МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна

Кафедра «Електронні обчислювальні машини»

«ДО ЗАХИСТУ»

Завідувач кафедри
_____ Жуковицький І. В.
(підпис) (ПІБ)
«____» _____ 20____р.

ДИПЛОМНА РОБОТА

на здобуття освітнього ступеня «магістр»

Галузь знань 12 Інформаційні технології

Спеціальність 125 Кібербезпека
(код) (повна назва)

Тема «Дослідження та розробка засобів демонстрації біометричної аутентифікації за клавіатурним почерком»

Theme « Research and development of tools for demonstrating biometric authentication by keyboard handwriting »

Керівник дипломного проекту	_____	_____	Остапець Д. О.
	(посада)	(підпис)	(ПІБ)
Консультант розділу з БЖД	_____	_____	Музикін М. І.
	(посада)	(підпис)	(ПІБ)
Нормоконтролер	_____	_____	Шаповалов В. О
	(посада)	(підпис)	(ПІБ)
Студент групи	_____	_____	Мусієнко М. І.
	(група)	(підпис)	(ПІБ)
Student		Musiienko Maksym	
		(family name)	

Дніпро
2020

Дніпровський національний університет залізничного транспорту імені академіка В.Лазаряна

Факультет Комп'ютерні технології і системи **кафедра** ЕОМ

Спеціальність Кібербезпека

ЗАТВЕРДЖУЮ:
зав. кафедри

_____
'_____'_____**20__ р.**

ЗАВДАННЯ
до дипломної магістерської роботи студента групи КБ1921 (966–М) Мусієнка Максима Ігоровича

1. Тема проекту (роботи) Дослідження та розробка засобів демонстрації біометричної аутентифікації за клавіатурним почерком

Затверджена наказом по університету № 945 / ст. від '16' грудня 2019 р.

2. Термін подання студентом закінченої роботи – 14 грудня 2020р.

3. Вихідні дані до проекту (роботи)

3.1. Методи та засоби біометричної аутентифікації.

3.2. Характеристики алгоритмів поведінкових біометричних систем.

4. Зміст розрахунково-пояснювальної записки (роботи)

4.1. Огляд та аналіз існуючих методів та засобів біометричної аутентифікації.

4.2. Аналіз відомих алгоритмів порівняння клавіатурного почерку.

4.3. Архітектура, інформаційна та функціональна структури комплексу.

4.4. Розробка програмного забезпечення комплексу.

4.5. Методика використання комплексу.

4.6. Охорона праці та безпека в надзвичайних ситуаціях.

5. Перелік креслень (з переліком обов'язкових креслень)

5.1. Характеристика відомих методів та засобів біометрії – 1-2

5.2. Порівняльна характеристика існуючих поведінкових методик – 1

5.3. Алгоритми порівняння клавіатурного почерку – 1

5.4. Організація розроблюваного комплексу – 1-2

5.5. Схеми основних алгоритмів програми – 1-2

5.6. Екранні форми програми – 1-2

5.7. Методика використання розробленого комплексу в учбовому процесі – 1

6. Консультанти (з назвами розділів)

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Розділ ОП та БНС			

7. Дата видачі завдання - « » 20 р. .

Керівник проекту _____(доц. Остапець Д.О.)
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва розділів дипломного проекту (роботи)	Термін виконання розділів проекту (роботи)	Примітки
1	Огляд та аналіз існуючих методів та засобів біометричної аутентифікації		15%
2	Аналіз відомих алгоритмів порівняння клавіатурного почерку		15%
3	Архітектура, інформаційна та функціональна структури комплексу		20%
4	Розробка програмного забезпечення комплексу		40%
5	Методика використання комплексу		5%
6	Розділ ОП та БНС		5%

Студент-дипломник_____

Керівник проекту_____(доц. Остапець Д.О.)

РЕФЕРАТ

Дипломна робота на тему: «Дослідження та розробка засобів демонстрації біометричної аутентифікації за клавіатурним почерком» складається зі вступу, 1 розділ – «Огляд та аналіз існуючих методів та засобів біометричної аутентифікації», де розглядаєм та аналізуємо існуючі методи та засоби біометричної аутентифікації; 2 розділ – «Аналіз відомих алгоритмів порівняння клавіатурного почерку» аналізуємо усі відомі для нас алгоритми порівняння клавіатурного почерку; 3 розділ – «Архітектура, інформаційна та функціональна структури комплексу» в якому розглядається архітектура, інформаційна та функціональні структури; 4 розділ - «Розробка програмного забезпечення комплексу» розробляється програмне забезпечення; 5 розділ - «Методика використання комплексу» складання плану використання в учбових цілях. Дипломна магістерська робота складається з двадцяти рисунків, шістнадцяти посилань. Загальний обсяг сторінок – 60 сторінок.

Об’єкт дослідження – біометрична аутентифікація за клавіатурним почерком.

Мета кваліфікаційної роботи - Дослідження та розробка засобів демонстрації біометричної аутентифікації за клавіатурним почерком.

Галузь застосування - широке застосування технологій для перевірки особистості нового покоління стало можливим завдяки розповсюдженню смартфонів з високою якістю мікрофонів і камер, які допомогли зробити цей процес більш простим. Завдяки досягненням у технології, біометрична аутентифікація може бути в лічені хвилини здійснена в будь-який момент, в будь-якому місці.

Ключові слова: АУТЕНТИФІКАЦІЯ, БІОМЕТРИКА, КЛАВІАТУРНИЙ ПОЧЕРК, PYTHON, ПРОГРАМА

ABSTRACT

Thesis on the topic: "Research and development of tools for demonstration of biometric authentication by keyboard handwriting" consists of an introduction, section 1 - "Review and analysis of existing methods and tools of biometric authentication", where we consider and analyze existing methods and tools biometric authentication; Section 2 - "Analysis of known algorithms for comparing keyboard handwriting" we analyze all known algorithms for comparing keyboard handwriting; Section 3 - "Architecture, information and functional structures of the complex" which examines the architecture, information and functional structures; Section 4 - "Software development of the complex" software is developed; Section 5 - "Methods of using the complex " drawing up a plan for use for educational purposes. The master's thesis consists of twenty drawings, sixteen references. The total volume of pages is 60 pages.

The object of research is biometric authentication according to the keyboard.

The purpose of the qualification work - Research and development of tools for demonstration of biometric authentication by keyboard handwriting.

Scope - The widespread use of next-generation identity verification technologies has been made possible by the proliferation of high-quality smartphones with high-quality microphones and cameras that have helped make the process easier. Thanks to advances in technology, biometric authentication can be performed in minutes at anytime, anywhere.

Keywords: AUTHENTICATION, BIOMETRICS, KEYBOARD, PYTHON, PROGRAM

ЗМІСТ

1 ОГЛЯД ТА АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА ЗАСОБІВ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ

1.1 Фактори аутентифікації

Щоб довести свою справжність, користувач повинен пред'явити один або кілька факторів аутентифікації, які можуть бути наступними:

- фактор знання передбачає наявність певної відомої тільки користувачу інформації;

- фактор володіння має на увазі, що користувач володіє деяким унікальним предметом, що містить необхідну характеристику (пластикові карти, USB-токени і т. д.);

- фактор властивості передбачає використання деякої фізичної особливості користувача, наприклад, відбиток пальця, райдужна оболонка ока і т. д.

Нижче будуть розглянуті різні способи реалізації цих факторів.

1.2 Багаторазовий пароль

Аутентифікація по багаторазовим паролів зазвичай передбачає наявність у користувача унікального ідентифікатора (логін) і, власне, пароля, який той може підбирати і змінювати самостійно. Пара «логін-пароль» зберігається в базі даних. Загальний алгоритм аутентифікації:

1. Користувач робить запит на доступ до системи, вводить ідентифікатор і пароль.

2. Введені унікальні дані надходять на сервер і порівнюються з еталонними.

3. Якщо дані збігаються з еталоном, аутентифікація вважається успішною, якщо немає - користувач переміщається до першого кроку [1].

Такий метод зараз залишається найпоширенішим методом аутентифікації завдяки найбільшою простоті у виконанні. Крім того, що запам'ятовується секретна фраза дуже зручна для користувачів, що знаходяться в постійному пе-

реміщенні і, таким чином, що підключаються з різних віддалених місць [2]. В іншому така аутентифікація має недоліки:

- практика показує, що користувачі зазвичай вибирають досить прості паролі, які можуть бути легко підібрані методом «грубої сили» (Наприклад, «qwerty», «1234»), або використовують ідентифікатор (ім'я) користувача, або ж пароль є словом з будь-якої мови [3];

- пароль легко забувається або втрачається. Крім того, зловмисник може швидко отримати його шляхом шахрайства (наприклад, фішинг) або шляхом застосування насильства до власника [3];

- пароль можна підглянути або перехопити при введенні;

- внаслідок величезної популярності і простоти парольної аутентифікації для цього методу існує найбільша кількість різних методик і утиліт, що дозволяють отримати його [4].

Багаторазові паролі нерідко використовується в якості другого фактора аутентифікації. Найбільш поширеним прикладом є PIN-код, розглянутий в [5].

1.3 Одноразовий пароль

Аутентифікація з використанням одноразових паролів [6] (або скорочено OTP - від англ. One Time Password) передбачає необхідність нового пароля для кожного входу в систему. Захищеність такого методу залежить від конкретної реалізації, однак головна перевага перед багаторазовими паролями незмінно - отримавши доступ до сесії аутентифікації і перехопивши одноразовий пароль, зловмисник не зможе використовувати його повторно, тому OTP забезпечує більш високу ступінь захисту.

Існують різні реалізації одноразових паролів:

- математичні алгоритми;

- тимчасова синхронізація;

- система запитів;

- використання SMS.

Перший підхід використовує однобічну функцію. Система одноразових паролів починає роботу від якогось початкового числа, після чого генерує паролі необхідну кількість разів.

Зловмисник, який отримав такий пароль, не зможе використовувати його по закінченню невеликого періоду часу або одного з'єднання. А щоб отримати наступний пароль в ланцюжку з попередніх, необхідно обчислити зворотну функцію.

Другий підхід, як правило, пов'язаний з апаратними токенами, що містять точні годинники, синхронізовані з годинником на сервері. В якості вихідної рядки виступають поточні показання цих годин. Зазвичай використовується не точна вказівка часу, а поточний інтервал до встановлених заздалегідь межами. Ці дані зашифровуються за допомогою секретного ключа і в відкритому вигляді відправляються на сервер разом з ім'ям користувача. Сервер при отриманні запиту на аутентифікацію виконує ті ж самі дії: отримує поточний час від свого таймера і зашифровує його. Після цього йому залишається тільки порівняти два значення: обчислене і отримане від віддаленого комп'ютера. Такий підхід використовується, наприклад, в токенах брелоках RSA SecurID [7].

Система запитів вимагає від користувача відправляти синхронізовані за часом запити, наприклад, шляхом введення значення в програмний токен. При цьому поява дублікатів неможливо, оскільки зазвичай використовується додатковий лічильник (таким чином, при відправці двох однакових запитів будуть згенеровані різні OTP).

Для доставки одноразових паролів часто використовуються SMS-повідомлення (див. Рисунок 1.1). Оскільки технологія SMS використовується у всіх мобільних телефонах і, отже, має низьку собівартість, то такий підхід дуже зручний для користувачів. Проте, SMS мають слабку ступінь захищеності, оскільки в ланцюг довіри включаються мобільні оператори, і існує небезпека перехоплення і перенаправлення повідомлень.

Рисунок 1.1 - Схема використання SMS-повідомлень

Незважаючи на те, що OTP дозволяють забезпечити набагато більш високу ступінь захищеності, ніж багаторазові паролі, у них є свої слабкі сторони:

- вразливість для атак типу «людина посередині», при якій підмінюється сервер аутентифікації, і користувач буде відправляти дані зловмисникові.

- для синхронних методів існує ризик розсинхронизації інформації на сервері і в програмному або апаратному забезпеченні користувача, коли дані про показання внутрішніх таймерів перестають збігатися.

- одноразові паролі також вразливі і для «фішингу», тобто отримання доступу до паролю шляхом шахрайства. Однак в силу короткого часу дії пароля ймовірність успіху для OTP набагато нижче, ніж для багаторазових паролів.

1.4 Токени

Токени представляють собою компактні пристрої, які користувач може носити з собою. Вони використовуються в більшості існуючих реалізацій OTP, що дозволяє віднести цей метод до двофакторної аутентифікації [8].

Існуючі токени можна розділити на три типи: токени без підключення, токени з підключенням (див. рисунок 1.2) і бездротові токени.

Рисунок 1.2 - Токен-брелок RSA SecurID

Токени без підключення ніяк не з’єднуються з комп'ютером користувача, натомість вони мають вбудований екран для відображення згенерованого одноразового пароля, який користувач вже вводить вручну.

Саме такий тип токенів використовується найчастіше в двофакторної аутентифікації.

Токени з підключенням не вимагають від користувача власноручного введення інформації, оскільки їм необхідний фізичний контакт з комп'ютером. Як правило, для реалізації таких токенів використовуються технології смарт-карт і USB.

Бездротові токени є свого роду гібридом двох попередніх типів, оскільки одночасно не вимагають фізичного підключення, але при цьому утворюють логічний зв'язок з комп'ютером клієнта.

В якості токена також може використовуватися мобільний телефон, що істотно знижує витрати і забезпечує серйозну зручність для користувачів.

Основною вразливістю всіх розглянутих токенів є можливість крадіжки або втрати предмета. Слід зазначити, що у разі використання двофакторної аутентифікації зловмисник, який отримав токен, що не зможе ним скористатися (оскільки в таких випадках необхідно також вводити PIN-код), що підвищує ступінь захищеності системи.

1.5 Біометрія

Фактор властивості (або біометричний фактор) передбачає систему розпізнавання людей по одній або більше фізичних або поведінкових рис. Біометричні методи дуже зручні для користувачів, оскільки такий ідентифікатор неможливо вкрасти або передати третій особі (але є незначна ймовірність його втрати або пошкодження).

Будь-яка біометрична система оцінюється за двома параметрами [9]:

- FAR (англ. False Acceptance Rate - коефіцієнт помилкового пропуску) - частота виникнення ситуацій, коли система дозволяє допуск незареєстрованому в системі користувачеві;

- FRR (англ. False Rejection Rate - коефіцієнт помилкового відмови) - частота відмови в доступі справжньому користувачеві системи.

Обидві характеристики отримують шляхом розрахунків на основі математичної статистики. Як правило, спроба знизити одну з характеристик веде до підвищення інший. Отже, необхідно знаходити баланс між ними для досягнення кращої захищеності.

Методи біометричної ідентифікації можна розділити на дві групи: статичні, тобто засновані на незмінних протягом життя рисах людини, і динамічні, засновані на змінюваних поведінкових характеристиках [10].

До статичних біометричних атрибутів відносяться:

- відбитки пальців;
- геометрія руки;
- геометрія лиця;
- термічний образ лиця;
- сітківка ока;
- райдужна оболонка ока;
- малюнок вен.

Динамічні атрибути включають:

- голос;
- рукописний почерк;

- клавіатурний почерк.

Статичність або динамічність атрибутів є одночасно як перевагою, так і недоліком. При крадіжці даних в системах, що використовують статичні атрибути, користувач не зможе змінити їх (на відміну, наприклад, від багаторазового пароля) і буде постійно перебувати під загрозою зламу. Динамічні ж атрибути можуть змінюватися мимоволі протягом життя, а отже, потребують оновлення.

Далі перераховані біометричні методи будуть розглянуті окремо.

1.5.1 Розпізнавання відбитків пальців

Розпізнавання відбитків пальців (або дактилоскопія) засновано на неповторності малюнка шкіри на пальцях (а також долонях) рук, який називається папілярним візерунком.

Існують різні типи сканерів для розпізнання відбитків:

- оптичні;
- теплові;
- ємнісні;
- радіочастотні;
- сканери тиску;
- ультразвукові [11].

Оптичні сканери мають різні реалізації оптичного методу розпізнавання.

1. FTIR-сканери (див. рисунок 1.3) використовують ефект порушеного повного внутрішнього відбиття (англ. Frusted Total Internal Reflection, FTIR). Ефект полягає в тому, що при падінні світла на кордон розділу двох середовищ світлова енергія ділиться на дві частини - одна відбивається від межі, інша проникає через межу в інше середовище. Частка відображеної енергії залежить від кута падіння світлового потоку. Починаючи з деякої величини даного кута, вся світлова енергія відбивається від межі розділу (що називається повним внутрішнім віддзеркаленням). У разі контакту більш щільним оптичним середовищем (поверхні пальця) з менш щільним в точці повного внутрішнього відображення пучок світла проходить через цю межу. Таким чином, від межі відіб'ються лише

пучки світла, що потрапили в певні точки повного внутрішнього відображення, до яких не була прикладена папілярний візерунок пальця.

Для захоплення отриманої світловий картинки поверхні пальця використовується спеціальний датчик зображення.

Рисунок 1.3 - FTIR-сканер для відбитків пальців

2. Оптоволоконні сканери (див. рисунок 1.4) являють собою матрицю, в якій всі хвилеводи на виході з'єднані з фотодатчиками. Чутливість кожного датчика дозволяє фіксувати залишковий світло, що проходить через палець, в точці дотику пальця з поверхнею матриці. Зображення всього відбитка формується за даними, зчитує з кожного фотодатчика. Даний метод має більш високу надійність і стійкістю обману, ніж попередній, але досить складний в реалізації.

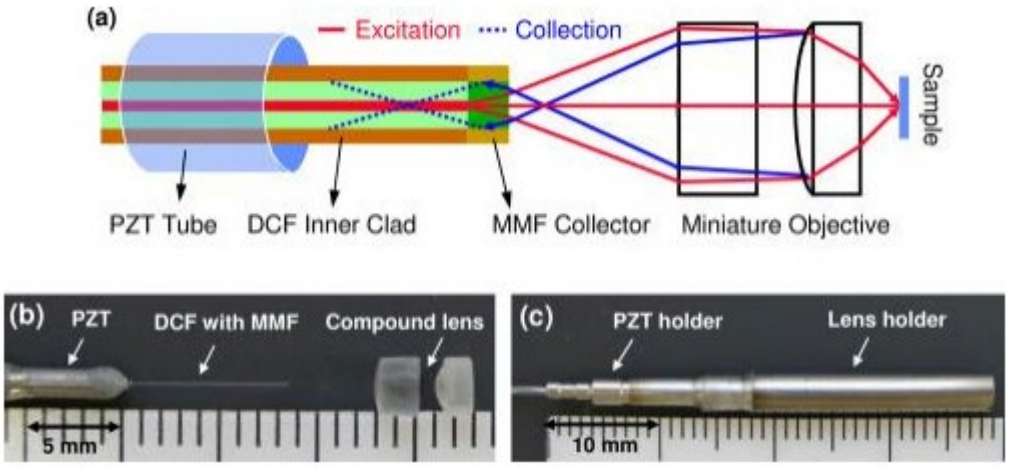

Рисунок 1.4 - Схема оптоволоконного сканера

В цілому, розпізнавання відбитків пальців на даний момент є найбільш поширеним біометричним методом аутентифікації. Дактилоскопія досить зручна у використанні, доступна багатьом користувачам (наприклад, в смартфонах моделі iPhone, Huawei і т. Д.) Підвищує стандартний рівень безпеки. Однак серед інших біометричних методів дактилоскопія програє в надійності, оскільки схильна до фальсифікації. Крім того, папілярний візерунок досить вразливий до пошкоджень, наприклад, дрібними подряпин і порізів.

1.5.2 Геометрія руки

Цей метод використовує форму кисті руки, зокрема, такі параметри,

як вигини пальців, їх довжину і ширину, аналогічні параметри (а також висоту) тильної сторони руки, відстань між суглобами і структура кістки (див. рисунок 1.5). Також геометрія руки включає в себе дрібні деталі

(Наприклад, зморшки на шкірі). За допомогою сканера, який складається з камери і підсвічувати діодів (при скануванні кисті руки, діоди включаються по черзі, це дозволяє отримати різні проекції руки), потім

будується тривимірний образ пензля руки. Надійність аутентифікації по геометрії руки порівнянна з аутентифікацією за відбитком пальця.

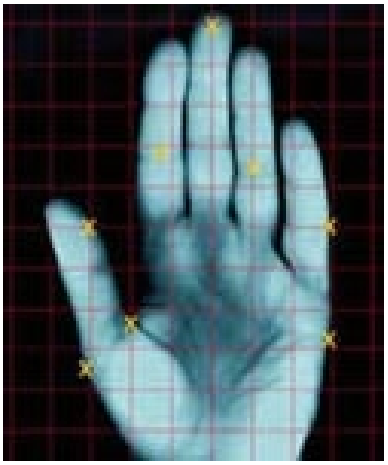

Рисунок 1.5 - Геометрична схема руки

1.5.3 Геометрія особи

Даний метод має два напрямки - двомірне і тривимірне розпізнавання особи [12].

Двомірне (або 2D-) розпізнавання на даний момент вважається найменш надійним біометричних методом, оскільки дуже чутливий до умов освітлення. При нерівномірному освітленні особи достовірність 2D-розпізнавання помітно знижується. Крім того, серйозний вплив надають додаткові елементи, такі як борода, вуса, окуляри і т. п. Однак даний метод не вимагає дорогого устаткування і дозволяє розпізнавати користувача навіть на дуже великій відстані від камери. Це дозволяє поєднувати його з іншими методами аутентифікації, наприклад з парольним.

3D-розпізнавання - вже набагато більш надійний метод, що представляє собою складну математичну задачу. Вона має на увазі побудова тривимірної моделі особи шляхом виділення контурів очей, брів, губ, носа, скул і інших лицьових складових. Після цього обчислюється відстань між цими елементами, і на основі цього будується тривимірна модель осіб.

Щоб знайти унікальний шаблон, відповідний певній людині, потрібно від 12 до 40 характерних елементів. Шаблон повинен враховувати безліч варіацій зображення на випадки повороту голови, нахилу, зміни освітленості, зміни виразу. Діапазон таких варіантів варіюється в залежності від цілей застосування даного способу (для ідентифікації, аутентифікації, віддаленого пошуку на досить великих територіях і т. д.) [10].

В цілому, 3D-розпізнавання особи має наступні переваги:

- відсутність необхідності контактувати зі скануючим пристроєм;

- низька чутливість до зовнішніх факторів, як на самій людині (поява окулярів, бороди, зміна зачіски), так і в його оточенні (освітленість, поворот голови);

- гарний рівень надійності (FRR і FAR), який можна порівняти з таким у дактилоскопії.

Основним недоліком 3D-розпізнавання, особливо в порівнянні з двомірним, є висока вартість обладнання та високий рівень технічної складності.

1.5.4 Термограма особи

Метод заснований на створенні температурної карти (або термограми) шляхом сканування особи в інфрачервоному світлі. Дослідженнями доведено, що термограма особи є унікальною біометричної характеристикою, на точність якої не впливають пластичні операції, старіння організму, зміна температури тіла. Крім того, даний метод, на відміну від геометричного, здатний розрізняти близнят.

Проте, на даний момент метод не має широкого поширення, оскільки не дає потрібної якості аутентифікації.

1.5.5 Сітківка ока

Сканер, який використовує цей метод (див. Рисунок 1.6), зчитує малюнок капілярів на поверхні сітківки ока. Сітківка має нерухому структуру, незмінну в часі. Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, спрямованого через зіницю до кровоносних судин на задній стінці ока. З отриманого сигналу виділяється кілька сотень особливих точок, інформація про які зберігається в шаблоні.

До переваг цього методу аутентифікації можна віднести найвищу надійність (FAR і FRR прагнуть до нуля) серед існуючих біометричних систем і безконтактний спосіб зняття даних. Однак такі системи мають високу вартість, малу доступність і відсутність широкого ринку поширення, тому й низьку інтенсивність розвитку. До того ж, подібні системи вимагають чіткого зображення і, як правило, чутливі до неправильної орієнтації сітківки. Тому потрібно дивитися дуже акуратно, а наявність деяких захворювань (наприклад, катаракти) може перешкоджати використанню даного методу.

Рисунок 1.6 - Сканер сітківки ока

1.5.6 Райдужна оболонка ока

В даному методі використовується унікальність ознак і особливостей райдужної оболонки ока. Райдужна оболонка утворюється ще до народження людини, і не змінюється протягом усього життя. За текстурою вона нагадує мережу з великою кількістю оточуючих кіл і малюнків, які можуть бути виміряні комп'ютером, і оскільки малюнок райдужної оболонки дуже складний, це дозволяє відібрати близько 200 точок. Крім того, райдужна оболонка, на відміну, наприклад, від відбитків пальців, захищена від пошкоджень рогівкою.

Таким чином, системи, що ідентифікують райдужну оболонку (див. рисунок 1.7), мають дуже високою надійністю (поступається тільки ідентифікації по сітківці ока), а також, як і розпізнавачі особи, можуть працювати на пристойній відстані (до декількох метрів). Крім того, незважаючи на те, що фальсифікація для даного методу можлива, є безліч способів протидії.

З недоліків методу можна відзначити відносно високу вартість обладнання, в порівнянні з дактилоскопічний методом і розпізнаванням обличя.

Малюнок 1.7 - Сканер райдужної оболонки ока

1.5.7 Рисунок вен

Малюнок вен є візерунок мережі видимих кровоносних судин руки. Камера отримує відображення сітки судин за допомогою інфрачервоного світла, відбитого гемоглобіном в крові. Спеціальна програма на основі отриманих даних створює цифрову згортку. Розпізнавання не вимагає контакту людини з скануючим пристроєм (див. рисунок 1.8).

Відповідно до статистики, даний метод має дуже високу надійність, порівнянну з такою у ідентифікації по райдужної оболонки, проте малюнок вен піддається зміни внаслідок захворювань, наприклад, артриту, що погіршує показники FAR і FRR. Крім того, перешкоджають новизна і мала ступінь вивченості методу, а отже, його низька поширеність. Проте, даний метод залишається одним з найбільш перспективних для одноразової аутентифікації.

Рисунок 1.8 - Сканер малюнка вен

1.5.8 Голос

Цей метод використовує різні комбінації частотних і статистичних характеристик голосу. Залежно від реалізації, можуть розглядатися такі параметри, як модуляція, інтонація, висота тону і т. д.

Одним з основних переваг розпізнавання по голосу є загальнодоступність, зручність і простота в застосуванні - даний метод не вимагає інший апаратури, крім загальнодоступних мікрофона і звукової плати. Однак людський голос досить складний для розпізнання зважаючи на свою мінливості - внаслідок захворювання, віку, зміни настрою. Крім того, проблему представляє і необхідність врахування шумів [13].

1.5.9 Рукописний почерк

Метод біометричної аутентифікації по рукописному почерку ґрунтується на специфічному русі людської руки під час підписання документів. Для збереження підпису використовують спеціальні ручки або сприйнятливі до тиску поверхні. Цей вид аутентифікації людини використовує його підпис. Шаблон створюється в залежності від необхідного рівня захисту. Зазвичай виділяють два наведених нижче способу обробки даних про підписи [14].

1. Аналіз самого підпису, тобто використовується просто ступінь збігу двох зображень. Недоліки такого способу очевидні - схильність фальсифікації і неможливість двічі заявити одне і ту ж підпис роблять даний метод безперспективним.

2. Аналіз динамічних характеристик написання, тобто для аутентифікації будується згортка, в яку входить інформація по підпис, часовими і статистичними характеристиками її написання. Даний спосіб дуже зручний, оскільки не вимогливий до обладнання і звичний для людини.

В цілому даний метод не є надійним, оскільки чіткий рукописний почерк формується не у всіх користувачів і є нестійкою характеристикою.

1.5.10 Клавіатурний почерк

Клавіатурний почерк [15] - характеристика, яка описується наступними параметрами:

- швидкість введення - кількість введених символів, розділене на час друку;

- динаміка введення, характеризується часом між натисканнями клавіш і часом їх утримання;

- частота виникнення помилок при введенні;

- використання клавіш, наприклад, які функціональні клавіші натискаються для введення великих літер і т. д.

Аутентифікація по клавіатурного почерку може проводитися двома способами:

- за набором ключової фрази (що дозволяє поєднати цю аутентифікацію з пральний);

- за набором довільного тексту.

Часові інтервали між натисканням клавіш на клавіатурі і час утримання клавіш дозволяють досить однозначно охарактеризувати почерк людини, що підтверджується рядом експериментів [16]. Але даний метод підходить далеко не для всіх користувачів, оскільки достатній для розпізнання клавіатурний почерк формується тільки для осіб з тривалим досвідом роботи на клавіатурі. Для інших користувачів ймовірність помилки досить висока, що робить цей метод неприйнятним для масового поширення.

2 ПРИНЦИП ДІЇ ТА АНГОРИТМ АУТЕНТИФІКАЦІЇ ЗА КЛАВІАТУРНИМ ПОЧЕРКОМ

2.1 Принцип дії біометричних систем аутентифікації

Біометричні системи розпізнають людей на основі їх анатомічних особливостей (відбитків пальців, способу особи, малюнка ліній долоні, райдужної оболонки, голоси) або поведінкових рис (підписи, ходи). Оскільки ці риси фізично пов'язані з користувачем, біометричний розпізнавання надійно в ролі механізму, що стежить, щоб тільки ті, у кого є необхідні повноваження, могли потрапити в будівлю, отримати доступ до комп'ютерної системи або перетнути кордон держави. Біометричні системи також мають унікальні перевагами - вони не дозволяють відректися від досконалої транзакції і дають можливість визначити, коли індивідуум користується декількома посвідченнями (наприклад, паспортами) на різні імена. Таким чином, при грамотній реалізації у відповідних додатках біометричні системи забезпечують високий рівень захищеності.

Правоохоронні органи вже більше століття в своїх розслідуваннях користуються біометричної аутентифікації з використанням відбитка пальця, а в останні десятиліття відбувається швидке зростання впровадження систем біометричного розпізнавання в урядових і комерційних організаціях у всьому світі. Хоча багато з цих впроваджень дуже успішні, існують побоювання з приводу незахищеності біометричних систем і потенційних порушень приватності через несанкціоновану публікації збережених біометричних даних користувачів. Як і будь-який інший аутентифікаційний механізм, біометричну систему може обійти досвідчений шахрай, який володіє достатнім часом і ресурсами.

Біометрична система на етапі реєстрації записує зразок біометричної риси користувача за допомогою датчика - наприклад, знімає обличчя на камеру. Потім з біометричного зразка витягуються індивідуальні риси - наприклад, Мінуцій (дрібні подробиці ліній пальця) - за допомогою програмного алгоритму екстракції рис (feature extractor). Система зберігає витягнуті риси як шаблон в базі даних поряд з іншими ідентифікаторами, такими як ім'я або ідентифікацій-

ний номер. Для аутентифікації користувач пред'являє датчику ще один біометричний зразок. Риси, витягнуті з нього, являють собою запит, який система порівнює з шаблоном заявленої особистості за допомогою алгоритму зіставлення. Він повертає рейтинг відповідності, що відображає ступінь схожості між шаблоном і запитом. Система приймає заяву, тільки якщо рейтинг відповідності перевищує заздалегідь заданий поріг.

Біометрична система вразлива для двох видів помилок. Коли система не розпізнає легітимного користувача, відбувається відмова в обслуговуванні, а коли самозванець невірно ідентифікується як авторизованого користувача, кажуть про вторгнення. Для таких збоїв існує маса можливих причин, їх можна поділити на природні обмеження і атаки зловмисників.

На відміну від систем аутентифікації по паролю, які вимагають точного відповідності двох алфавітно-цифрових рядків, біометрична аутентифікаційних система покладається на ступінь схожості двох біометричних зразків, а оскільки індивідуальні біометричні зразки, отримані в ході реєстрації та аутентифікації, рідко ідентичні, біометрична система може робити помилки аутентифікації двох видів. Хибне невідповідність відбувається, коли два зразка від одного і того ж індивідуума мають низьку схожість і система не може їх зіставити. Хибне відповідність відбувається, коли два зразка від різних індивідуумів мають високу подібність і система некоректно оголошує їх збігаються. Хибне невідповідність веде до відмови в обслуговуванні легітимного користувача, тоді як помилкове відповідність може призвести до вторгнення самозванця. Оскільки йому не треба застосовувати якісь спеціальні заходи для обману системи, таке вторгнення називають атакою нульового зусилля. Велика частина досліджень в області біометрії за останні п'ятдесят років була зосереджена на підвищенні точності аутентифікації - на мінімізації помилкових невідповідностей і відповідностей.

Для визначення ефективності СКУД на основі біометричної ідентифікації використовують наступні показники:

- FAR (false acceptance rate) - коефіцієнт помилкового пропуску;

- FMR (false match rate) - ймовірність, що система невірно порівнює вхідний зразок з невідповідним шаблоном в базі даних;

- FRR (false rejection rate) - коефіцієнт помилкового відмови;

- FNMR (false non-match rate) - ймовірність того, що система помилиться у визначенні збігів між вхідним зразком і відповідним шаблоном з бази даних;

- графік ROC - візуалізація компромісу між характеристиками FAR і FRR;

- коефіцієнт відмови в реєстрації (FTE або FER) - коефіцієнт безуспішних спроб створити шаблон з вхідних даних (при низьку якість останніх);

- коефіцієнт помилкового утримання (FTC) - ймовірність того, що автоматизована система не здатна визначити біометричні вхідні дані, коли вони представлені коректно;

- ємність шаблону - максимальна кількість наборів даних, які можуть зберігатися в системі[3].

2.2 Принцип дії аутентифікації за клавіатурним почерком

Для реалізації біометричної аутентифікації буде використовуватись реалізовано два режима, які обираються з головного меню програми, режим навчання та режим аутентифікації. Режим навчання – режим в якому користувач створює еталон свого клавіатурного почерку, для нормальної роботі програми необхідно щоб користувач вводив як можна більше тексту. Режим аутентифікації – режим в якому користувач вводить логін та набирає текст у відповідне вікно програми, а потім натискає на кнопку аутентифікації, в той момент порівнюється дані введені користувачем з еталоном, котрий зберігається в базі.

Узагальнений алгоритм режиму навчання представлений на рис. 2.1.

Рисунок 2.1 – Алгоритм режиму навчання

Узагальнений алгоритм режиму аутентифікації представлений на рис. 2.2.

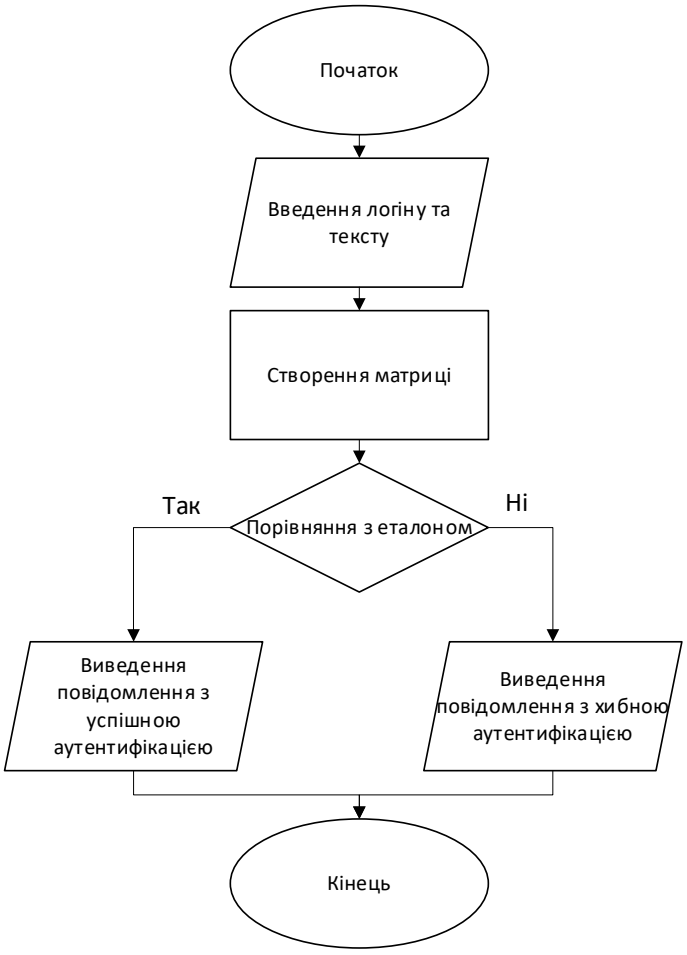

Рисунок 2.1 – Алгоритм режиму аутентифікації

2.3 Алгоритм порівняння зразків клавіатурного почерку за допомогою міри Хеммінга

Для порівняння зразків за допомогою міри Хеммінга використовується дві характеристики, часові зарубки (*vi*):

- час утримання клавіші;

- інтервал між натисками пар клавіш.

Для створення масиву даних користувача розраховується математичне очікування:

$$m_j(v_j) = \frac{(j-1)m_{j-1}(v_i) + v_{ij}}{j} \tag{2.1}$$

де $m_j(v_j)$ – середнє значення величини v_i після j-ї ітерації введення тексту;

i – порядковій номер часової зарубки в векторі;

v_{ij} – значення i-ї часової зарубки при j-му введенні тексту.

Для кожного запису в масиві розраховується середньоквадратичне відхилення ($\sigma_j(v_j)$):

$$\sigma_j(v_j) = \sqrt{\frac{(j-2)\sigma_{j-1}^2(v_i) + v_{ij} + (v_{ij} - m_j(v_j))^2}{j-1}} \tag{2.2}$$

Для запису всіх часових зарубок необхідно обчислити діапазон, який індивідуальний для кожного користувача. Перед записом до масиву дані перевіряються на факт потрапляння значення до розрахованого діапазону. Для отримання високої точності необхідно щоб користувач ввів великий фрагмент тексту. Межі діапазону розраховуються за формулами:

$$min(v_i) = m(v_i) - t[L, (1-P_i)] \cdot \sigma(v_i) \tag{2.3}$$

$$max(v_i) = m(v_i) + t[L, (1-P_i)] \cdot \sigma(v_i) \tag{2.3}$$

де L – кількість введень користувачем значення отриманих при реєстрації, далі використовується як ступінь свободи при виборі коефіцієнта Стьюдента;

P_i – значення коефіцієнту FRR;

$t[L,(1-P_i)]$ – коефіцієнт Стьюдента, зо відповідає значенню FRR та L.

Якщо представити довжину вектору часових зарубок як k, $i \in [1,k]$;

- v_i – значення i-ї часової зарубки у векторі;

- $m(v_i)$ – середнє значення елементу вектора, отримане при реєстрації;

- $\sigma(v_i)$ – середнє відхилення значення, котре розраховується при реєстрації,

то оцінка схожості S, що надається алгоритмом щільності ймовірностей Гауса для порівняння векторів, розраховується за формулою:

$$S = \frac{\sum_{i=1}^{k} S_i}{k}, \tag{2.4}$$

де S_i – оцінка для кожного елементу вектору:

$$S_i = e^{\frac{(v_i - m(v_i))^2}{2 \cdot \sigma^2(v_i)}} \tag{2.5}$$

Для даного методу реалізації міри Хеммінга граничні значення, коефіцієнти FAR та FRR визначаються експериментальним шляхом та обираються оптимальні значення.

3 АРХІТЕКТУРА, ІНФОРМАЦІЙНА ТА ФУНКЦІОНАЛЬНА СТРУКТУРИ КОМПЛЕКСУ

3.1 Інформаційна структура комплексу

Інформаційна структура комплексу – це спосіб організації компонентів системи за їх інформаційним призначенням, а також зав'язків, що забезпечують необхідну взаємодію усіх цих компонентів.

Основні елементи комплексу аутентифікації:

- пристрій для зчитування біометричної характеристики;
- зразок який тільки зчитали;
- блок по обробці зчитаних біометричних даних;
- контрольний шаблон біометричної характеристики;
- база даних, яка зберігає еталонні шаблони користувачів;
- сам еталонний шаблон;
- блок для порівняння контрольного та еталонного зразків.

Пристрій зчитування характеристик – являє собою клавіатуру ПК. Процес представлення характеристики зводиться до вводу тексту

Зразок – являє собою два набори часових інтервалів: час утримання клавіші, інтервал між натисканням клавіши. Виміряні при введені тексту.

Обробка – виконує формування контрольного шаблону із отриманого зразка. Реалізується програмно, тобто як частина програмного комплексу системи.

Контрольний шаблон – єдиний масив часових зарубок. Представляється, як для порівняння з еталонним шаблоном при проходженні аутентифікації.

База даних – набір текстових файлів, які містять в собі еталонні шаблони користувачів. База формується в навчальному режимі.

Еталонний шаблон – набір масивів характеристик часових зарубок. Формується при роботі користувача в режимі навчання. Зберігається у базі даних системи.

Порівняння – реалізація методики аналізу клавіатурного почерку на основі міри Хеммінга.

Для зберігання даних використовується формат *.json, за простоту розуміння та використання, цей формат має не обмежені можливості для розширення, його можна перетворити в структуру даних за допомогою більшості мов програмування, а також більшість мов програмування мають функції та бібліотеки для зчитування та створення структур JSON [тезиси].

Програма аналізує усі символи ASCII таблиці за виключенням керуючих перших 32 символів.

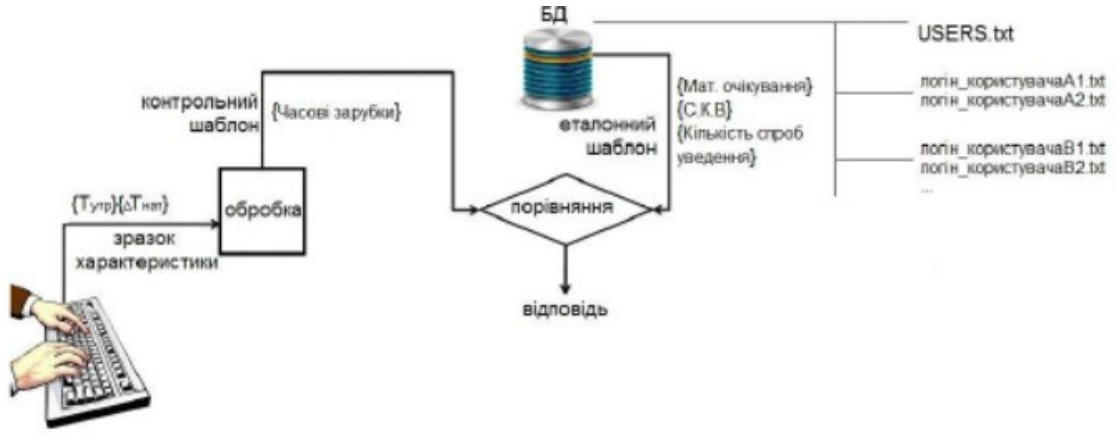

Рисунок 3.1 – Інформаційна структура системи

3.3 Функціональна структура комплексу

Під функціональною структурою в загальному випадку розуміють сукупність процедур, операцій, що циклічно повторюються, також їх зв’язки, орієнтованих на результат роботи системи. Структура формується з метою розкриття призначених функціональних компонентів системи.

Послідовність типових операцій і процедур при аутентифікації представлена на рисунку 3.2:

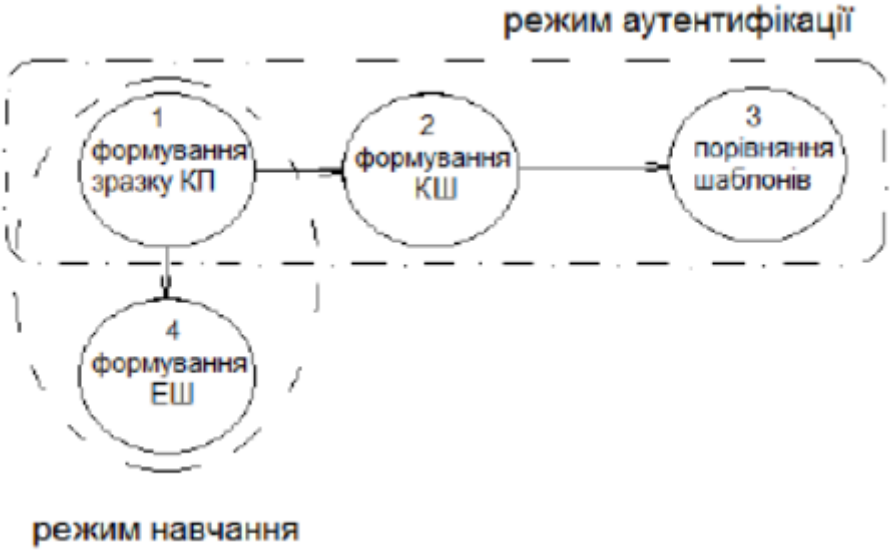

Рисунок 3.2 – Послідовність типових процедур при аутентифікації

На рисунку 3.2 під 1 слід розуміти представлення біометричної характеристики і формування зразку КП.

Вхідними даними, можна вважати: фрагмент тексту, який вводив користувач.

Вихідні дані: масиви часів утримання клавіш, та масив інтервалів між натисканнями клавіш (зразок біометричної характеристики)

Під 2 – Формування КШ слід розуміти обробку сформованого зразка для формування контрольного шаблону користувача.

Вхідні дані: зразок біометричної характеристики.

Вихідні дані: контрольний шаблон користувача.

Під 3 – Порівняння шаблонів слід розуміти – порівняння контрольного шаблону з еталонним, що зберігається у БД

Вхідні дані: контрольний та еталонний шаблони користувача.

Вихідні дані: відповідь про аутентифікацію.

Під 4 слід розуміти – формування еталонного шаблону КП та збереження його у файл.

Вхідні дані: фрагмент тестового тексту, уведений користувачем для зняття часових характеристик почерку.

Вихідні дані: еталонний шаблон користувача.

4 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСУ

4.1 Вибір мови програмування та середовища розробки

Python – інтерпретована об’єктно-орієнтована мова програмування високого рівня з строгою динамічною типізацією. Структури даних високого рівня разом із динамічною семантикою та динамічним зв’язуванням роблять її привабливою для швидкої розробки програм, а також як засіб поєднання існуючих компонентів. Python підтримує модулі та пакети модулів, що сприяє модульності та повторному використанню коду. Інтерпретатор Python та стандартні бібліотеки доступні як у скомпільованій так і у вихідній формі на всіх основних платформах. В мові програмування Python підтримується декілька парадигм програмування, зокрема: об’єктно-орієнтована, процедурна, функціональна та аспектно-орієнтована. Серед основних її переваг можна назвати такі: – чистий синтаксис (для виділення блоків слід використовувати відступи); – переносність програм (що властиве більшості інтерпретованих мов); – можливість використання Python в діалоговому режимі; – стандартний дистрибутив має просте, але разом із тим досить потужне середовище розробки, яке зветься IDLE і яке написане на мові Python; – зручний для розв’язання математичних проблем (має засоби роботи з комплексними числами, може оперувати з цілими числами довільної величини, у діалоговому режимі може використовуватися як потужний калькулятор); – відкритий код. Виділяють такі недоліки Python: – Низька швидкодія; – Відсутність статичної типізації; – Неможливість модифікації вбудованих класів (int, str та інших подібних).

Середовищем розробки було обрано PyCharm, тому що дана IDE э дуже потужним інструментом для розробки. PyCharm своїми вбудованими засобами дозволяє відкривати бази даних, користуватися налагодженням програм та багато іншими корисними функціями під час розробки.

4.2 Перелік функціональних компонентів комплексу

Програмний комплекс складається з головного меню програми (див. рис. 4.1) в якому можливо обрати необхідний режим роботи програми: навчання (Learning) або аутентифікація (Authentication).

Рисунок 4.1 – Головне меню програми

Для створення графічного інтерфейсу програми було використано відкриту бібліотеку PySimpleGui. В цій бібліотеці можливо створити свій кастомний шаблон з необхідними полями та кнопками.

Обираючи режим навчання користувачу надається можливість ввести ім’я користувача та тестовий текст у відповідних полях рис. 4.2.

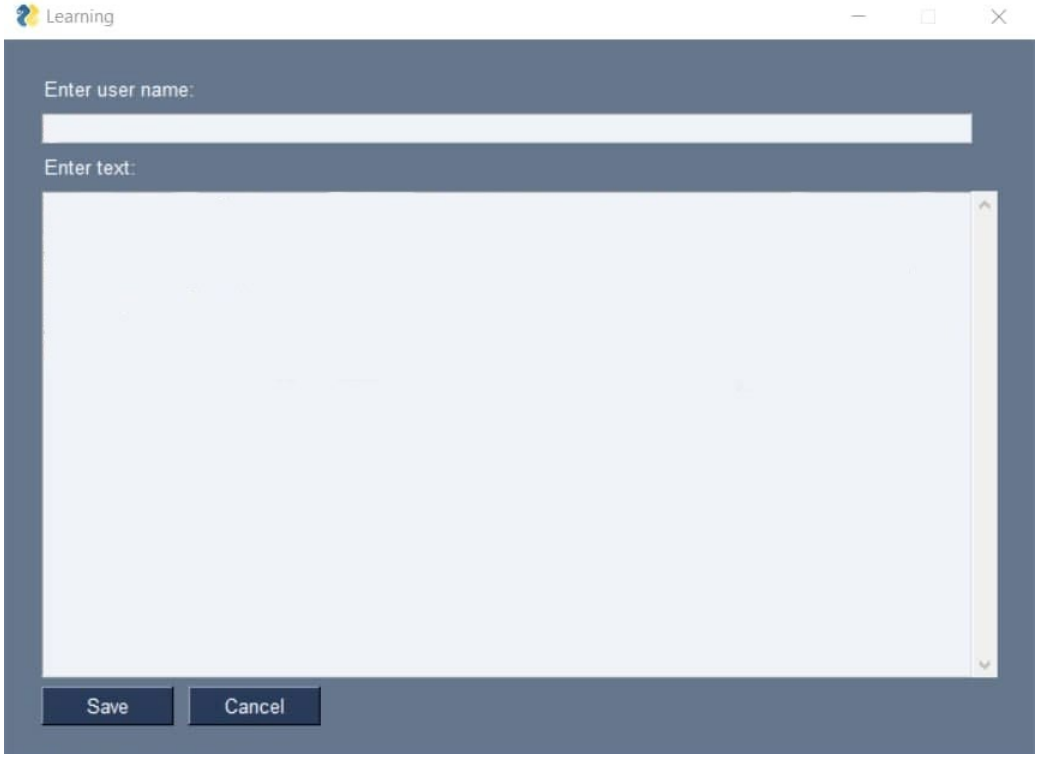

Рисунок 4.2 – Вікно режиму навчання

Після відкриття вікна режиму навчання у фоновому процесі починається виконуватися процес аналізу натиску всіх клавіш клавіатури. Фоновій процес реалізований за допомогою стандартної бібліотеки _thread. Фоновий процес виконаний для того щоб збирати дані про користувача навіть в момент введення імені користувача.

Під час кожного натискання клавіші аналізується код клавіші, час утримання та інтервал між натиском передостанньої та останньої клавіші. Для кожної клавіші розраховується математичне очікування утримання клавіші та записується в окремий файл. Інтервал між натисканням двох останніх клавіш також розраховується математичне очікування на основі даних які зберігаються та щойно введених даних. Для кожного другого натиску однієї і тієї ж пари клавіш розраховується додатково дисперсія, в файл записується математичне очікування, кількість натисків кожної пари клавіш та значення дисперсії.

Після введення тексту користувач має натиснути на кнопку збереження даних, після цього дані запишуться у два файли, які відповідають користувачу, а також поповниться файл бази користувачів.

Для проходження аутентифікації користувач має вибрати відповідний пункт головного меню програми, після чого відкриється вікно аутентифікації рис. 4.3.

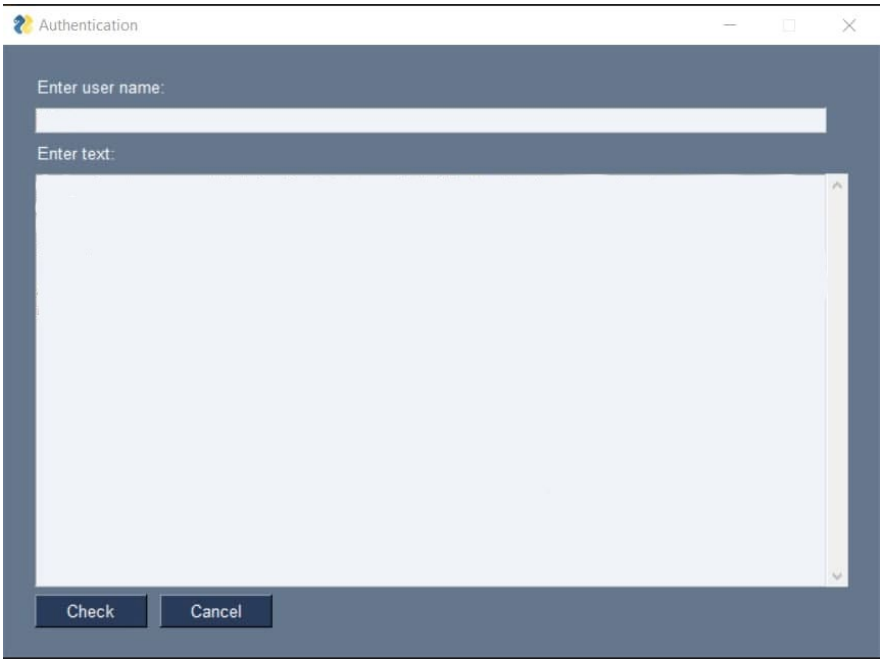

Рисунок 4.3 – Вікно режиму аутентифікації

Після відкриття вікна аутентифікації програма також автоматично запускає в новому потоці процес, котрий аналізує та збирає ті самі дані як в режимі навчання. Після натиску на клавішу програми перевірити (Check) програма порівнює значення отримані в момент реєстрації користувача та дані в момент проходження аутентифікації. В результаті виконання необхідних розрахунків програма демонструє на скільки відсотків схожі дані в базі з даними отриманими в момент аутентифікації. Текст програм зображений в додатку А.

4.3 Тестування комплексу

Для тестування комплексу було створено новий обліковий запис (див. рис. 4.4).

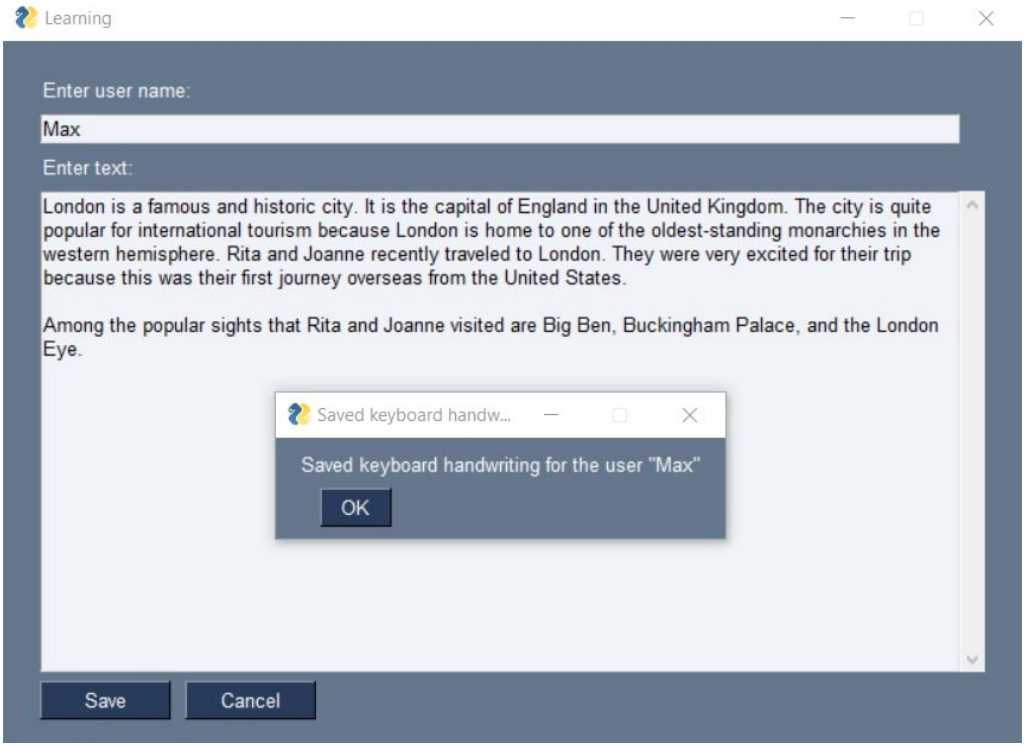

Рисунок 4.4 – Створення облікового запису

Для тестування використовував той самий текст введений мною (див. рис. 4.5) та одногрупником (див. рис. 4.6).

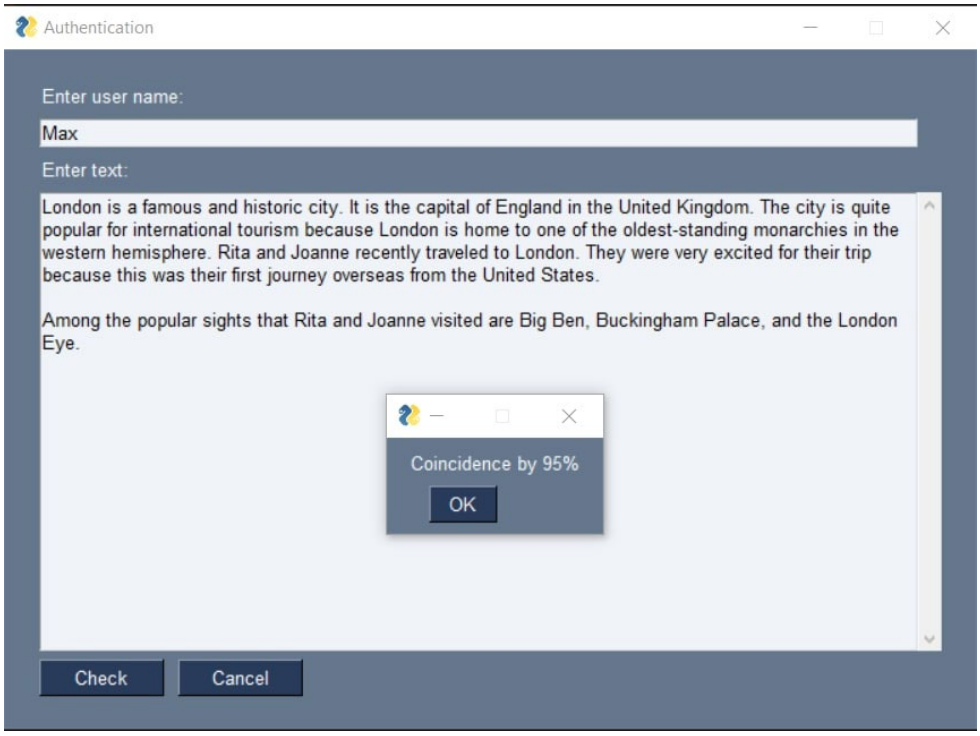

Рисунок 4.5 – Результат введення тексту користувачем

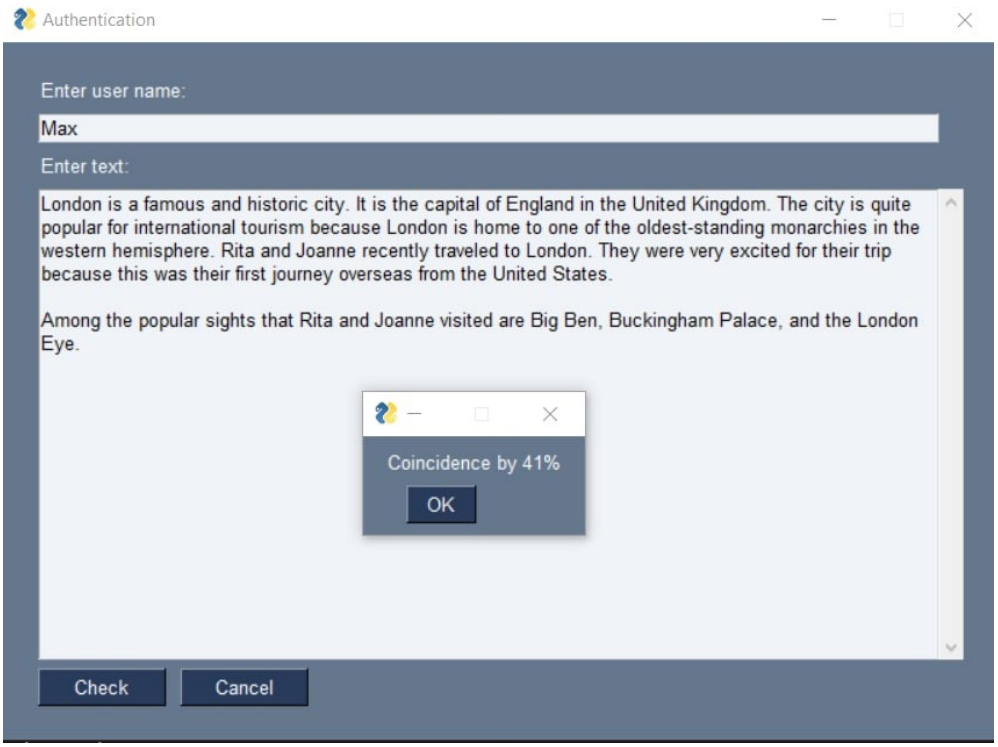

Рисунок 4.5 – Результат введення тексту користувачем

За результатами можна побачити, що я успішно пройшов аутентифікацію, а одногрупник має низький відсоток схожості з еталонним значенням.

5 МЕТОДИКА ВИКОРИСТАННЯ КОМПЛЕКСУ

5.1 Інструкція використання комплексу

Програмний комплекс складається з трьох вікон:

- вікно головного меню, в якого обирається режим роботи (див. рис. 5.1);
- вікно навчання (див. рис. 5.2);
- вікно аутентифікації (див. рис. 5.3);

Рисунок 5.1 – Головне меню вибору режиму

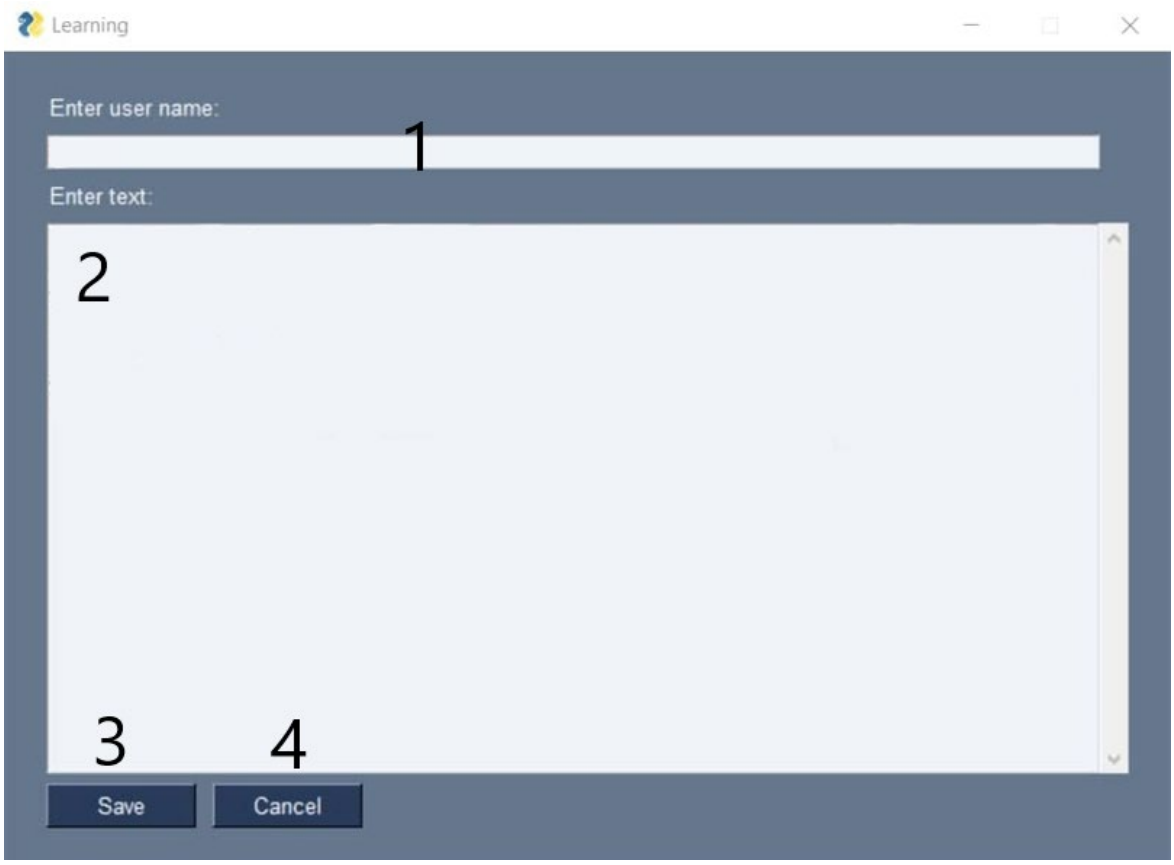

Рисунок 5.2 – Вікно режиму навчання

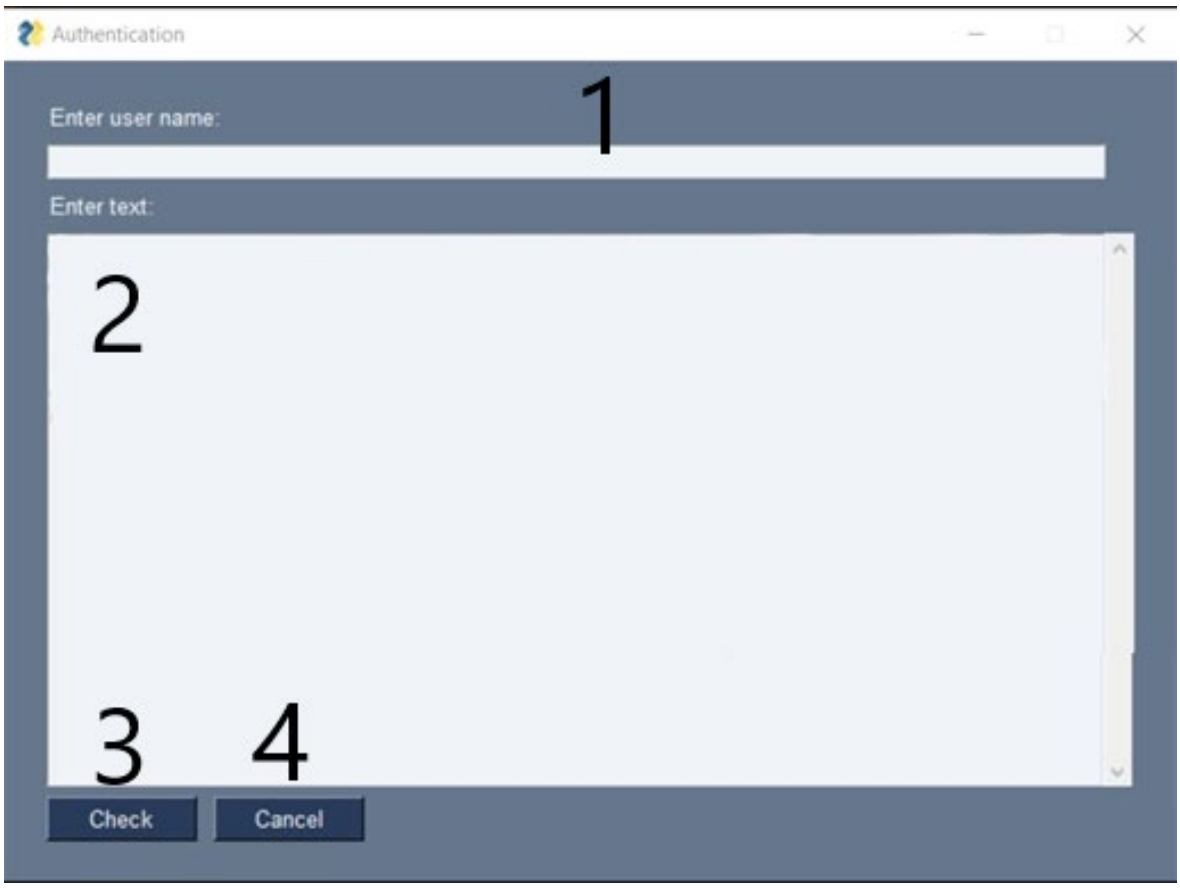

Рисунок 5.3 – Вікно режиму аутентифікації

В режимі аутентифікації користувачеві надається можливість введення імені користувача (поле 1), а також тексту для збереження еталонного зразку для користувача (поле 2). Програма аналізує клавіші з ASCII кодом 32 и більше, це виключає всі керуючі символи (див. рис. 5.4). Процес аналізу введення клавіш відбувається у фоновому режимі, тому для більш чіткого розпізнання рекомендується увійти в режим навчання та ввести великий текст для створення обширного еталону. Бажано використовувати різні комбінації клавіш.

Після введення значень необхідно натиснути на кнопку 3 для збереження даних. Данні зберігаються у файлах формату: “user_name-matrix1d.json, “user_name-matrix2d.json” та “user_list.json”.

У файлі “user_name-matrix1d.json” (див. рис. 5.5) зберігається математичне очікування часу утримання кожної клавіші у форматі одномірного масиву, індекси клавіш у файлі зміщені на 32 через виключення з аналізу керуючих символів.

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;	`
1	1	001	SOH (start of heading)	33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;	a
2	2	002	STX (start of text)	34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;	b
3	3	003	ETX (end of text)	35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;	c
4	4	004	EOT (end of transmission)	36	24	044	&#36;	$	68	44	104	&#68;	D	100	64	144	&#100;	d
5	5	005	ENQ (enquiry)	37	25	045	&#37;	%	69	45	105	&#69;	E	101	65	145	&#101;	e
6	6	006	ACK (acknowledge)	38	26	046	&#38;	&	70	46	106	&#70;	F	102	66	146	&#102;	f
7	7	007	BEL (bell)	39	27	047	&#39;	'	71	47	107	&#71;	G	103	67	147	&#103;	g
8	8	010	BS (backspace)	40	28	050	&#40;	(	72	48	110	&#72;	H	104	68	150	&#104;	h
9	9	011	TAB (horizontal tab)	41	29	051	&#41;	)	73	49	111	&#73;	I	105	69	151	&#105;	i
10	A	012	LF (NL line feed, new line)	42	2A	052	&#42;	*	74	4A	112	&#74;	J	106	6A	152	&#106;	j
11	B	013	VT (vertical tab)	43	2B	053	&#43;	+	75	4B	113	&#75;	K	107	6B	153	&#107;	k
12	C	014	FF (NP form feed, new page)	44	2C	054	&#44;	,	76	4C	114	&#76;	L	108	6C	154	&#108;	l
13	D	015	CR (carriage return)	45	2D	055	&#45;	-	77	4D	115	&#77;	M	109	6D	155	&#109;	m
14	E	016	SO (shift out)	46	2E	056	&#46;	.	78	4E	116	&#78;	N	110	6E	156	&#110;	n
15	F	017	SI (shift in)	47	2F	057	&#47;	/	79	4F	117	&#79;	O	111	6F	157	&#111;	o
16	10	020	DLE (data link escape)	48	30	060	&#48;	0	80	50	120	&#80;	P	112	70	160	&#112;	p
17	11	021	DC1 (device control 1)	49	31	061	&#49;	1	81	51	121	&#81;	Q	113	71	161	&#113;	q
18	12	022	DC2 (device control 2)	50	32	062	&#50;	2	82	52	122	&#82;	R	114	72	162	&#114;	r
19	13	023	DC3 (device control 3)	51	33	063	&#51;	3	83	53	123	&#83;	S	115	73	163	&#115;	s
20	14	024	DC4 (device control 4)	52	34	064	&#52;	4	84	54	124	&#84;	T	116	74	164	&#116;	t
21	15	025	NAK (negative acknowledge)	53	35	065	&#53;	5	85	55	125	&#85;	U	117	75	165	&#117;	u
22	16	026	SYN (synchronous idle)	54	36	066	&#54;	6	86	56	126	&#86;	V	118	76	166	&#118;	v
23	17	027	ETB (end of trans. block)	55	37	067	&#55;	7	87	57	127	&#87;	W	119	77	167	&#119;	w
24	18	030	CAN (cancel)	56	38	070	&#56;	8	88	58	130	&#88;	X	120	78	170	&#120;	x
25	19	031	EM (end of medium)	57	39	071	&#57;	9	89	59	131	&#89;	Y	121	79	171	&#121;	y
26	1A	032	SUB (substitute)	58	3A	072	&#58;	:	90	5A	132	&#90;	Z	122	7A	172	&#122;	z
27	1B	033	ESC (escape)	59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123;	{
28	1C	034	FS (file separator)	60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124;	|
29	1D	035	GS (group separator)	61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125;	}
30	1E	036	RS (record separator)	62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126;	~
31	1F	037	US (unit separator)	63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127;	DEL

Рисунок 5.4 – Таблиця ASCII кодів

Рисунок 5.5 – Приклад “user_name-matrix1d.json” файлу

У файлі “user_name-matrix2d.json” (див. рис. 5.6) зберігається математичне очікування часу утримання кожної пари останніх натиснутих клавіш, кількість натисків пар клавіш та значення дисперсії, у форматі трьомірного масиву.

Рисунок 5.6 – Приклад “user_name-matrix2d.json” файлу

Також у файл “user_list.json” (див. рис. 5.7) записується ім’я користувача, щоб зберігати базу користувачів у форматі JSON.

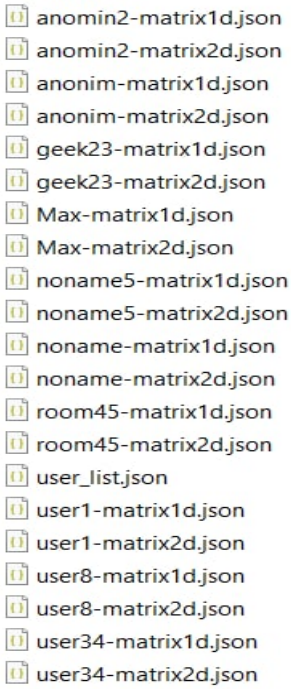

Рисунок 5.6 – Приклад “user_list.json” файлу

5.2 Методика використання в навчальному процесі

Даний програмний комплекс підходить для демонстрації біометричної аутентифікації на основі клавіатурного почерку реалізованого на основі міри Хеммінга. Комплекс дозволяє проаналізувати наступні етапи процесу аутентифікації:

- процес розрахунку математичного утримання, дисперсії, кількості натиснутих пар клавіш для тексту, який вводить користувачем, шляхом виводу проміжних значень у термінал;

- аналіз еталонних шаблонів користувачів, які зберігаються у відкритих файлах формату JSON, котрий дозволяє відобразити дані у зручному для користувача вигляді;

- порівняння еталонного значення шаблону користувача зі значенням отриманим під час спроби аутентифікації, та отримання відсоткового співвідношення схожості шаблонів, розрахованого за мірою Хеммінга.

5.3 Висновки за розділом

Програмний комплекс може бути використаний в учбовому процесі в якості демонстрації аутентифікації користувачів з використанням клавіатурного почерку при підготовці бакалаврів за спеціальністю «Кібербезпека», при проведенні лабораторних або практичних занять в рамках дисципліни «Методи та засоби захисту інформації». Студенти обзнайомлюючись з даним програмним комплексом отримають практичні навички по біометричній аутентифікації, а саме біометричній аутентифікації за клавіатурним почерком.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Вимоги безпеки при виконанні робіт на робочому місці

Охорона праці грає важливу роль в житті робітників. Метою управління охороною праці є забезпечення безпеки, збереження здоров'я та працездатності людини в процесі праці. Ця мета досягається виконанням відповідних функцій управління, тобто комплексом взаємопов'язаних видів, що здійснюються суб'єктом управління цілеспрямовано на об'єкт управління.

Згідно зі ст. 15 Закону України від 14.10.1992 р. № 2694-XII «Про охорону праці» [1] така служба обов’язково повинна бути створена на підприємстві з кількістю працюючих 50 і більше осіб відповідно до Типового положення про службу охорони праці.

Обов’язок роботодавця – затвердити документи, передбачені ст. 13 Закону України № 2694 [2]. Вони повинні встановлювати правила виконання робіт і поведінки працівників на території підприємства, у виробничих приміщеннях, на будівельних майданчиках і робочих місцях. Інструкції та інша документація з охорони праці розробляються керівниками структурних підрозділів на підставі положень законодавства з охорони праці, типових інструкцій та технологічної документації підприємства з урахуванням виду діяльності підприємства і конкретних умов праці на ньому.

Перед початком роботи нового працівника роботодавець згідно зі ст. 29 Кодексу законів про працю України [3] зобов’язаний проінформувати його під розписку про умови праці, наявні на його робочому місці. У тому числі, про всі небезпечні чи шкідливі виробничі фактори, які ще не усунуто, та про можливі наслідки їх впливу на здоров’я працівника, а також про можливі пільги та компенсації за роботу в таких умовах.

Згідно до Закону України «про охорону праці» [1] Робочі місця мають відповідати вимогам цих Правил та Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних ма-

шин, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 №7 (ДСанПіН 3.3.2-007-98) [4].

Вимоги охорони праці до виробничих приміщень де працюють ЕОМ: Вимоги стосовно:

- Освітлення;
- рівнів шуму;
- вібрації;
- електромагнітного;
- ультрафіолетового;
- інфрачервоного випромінювання та електростатичного поля викладено у ДСанПіН [4];
- Виробничі об'єкти повинні відповідати проектній документації

Під час експлуатації будівель та споруд, де розміщені робочі місця операторів забезпечуватись вимоги:

- Положення про безпечну та надійну експлуатацію виробничих будівель
- Правил обстежень, оцінки технічного стану та паспортизації будівель
- Електробезпеки будівель та приміщень, де розміщені робочі місця операторів,
- Щодо пожежної безпеки будівель та приміщень
- Відповідати Правилам пожежної безпеки України

Вимоги безпеки перед початком роботи з комп'ютером (ноутбуком) та іншою оргтехнікою

- Оглянути і переконатися у справності обладнання, електропроводки. У разі виявлення несправностей, до роботи не приступати. Повідомити про це керівника і, тільки після усунення несправностей і його дозволу, приступити до роботи.
- Перевірити освітлення робочого місця, за необхідності, вжити заходів до його нормалізації.

- Перевірити наявність та надійність захисного заземлення устаткування.
- Перевірити стан електричного шнура і вилки.
- Перевірити справність вимикачів та інших органів управління персональним комп'ютером та оргтехніки.
- При виявленні будь-яких несправностей, комп'ютер та оргтехніку не вмикати і негайно повідомити про це завідувача дошкільним навчальним закладом.
- Ретельно провітрити приміщення з персональним комп'ютером та оргтехнікою, переконатися, що мікроклімат у приміщенні знаходиться в допустимих межах: температура повітря в холодний період року 22-24°С, в теплий період року - 23-25°С, відносна вологість повітря — 40-60%.
- Включити монітор і перевірити стабільність і чіткість зображення на екрані, переконатися у відсутності запаху диму від комп'ютера та оргтехніки.

Вимоги безпеки під час роботи:

- Виконувати тільки ту роботу, яка має бути за робочим планом.
- Вмикати і вимикати електронне обладнання тільки вимикачами, забороняється проводити вимкнення вийманням вилки з розетки.
- Не палити на робочому місці.
- Суворо виконувати загальні вимоги по електробезпеці та пожежній безпеці.
- Електронне обладнання, технічні засоби навчання необхідно використовувати у суворій відповідальності з експлуатаційною документацією до нього.
- Про всі несправності та збої в роботі устаткування та апаратури, або їх відсутності необхідно повідомити безпосередньо керівника.
- Забороняється знімати захисні пристрої з обладнання і працювати без них.
- Забороняється під час роботи пити будь-які напої, приймати їжу.

- Забороняється залишати включене обладнання без нагляду.
- Самостійно розбирати та проводити ремонт електронної та електронно-механічної частини комп'ютера, периферійних пристроїв, оргтехніки категорично забороняється. Ці роботи може виконувати тільки спеціаліст або інженер з технічного обслуговування комп'ютерної техніки.

Вимоги безпеки після закінчення роботи з комп'ютером, принтером, ксероксом, сканером та іншою оргтехнікою

- Вимкнути комп'ютер, ноутбук, телевізор, плазмову панель, LCD-екран, принтер, ксерокс, сканер, колонки та іншу оргтехніку від електромережі, для чого необхідно вимкнути тумблери, а потім акуратно витягнути штепсельні вилки з розетки.
- Протерти зовнішню поверхню комп'ютера чистою вологою тканиною. При цьому не допускайте використання розчинників, одеколону, препаратів в аерозольній упаковці.
- Прибрати робоче місце. Скласти диски у відповідне місце зберігання.
- Ретельно провітрити приміщення з персональним комп'ютером та іншою оргтехнікою.

5.2 Шкідливі виробничі фактори на робочому місці

Під час роботи на виробництві на людину можуть впливати один, або низка небезпечних та шкідливих виробничих факторів. Безпека того чи іншого технологічного процесу може бути визначена за їх кількістю і за ступенем небезпеки кожного з них зокрема. Безпека праці на виробництві визначається ступенем безпеки окремих технологічних процесів.

Небезпечні й шкідливі виробничі фактори стандартом ГОСТ 12.0.003-74 [5] поділяються на:

- Фізичні;
- хімічні;
- біологічні;
- психофізіологічні.

Останні за характером впливу на людину підрозділяються на фізичні й нервово-психічні перевантаження, а інші - на конкретні небезпечні й шкідливі виробничі фактори.

Шкідливі виробничі фактори — фактори середовища і трудового процесу, які можуть викликати професійну патологію, тимчасове або стійке зниження працездатності, підвищити частоту соматичних та інфекційних захворювань, призвести до порушення здоров'я потомства.

Найчастіші захворювання:

- варикозне захворювання
- простатит
- серцево-судинні захворювання
- остеохондроз
- перенапруження очей

Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці даного програмного комплексу:

- Організація робочого місця

Приміщення, в якому працює програміст, має загальну площу 20 м2, висоту стелі 3 м. У приміщенні знаходиться 7 робочих місць з ПК. Кожне робоче місце обладнане робочім столом площею 1,2 м2, стільцем та персональним комп'ютером, що складається з монітора, системного блоку, клавіатури та миші. Слід відзначити, що площа одного робочого місця оператора ПК не повинна бути меншою за 6м2, а об'єм не менший за 20м3, тобто площі та об'єму даного приміщення не вистачає для розташування 7 робочих місць операторів ПК.

Аналіз умов праці показує, що у приміщенні лабораторії на програміста можуть негативно впливати наступні фізичні та психофізіологічні фактори:

- підвищена або знижена температура повітря робочої зони;
- підвищена або знижена вологість повітря;
- недостатня освітленість робочого місця;
- підвищений рівень шуму на робочому місці;
- підвищена іонізація повітря;

- підвищений рівень електромагнітних випромінювань;
- нервово-психічні перевантаження (розумова перенапруга, перенапруга аналізаторів);
- фізичні перевантаження (одноманітна поза викликає статичну втому).

- Мікроклімат робочої зони програміста

Робота програміста за енерговитратами відноситься до категорії легких робіт Іа, Іб, тому повинні дотримуватися наступні вимоги згідно ДСН 3.3.6.042-99 [6]:

- оптимальна температура повітря – 22°С (допустима – 20-24°С);
- оптимальна відносна вологість – 40-60% (допустима – не більш 75%);
- швидкість руху повітря не більш 0,1 м/с.

- Освітлення робочого місця

Нормованим параметром природного освітлення згідно ДБН В.2.5–28 – 2006 [7] є коефіцієнт природного освітлення (КПО). КПО встановлюється в залежності від розряду виконуваних зорових робіт. Робота програміста відноситься до робіт середньої точності (IV розряд зорових робіт, мінімальний розмір об'єкту розрізнення складає 0,5-1,0мм), для яких при використанні бокового освітлення КПО=1,5%. Для штучного освітлення нормованим параметром виступає Емін – мінімальний рівень освітленості, та Кп – коефіцієнт пульсації світлового потоку, який не повинний бути більшим ніж 20%. Мінімальна освітленість встановлюється в залежності від розряду виконуваних зорових робіт. Для IV розряду зорових робіт вона складає 300-500 лк.

1.1 Дії працівників в аварійних ситуаціях

Згідно з постановою Головного державного санітарного лікаря України [4]. При ураженні електричним струмом необхідно якомога швидше звільнити потерпілого від струмопровідних частин обладнання. Дотик до струмопровідних частин (мережі під напругою) у більшості випадків призводить до судом

м’язів, тобто людина самостійно не в змозі відірватися від провідника. Тому необхідно швидко відключити ту частину електрообладнання, до якої доторкається людина. Будь-яке зволікання при наданні допомоги, а також невміння того, хто допомагає, надати кваліфіковану допомогу, призводить до загибелі людини, яка знаходиться під дією струму.

При звільненні потерпілих від струмопровідних частин або проводу в електроустановках напругою до 1000 В відключають струм, використовуючи сухий одяг, палицю, дошку, шапку, сухі рукавиці, рукав одягу, діелектричні рукавиці. Провідники перерізають інструментом з ізольованими ручками, перерубують сокирою з дерев’яним сухим топорищем.

Якщо потерпілий після звільнення від дії електричного струму і надання медичної допомоги прийшов до тями, його не слід одного відправляти додому або допускати до роботи. Такого потерпілого слід доставити в лікувальний заклад, де за ним буде встановлено спостереження, так як наслідки від впливу електричного струму можуть проявитися через кілька годин і привести до більш важких наслідків.

Вимоги техніки безпеки та безпеки життєдіяльності в аварійних ситуаціях при роботі з комп'ютером та іншою оргтехнікою

- Якщо на металевих частинах обладнання виявлено напругу (відчуття струму), заземлюючий провід обірваний, необхідно вимкнути обладнання, негайно доповісти керівникові про несправності електрообладнання і без його вказівки до роботи не приступати.
- При припиненні подавання електроенергії, вимкнути обладнання.
- При появі незвичного звуку, запаху паленого, мимовільного відключення комп'ютера та оргтехніки, негайно припинити роботу і поставити до відома керівника.
- При виникненні пожежі негайно вимкнути обладнання, знеструмити електромережу за винятком освітлювальної мережі, повідомити про пожежу всім працюючим і приступити до гасіння осередку пожежі наявними засобами пожежогасіння.

- При нещасному випадку необхідно, насамперед, звільнити потерпілого від травмуючого фактора, звернутися до медпункту, зберегти, по можливості, місце травмування в тому стані, в якому воно було на момент травмування. При звільненні потерпілого від дії електроструму слідкуйте за тим, щоб самому не опинитися в контакті з токоведучою частиною та під напругою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрєєва, О.О. Система аутентифікації, заснована на використанні акустичних властивостей серця [Текст] / Е.А. Андрєєва // Доповіді Томського державного університету систем управління і радіоелектроніки. - 2012. - № 2. - С. 153-156

2. Брагіна Є.К. Сучасні методи біометричної аутентифікації: огляд, аналіз і визначення перспектив розвитку [Текст] / Є.К. Брагіна, С.С. Соколов // Вісник Астраханського державного технічного університету. - 2016. - № 4. - С. 40-45.

3. 0 Шибанов, С.В. Порівняльний аналіз сучасних методів аутентифікації користувача [Текст]/ С.В.Шибанов, Д.А. Карпушин // Математичне та програмне забезпечення систем у промисловій та соціальній сферах. - 2015. - №1. - С. 33-37.

4. Нікішова, А. В. Програмний комплекс виявлення атак на основі аналізу даних реєстру [Текст]/ А.В. Нікішова, А. Е Чурилін // Вісник ВолДУ. Серія 10. Інноваційна діяльність. - 2012. - № 6. - С. 152-155.

5. Шапіро, Л. Active Directory Domain Services. Двухфакторная аутентифікація. Теоретичні основи [Текст] / Л. Шапіро // Системний адміністратор. - 2010. - № 7-8. - С. 100-105.

6. Комаров, А. Сучасні методи аутентифікації: токен і це все пронем [Текст] / А. Комаров // T-Comm: Телекомунікації та Транспорт. - 2008. - № 2. - С. 23-26.

7. Ісхаков, А.Ю. Двухфакторная аутентифікація на основі про- граммного токена [Текст] / А.Ю. Ісхаков, Р.В. Мещеряков, І.А. Ходашінскій // Питання захисту інформації. - 2013. - № 3. - С. 23-28.

8. Labati, R.D., Sassi R., Scotti F. ECG biometric recognition: Permanence analysis of QRS signals for 24 hours continuous authentication [Text]/ R.D. Labati, R. Sassi, F. Scotti // Information Forensics and Security (WIFS), 2013 IEEE International Workshop on. – IEEE, 2013. – P. 31–36.

9. Ross, A. An introduction to biometric systems [Text]/ A. Ross, A.K. Jain, S. Prabhakar // IEEE Trans Circuits Syst Video Technol. – 2004. – №14. – P. 4–20

10. Моржаков, В. Сучасні біометричні методи иденти-ції [Текст]/ В. Моржаков, А. Мальцев // Безпека. Достовірність. Інформація. - 2009. - №. 83. - С. 44-48.

11. Гурєєва, О. Біометрична ідентифікація за відбитками пальців. Технологія FingerChip [Текст]/ О. Гурєєва // Компоненти та технології. - 2007. - №. 69. - С. 176-180.

12. Ложников, П.С. Аутентифікація користувачів комп'ютера по клавіатурного почерку і особливостям особи [Текст]/ П.С. Ложников, А.Е. Сулавко, Е.В. Бура // Питання кібербезпеки. - 2017. - № 4. - С. 24-34.

13. Афанасьєв, А.А. Безперервна аутентифікація диктора при веденні телефонних переговорів по низькошвидкісних цифрових каналах [Текст]/ А.А. Афанасьєв // Питання кібербезпеки. - 2016. - № 3. - С.60-68.

14. Мартинова, Л.Є. Дослідження та порівняльний аналіз методів аутентифікації [Текст]/ Л. Є. Мартинова, М.Ю. Умніцин, К.Є. Назарова // Молодий вчений. - 2016. - № 19. - С. 90-93.

15. Гузик, В.Ф. Біометричний методи аутентифікації [Текст]/ В.Ф. Гузик, М. Н. Десятерик. // Известия Південного федерального університету. Технічні науки. - 2000. - Т. 16. - №. 2. - С. 129-133.

16. Сабанов, А. Г. Основні процеси аутентифікації [Текст]/ А. Г. Сабанов //Питання захисту інформації. - 2012. - № 3. - С. 54-57.