгоритму можна розділити на декілька похідних,прикладом можна навести алгоритм відображений на рисунку 3.1.


Рисунок 3.1 - алгоритм

У роботі були використані:

– інструменти, бібліотеки та класи, доступні в .Net Framework, які економлять багато часу для написання коду.

– Одна з найвідоміших мов програмування C+;

Фреймворк реалізований на C + з використанням .Net Framework .

Даний фреймворк дозволяє експериментувати в базах даних типу B від FVC2000, FVC2002 і FVC2004, і в базах даних типу A від FVC2002 і FVC2004. У цих експериментах ми виконуємо індикатори the Fingerprint Verification Competitions (EER (%), FMR100 (%), FMR1000 (%), ZeroFMR (%), Time (ms) і ROC curves). Крім того, ми можемо робити досліди навіть зі звичайним протоколом і різними базами даних.

Ми впровадили алгоритми розпізнавання відбитків пальців, що були запропоновані Tico і Kuosmanen, Jiang і Yau, Medina-Pérez. Варто відмітити, що, навпаки від Qi, який використовує набір шаблонів відбитків пальців, наші алгоритми спрямовані на зіставлення протоколів введення відбитка пальця. Крім того, ми проаналізували і використали алгоритми виділення ознак, запропоновані Ratha, та орієнтувалися на отримання зображень. Цей фреймворк дозволяє нам легко додавати нові алгоритми розпізнавання відбитків і алгоритми виділення ознак без зайвих зусиль і перекомпіляції фреймворка.

Наша робота складається з файлів:

– Вхідний код документації;

– Вихідні файли нашого фреймворка.

– Гіперпосилання для самого розширення з метою його дослідження.

Приклад поточного аналізу за допомогою вихідного коду
проаналізований на рисунку 3.2.

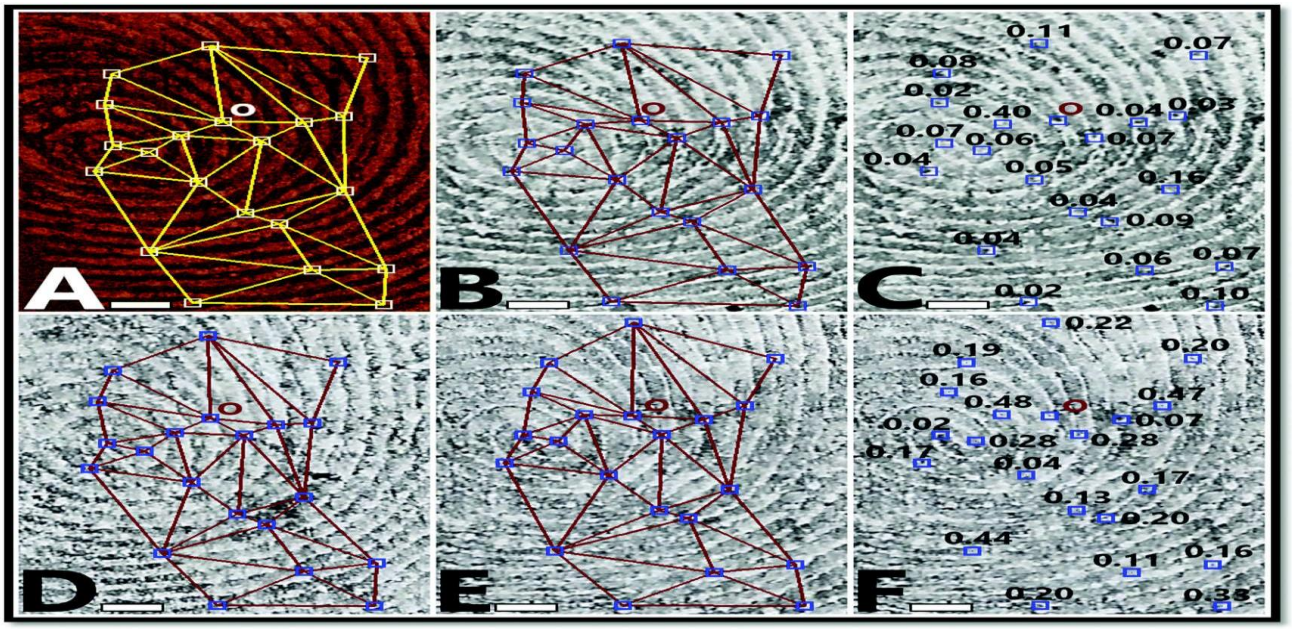


Рисунок 3.2 - аналіз біометрії за допомогою вихідного коду

Отже, створення мультимодальної бази біометричних даних – це важливий момент у розвитку інформаційно-довідкового забезпечення досудового розслідування кримінальних правопорушень. Але так як процес створення такої бази є досить складним, то інтегрований банк даних можна охарактеризувати особливостями, які наведені нижче.

Інтеграція багатьох інформаційних обліків, взаємопов'язаних через центральне ядро даних. Застосування загальної технології обробки інформації. Повномасштабний комплекс засобів забезпечення безпеки і надійності. Накопичення і гарантоване зберігання великих обсягів інформації.

Забезпечення віддаленого доступу користувача та підтримка численних типів даних, зокрема широкого спектру промислових стандартів біометричних даних.

Використання типових форм фреймворку на основі C+, чи за допомогою інших властивостей розкриває саме методологію визначення бінарного коду, котрий створюється для фіксування суб’єкта ідентифікації.

Моделювання та створення окремих регістрів інформації передбачає собою інформаційно-зчитувальну систему, яка допомагає ідентифікувати окремі алгоритми ядр даних та запустити складний процес дешифрування інформації після проведення одноетапної чи двоетапної автентифікації особи.

# 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНА ПРАЦІ

## 4.1. Проведення інструктажів з охорони праці

Для працівників які використовують біометричну автентифікацію в системах керування доступом на основі технології SSO проводять інструктаж з охорони праці,згідно з типовим положенням про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженим наказом Державного комітету України з нагляду за охороною праці 30.01.2017 № 140.

Визначення понять і термінів, наведених у типовому положенні навчання з питань охорони праці - це навчання працівників, учнів, курсантів, студентів, слухачів з метою отримання необхідних знань і навичок з питань охорони праці або безпечного ведення робіт. Робота з підвищеною небезпекою - є робота в умовах впливу шкідливих та небезпечних виробничих чинників або така, де є потреба професійному доборі, чи пов'язана з обслуговуванням, управлінням, застосуванням технічних засобів праці або технологічних процесів, що характеризуються підвищеним ступенем ризику виникнення аварій, пожеж, загрози життю, заподіяння шкоди здоров'ю, майну, довкіллю. Спеціальне навчання - є щорічне вивчення працівниками, які залучаються до виконання робіт з підвищеною небезпекою або там, де є потреба в професійному доборі, вимог відповідних нормативно-правових актів з охорони праці. Стажування - набуття особою практичного досвіду виконання виробничих завдань і обов'язків на робочому місці підприємства після теоретичної підготовки до початку самостійної роботи під безпосереднім керівництвом досвідченого фахівця. Дублювання - самостійне виконання працівником професійних обов'язків на робочому місці під наглядом досвідченого працівника з обов'язковим проходженням протиаварійного і протипожежного тренувань.

Організація проведення інструктажів з питань охорони праці. Працівники, під час прийняття на роботу та періодично, повинні проходити на підприємстві інструктажі з питань охорони праці, надання першої медичної

допомоги потерпілим від нещасних випадків, а також з правил поведінки та дій при виникненні аварійних ситуацій, пожеж і стихійних лих.

Вступний інструктаж проводиться з усіма працівниками, які приймаються на постійну або тимчасову роботу, незалежно від їх освіти, стажу роботи та посади з працівниками інших організацій, які прибули на підприємство і беруть безпосередню участь у виробничому процесі або виконують інші роботи для підприємства з учнями та студентами, які прибули на підприємство для проходження трудового або професійного навчання з екскурсантамиу разі екскурсії на підприємство.

Первинний інструктаж первинний інструктаж проводиться до початку роботи безпосередньо на робочому місці з працівником новоприйнятим на підприємство або до фізичної особи, яка використовує найману працю; який переводиться з одного структурного підрозділу підприємства до іншого;який виконуватиме нову для нього роботу відрядженим працівником іншого підприємства, який бере безпосередню участь у виробничому процесі на підприємстві. Первинний інструктаж на робочому місці проводиться індивідуально або з рупою осіб одного фаху за діючими на підприємстві інструкціями з охорони праці відповідно до виконуваних робіт.

Повторний інструктаж повторний інструктаж на робочому місці індивідуально з окремим працівником або групою працівників, які виконують однотипні роботи, за обсягом і змістом переліку питань первинного інструктажу. Позаплановий інструктаж позаплановий інструктаж проводиться з працівниками на робочому місці або в кабінеті охорони праці.

Позаплановий інструктаж може проводитись індивідуально з окремим працівником або з групою працівників одного фаху. Обсяг і зміст позапланового інструктажу визначаються в кожному окремому випадку залежно від причин і обставин, що спричинили потребу його проведення.

Цільовий інструктаж проводиться з працівниками при ліквідації аварії або стихійного лиха,при проведенні робіт, на які відповідно до законодавства оформлюються наряд-допуск наказ або розпорядження. Інструктаж проводиться індивідуально з окремим працівником або з групою працівників

Первинний, повторний, позаплановий і цільовий інструктажі проводить безпосередній керівник робіт або фізична особа, яка використовує найману працю. Про проведення первинного, повторного, позапланового та цільового інструктажів та їх допуск до роботи, особа, яка проводила інструктаж,уносить запис до журналу реєстрації інструктажів з питань охорони праці на робочому місці. Сторінки журналу реєстрації інструктажів повинні бути пронумеровані, прошнуровані і скріплені печаткою.

Новоприйняті на підприємство працівники після первинного інструктажу на робочому місці до початку самостійної роботи повинні під керівництвом досвідчених, кваліфікованих працівників пройти стажування протягом не менше 2-15 змін або дублювання протягом не менше шести змін. стажування або дублювання проводиться, як правило, під час професійної підготовки на право виконання робіт з підвищеною небезпекою у випадках, передбачених нормативно-правовими актами з охорони праці.

Працівники, функціональні обов'язки яких пов'язані із забезпеченням безаварійної роботи об'єктів підвищеної небезпеки або з виконанням окремих робіт підвищеної небезпеки до початку самостійної роботи повинні проходити дублювання з обов'язковим проходженням у цей період протиаварійних і протипожежних тренувань відповідно до плану ліквідації аварій.Перелік посад і професій працівників, які повинні проходити стажування,а також тривалість стажування визначаються керівником підприємства відповідно до нормативно-правових актів з охорони праці. Тривалість стажування залежить від стажу і характеру роботи, а також відкваліфікації працівника.Роботодавцю надається право своїм наказом звільняти від проходження стажування працівника, який має стаж роботи за відповідною професією не менше 3 років або переводиться з одного підрозділу до іншого, де характер роботи та тип обладнання, на якому він працюватиме, не змінюються.

Стажування проводиться за програмами для конкретної професії, які розробляються на підприємстві відповідно до функціональних обов'язків працівника і затверджуються керівником підприємства чи структурного підрозділу. Стажування проводиться на робочих місцях свого або іншого

подібного за технологією підприємства. У процесі стажування працівники повинні виконувати роботи, які за складністю, характером, вимогами безпеки відповідають роботам, що передбачаються функціональними обов'язкам и цих працівників.

Після закінчення стажування та при задовільних результатах перевірки знань з питань охорони праці наказом роботодавця працівник допускається до самостійної роботи, про що робиться запис у журналі реєстрації інструктажів, у протилежному випадку, якщо працівник не оволодів необхідними виробничими навичками чи отримав незадовільну оцінку з протиаварійних та протипожежних тренувань, то стажування новим наказом може бути продовжено на термін не більше двох змін.

### 4.2 Допомога при теплових і сонячних ударах

Працівники які працюю з використанням біометричної автентифікації в системах керування доступом на основі технології SSO зобов’язанні вміти надавати першу допомогу при тепловому або сонячних ударах. Сонячний удар – це розлад функції головного мозку, викликаний тривалим впливом прямих сонячних променів на непокриту голову людини. Незабаром після несприятливого впливу, розвиваються симптоми сонячного удару, при яких потерпілому слід надати невідкладну допомогу.

Сонячний удар є одним з видів теплового удару його поділяють за трьома ступенями важкості. Легкий проявляється головним болем, нудотою, збільшенням частоти пульсу і дихання, розширенням зіниць, зневодненням шкіри. Середній основні симптоми – різкий занепад сил, м'язова гіпотонія, сильний головний біль, нудота, блювота, сплутаність свідомості t тіла до 39-40. Важкий серед частих ознак – втрата свідомості м'язові спазми, галюцинації, марення, рухове занепокоєння різного ступеню вираженості, зневоднення шкіри, глухі тони серця, t тіла до 42 °С.

Причини та наслідки стану фактори, які впливають на розвиток сонячного удару:

– вік старше 60 років;

– дошкільний вік;

– гестація;

– хронічні та гострі проблеми зі здоров'ям (ІХС, гіпертензія, хвороби ендокринної системи, бронхіальна астма, хронічні та гострі гепатити, психічні захворювання;

– перенесені раніше інсульт або інфаркт;

– алергічні реакції;

– порушення потовиділення;

– ожиріння;

– висока метеочутливість;

– перебування під впливом різних хімічних речовин (алкоголь, наркотики чи інші токсини);

– вживання недостатньої кількості рідини;

– прийом діуретиків;

– сильні фізичні навантаження під відкритим сонцем;

– підвищена вологість навколишнього середовища;

– носіння одягу не по погоді.

Симптоми сонячного удару у дорослих і дітей:

– інтенсивне почервоніння шкірних покривів;

– різкий занепад сил;

– сонливість;

– диспное;

– сплутаність свідомості;

– липкий піт;

– сильний головний біль;

– дискоординація в просторі;

– розширення зіниць;

– підвищена частота пульсу;

– підвищення температури до 40 °С і вище;

– диспепсичні розлади;
– затримка сечовипускання;
– непевна хода;
– проблеми зорового сприйняття
– посиніння епідермісу (при порушенні дихальної функції).

У важких випадках спостерігаються судоми, втрата свідомості, а іноді потерпілий впадає в кому, трапляються епілептичні напади.

Найбільш небезпечним наслідком сонячного удару є порушення дисемінованого внутрішньосудинного згортання, гостра ниркова або печінкова недостатність. Частими ускладненнями сонячного удару, за відсутності адекватної медичної допомоги, є такі проблеми з боку кровоносної та сечовидільної системи.

Перша допомога при сонячному ударі до приїзду швидкої допомоги не потребує спеціальної підготовки. Щоб полегшити стан, слід:

– відвести потерпілого в тінь;
– забезпечити приплив свіжого повітря;
– дати прохолодне пиття;
– прикласти прохолодні компреси на чоло і потилицю;
– при запамороченні потерпілого потрібно розмістити в горизонтальному положенні.

Ні в якому разі не варто використовувати дуже холодну воду і напої для охолодження тіла потерпілого. Холод може призвести до сильного спазму судин і ускладнення стану хворого.

Лікування сонячного удару під контролем медпрацівників потрібне не тільки в разі важких сонячних ударів, оскільки тільки медпрацівники можуть запобігти ймовірності розвитку інфаркту, інсульту та інших патологій, викликаних перегрівом. За симптомами складно точно визначити ступінь тяжкості потерпілого, тому виклик "швидкої" потрібний в будь-якому випадку.

Профілактика сонячного удару полягає в дотриманні наступних правил і рекомендацій:

– обмеження перебування на сонці;

– носіння легкого світлого одягу з натуральних матеріалів і головних уборів у спеку;

– дотримання питного режиму (вживання не менше 2,0 літрів чистої води на добу);

– відмова від важкої їжі на користь легкозасвоюваної (овочі, фрукти, кисломолочні продукти);

– обмежувати перебування на сонці в години найбільшої сонячної активності (з 12 до 16 годин) – в цей час потрібно надягати одяг, що максимально закриває шкіру, головні убори, креми з УФ-фільтрами, парасолі від сонця;

– відмовитися від вживання алкоголю;

– відмовитися від нанесення на обличчя декоративної косметики (закорковування пор косметичними засобами може призвести до перегріву);

– приймати прохолодний душ кілька разів на день (по можливості);

– відмовитися від активних фізичних навантажень в спекотні дні;

# ВИСНОВКИ

Використання технології SSO з використанням біометричних даних дозволяє автоматизувати багато рутинних процесів, спрощує авторизацію у різні підвідомчі системи та , зменшує час на їх авторизацію та ідентифікацію особи, яка намагає увійти в систему  та покращує загальну продуктивність. Користувачі отримують зручний доступ до необхідних інтернет ресурсів реєстрів та інших, що сприяє швидкій та ефективній роботі.

Економічність: технології SSO з використанням біометричних даних дозволяє до значних економічних вигод. Зменшення використання паперу, печаток та інших матеріалів для документів сприяє зниженню витрат на їх друку, зберігання та транспортування, а також допомагає сформувати наладжений механізм роботи  на підприємстві, навіть використовуючи один апарат ідентифікації особи.

Безпека і конфіденційність: технології SSO з використанням біометричних даних дозволяє, як найбільше зберегти персональні дані такого користувача, зберегти підвідомчу йому інформацію, а також дозволяє відстежувати рух авторизації користувачів у підвідомчих системах, а також дозволяє здійснити перевірку осіб що здійснювали запит на таку інформацію за допомогою збереження даних об’єкта ідентифікатора.

Що до безпеки то слід заначити, що із стрімки розвитком інформаційних технологій також і зростає варіація можливостей злому таких систем, а також у варіації пришвидшення створення нових алгоритмів за допомогою простого коду авторизації користувача  залишається відкрите питання створення додаткових систем захисту,  на даний факт вливає виключно людський чинник та фактор проте неодноразово було доведено, що провідні компанії при створенні системи авторизації на основі технології SSO з використанням біометричних даних не рідко працюють першочергово над випущенням самого продукту, а вже пізніше над окремим модулем шифрування інформації, чи системними оновлення безпеки даних, що в свою черго при реалізації продукту дозволяє зловмисникам швидко отримати доступ до персоналізованих баз даних

та до конфеденційної інформації.

Законознавство: У більшості країн світу використання технології SSO з використанням біометричних даних є першочерговою засадою з питань пришвидшення та автоматизації роботи працівників підприємств установ та закладів.

Міжнародна інтеграція: Впровадження систем  на основі технології SSO з використанням біометричних даних дозволяє покращити та пришвидчити співпрацю між різними організаціями та установами, включаючи міжнародний рівень. Це може бути особливо важливим для організацій, які мають багато філіальну структуру або здійснюють міжнародну діяльність.

Покращення взаємодії з громадськістю: Впровадження технології на базі SSO з використанням біометричних даних дозволяє покращити взаємодію державних органів, установ та підприємств з громадськістю. За допомогою цих систем можна швидко і зручно надсилати, отримувати та обробляти запити, звернення та скарги громадян, забезпечуючи більш прозору та відкриту комунікацію.

Масштабованість: технології SSO з використанням біометричних даних потенціал  можливо і передбачувані для масштабування та розширення в майбутньому. За рахунок розвитку технологій та зростання потреб організацій можливо впровадження нових функцій та можливостей, що дозволить ще більше поліпшити процеси обробки документів та комунікації, проте в проблеми захисту таких систем являєтеся фактором що гальмує такий процес.

Технологічний розвиток: З огляду на швидкий технологічний розвиток і постійне вдосконалення систем, можна очікувати появу нових функцій, інструментів та можливостей. Це відкриває шлях до подальшого вдосконалення процесів обробки документів та поліпшення комунікації між організаціями та пришвидшенні авторизації користувача.

Слід зазначити що використання  таких систем дозволяє організаціям відповідати законодавчим вимогам та забезпечувати безпеку та захист інформації. Сертифіковані провайдери електронного цифрового підпису гарантують відповідність системи законодавчій та нормативній базі.

Україномовна локалізація та можливість отримання технічної підтримки державною мовою також стають важливими факторами для українських державних структур.

Тож розвиток технології SSO з використанням біометричних даних має стати чи не першочерговим об’єктом дослідження та подальшого вдосконалення, як на технічному рівні так і на законодавчому, адже такі технології відіграють один із найважливіших аспектів у суспільно-корисному житті, та допомагає як пришвидшувати роботу так і автоматизувати її.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 16 січня 2014 р. № 30. URL: https://zakon.rada.gov.ua /laws/show/3475-15 (дата звернення: 15.05.2021).

2. Про основні засади забезпечення кібербезпеки України : Закон України від 21 червня 2018 р. № 2469-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 15.05.2021).

3. Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України": Указ Президента України від 27 січня 2016 р. URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html. (дата звернення: 15.05.2021).

4. Команда CERT-UA Держспецзв'язку з 18 по 24 квітня зареєструвала 2882 кіберінциденти : Офіційний сайт ДССЗЗІ. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=320629&cat_id=3 17163 (дата звернення: 15.05.2021).

5. Applying Cyber Kill Chain® Methodology to Network Defense : GAINING THE ADVANTAGE Lockheed Martin. URL: https://www. lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the

6. _Advantage_Cyber_Kill_Chain.pdf.Про управління інформаційною безпекою : Закон Сполучених Штатів Америки. Від 17 грудня 2002 р. Режим доступу до ресурсу: https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-07publ347.pdf(дата звернення: 15.05.2021).

7. Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу : Директива Європейського Парламенту і Ради (ЄС) 2016/1148. URL: https://zakon.rada.gov.ua/laws/show/984_013-16 (дата звернення: 15.05.2021).

8. Про затвердження Порядку доступу до мережі Інтернет : Аналіз регуляторного впливу проекту постанови Кабінету Міністрів України від 01січня 2019 р. URL: http://195.78.68.84/dsszzi/control/uk/publish/article?showHid den =1&art_id=299628&cat_id=38837 (дата звернення: 15.05.2021)

9. Носенко К. М., Півторак О. І., Ліхоузова Т. А. Огляд систем

виявлення атак в мережевому трафіку : Міжвідомчий науково-технічний збірник “Адаптивні системи автоматичного управління”, 2014. 67–75с.

10. K. K. Security Management Process in Distributed, Large Scale High Performance Systems : Online Journal on Power and Energy Engineering.2015. – URL : https://www.researchgate.net/publication/268356955_Security_Management_Process_in_Distributed_Large_Scale_High_Performance_Systems.

11. Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України" : УКАЗ ПРЕЗИДЕНТА УКРАЇНИ від 27 січня 2016 р. URL: https://zakon.rada.gov.ua/laws/show/96/2016.

12. Конвенція про кіберзлочинність : веб-сайт Верховної Ради України : від 07 вересня 2005р. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 15.05.2021).

13. Оперативна інформація Держспецзв’язку щодо захисту державних інформаційних ресурсів : від 16 червня 2020 URL: http://www.dsszzi.gov.ua/ dsszzi/control/uk/publish/article;jsessionid=07515BBA5DC8FCDE53AF420BD4C 0 5FB8.app1?art_id=321621&cat_id=317163 (дата звернення: 15.05.2021).

14. Про електронні довірчі послуги : Закон України № 440-IX від 14 січня 2020р. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 15.05.2021).

15. Закон України Про електронні документи та електронний документообіг (Відомості Верховної Ради України (ВВР), 2003, https://zakon.rada.gov.ua/laws/show/851-15#Text.

16. Чирський Ю.В. Запровадження системи електронного документообігу в Україні. Режим доступу: http://old.minjust.gov.ua/7546.

17. Що таке електронне урядування? (поширення практик електронного урядування в бібліотеках) : методичні поради / Ярмолинецька ЦРБ, уклад. Слободян О.Л. – Ярмолинці, 2014. – 16 с. Режим доступу:

http://biblioyar.at.ua/Metod_modul/Metod_vudannya/2014/shho_take_eurjaduvannja.pdf

18. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 9: Електронний документообіг. Реінжиніринг адміністративних процесів в органах публічної влади / [С.П. Кандзюба, Р.М. Матвійчук, Я.М. Сидорович, П.М. Мусієнко]. – К.: ФОП Москаленко О. М., 2017. – 64 с. Режим доступу: https://onat.edu.ua/wp-content/uploads/2018/05/Part_009_Feb_2018.pdf.

19. Постанова Кабінету Міністрів України від 17 січня 2018 р. № 55 «Деякі питання документування управлінської діяльності». Режим доступу: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF.

20. Закону України «Про електроні довірчі послуги» Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text