Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Біометрична ідентифікація особистості на основі аналізу динаміки почерку роботи на клавіатурі

08-54.БКР.003.00.000 ПЗ

Виконав: студент 4 курсу, групи 2КІ-23мс
спеціальності 123 — «Комп'ютерна інженерія»
освітня програма — «Комп'ютерна інженерія»
Болденюк Н.А.

Керівник к.т.н., доц. каф. ОТ
Колесник І. С.

Рецензент к.т.н.. доцент, зав.каф. МБІС
Карпінець В. В.

Допущено до захисту
Завідувач кафедри ОТ
д.т.н., проф. Азаров О. Д.

"19" 06 2025 р.

Вінниця ВНТУ – 2025 рік

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедраобчислювальної техніки
Освітньо—кваліфікаційний рівень бакалавр
Галузь знань — 12 Інформаційні технології
Спеціальність— 123 Комп'ютерна інженерія
Освітня програма— Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ проф., д.т.н.
Азаров О. Д.
21 березня 2025 року

З А В Д А Н Н Я

НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Болденюку Нікіті Андрійовичу

1 Тема роботи: Біометрична ідентифікація особистості на основі аналізу динаміки почерку роботи на клавіатурі, керівник Колесник Ірина Сергіївна, к.т.н., доцент кафедри ОТ, затверджено наказом вищого навчального закладу № 97 від « 20 » березня 2025 р.

2 Строк подання студентом роботи 13.05.2025р.

3 Вихідні дані до роботи: технічний опис архітектури та технологій IoT: платформа Raspberry Pi, Wi-Fi адаптер Auspi Wireless Adapter і, SSH-з'єднання, мова програмування Java та фреймворк Spring Boot.

4 Зміст розрахунково-пояснювальної записки: вступ огляд та аналіз методів та засобів біометричної ідентифікації, механізми розпізнавання клавіатурного почерку, практична реалізація системи.

5 Перелік графічного матеріалу: порівняння часу між натисканням клавіш двох зразків у першого користувача.

Перелік ілюстративного матеріалу: Алгоритм отрмання шаблону.

6 Консультанти розділів роботи приведені в таблиці 1.

Таблиця 1 — Консультанти роботи

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-3	к.т.н., доц. каф. ОТ Колесник І.С.	21.03.2025р.	13.06.2025р.
Нормоконтроль	ас.каф.ОТ Швець С.І.	14.05.2025р.	30.05.2025р.

7 Дата видачі завдання 21.03.2025 р.

8 Календарний план приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів дипломної Роботи	Строк виконання	Підпис
1	Постановка задачі роботи	21.03.25	
2	Огляд предметної області	21.03.25— 29.03.25	
3	Розробка моделей розпізнавання	21.03.25— 29.03.25	
4	Дослідження основних підходів до ідентифікації на основі клавіатурного почерку	30.03.25— 11.04.25	
5	Дослідження основних підходів до ідентифікації на основі клавіатурного почерку	12.04.25— 26.04.25	
6	Тестування та демонстрація роботи системи	27.04.25— 07.05.25	
7	Оформлення пояснювальної записки та ілюстративного матеріалу	08.05.25	
8	Перевірка якості виконання бакалаврської роботи та усунення недоліків	14.05.25	

Студент Болденюк НІКІТА

Керівник роботи к.т.н., доц. Ірина КОЛЕСНИК

АНОТАЦІЯ

УДК 004.3

Болденюк Н.А. Біометрична ідентифікація особистості на основі аналізу динаміки почерку роботи на клавіатурі.

Бакалаврська кваліфікаційна робота зі спеціальності 123 — комп'ютерна інженерія, освітня програма — комп'ютерна інженерія. Вінниця: ВНТУ, 2025, 77 с.

На укр.мові. Бібліогр.: 13 назв, рис. 30, табл. 5.

У бакалаврській кваліфікаційній роботі проаналізовано біометричні методи ідентифікації, алгоритми розпізнавання за клавіатурним почерком. Обрано метод біометричної ідентифікації та аутентифікації за клавіатурним почерком під час введення текстового фрагменту. Наведені узагальнені алгоритми роботи засобів в різних режимах, розроблено програмне забезпечення засобів та перевірена його працездатність, створено інструкцію з використання.

Ключові слова: біометрична ідентифікація, клавіатура, тривалість натиску, ключова послідовність.

ABSTRACT

Boldenyk N. A. Biometric personal identification based on the analysis of handwriting dynamics on the keyboard.

Bachelor's qualification work in specialty 123 - computer engineering, educational program - computer engineering. Vinnytsia: VNTU, 2025, 77 p.

In Ukrainian. Bibliography: 13 titles, fig. 30, tab. 5.

The bachelor's qualification work analyzed biometric identification methods and keyboard handwriting recognition algorithms. The method of biometric identification and authentication by keyboard handwriting when entering a text fragment is chosen. Generalized algorithms for the operation of the devices in different modes are presented, the software for the devices has been developed and its performance has been tested, and instructions for use have been created.

Keywords: biometric identification, keyboard, keystroke duration, key sequence.

ЗМІСТ

ВСТУП

Біометричні методи розпізнавання використовувалися людством протягом усієї історії. Люди точно розпізнають знайомих людей за обличчям, голосом та ходою. Удосконалення систем автоматичної обробки інформації, швидкий розвиток інформатизації суспільства, зростання доступності персональних комп'ютерів, розвиток локальних та глобальних інформаційних мереж значно підвищили вимоги до надійності та безпеки інформації об'єктів, що беруть участь у впровадженні та експлуатації інформаційних мереж і систем.

Традиційні методи ідентифікації та розпізнавання, засновані на використанні мобільних ідентифікаторів, паролів та кодів доступу, мають низку суттєвих недоліків, пов'язаних з використанням атрибутивних та знаннєвих ознак розпізнавання для визначення особистості користувача. Цей недолік усувається при використанні біометричних методів ідентифікації. Біометричні ознаки є невід'ємною частиною людини, тому їх не можна забути чи втратити.

Біометричні системи ідентифікації та розпізнавання, звичайно, складні в реалізації, а їхні можливості наразі дуже обмежені через недосконаліть апаратного забезпечення та математичних моделей. Однак, враховуючи їх постійний розвиток, біометричні системи можуть суттєво замінити інші типи систем. Впровадження зручних для користувача систем біометричної ідентифікації та розпізнавання є важливим питанням, тому тема роботи є актуальною.

Слід враховувати, що клавіатурний почерк є нестатичною біометричною характеристикою людини та може змінюватися залежно від психоемоційного та фізичного стану користувача. Тому точність ідентифікації та перевірки клавіатурного почерку в програмних спробах є низькою, як і можливість великої кількості помилок першого та другого типів. Як наслідок, він не підходить для таємного керування клавіатурою та ідентифікації місцезнаходження оператора, тому тема цієї роботи є обов'язково **актуальною**.

Мета роботи — створення системи біометричної ідентифікації особистості на основі аналізу динаміки почерку роботи на клавіатурі

.

Задачі дослідження:

— визначення характеристик комп’ютерного почерку;

— дослідження алгоритмів, методів, моделей та засобів визначення КП користувача інформаційної системи;

— дослідження та створення математичної моделі визначення КП користувача інформаційної системи;

— розробка алгоритму дослідження КП користувача за тривалістю утримання клавіш;

— розробка алгоритму дослідження КП користувача за часом між натисненням клавіш;

— розробка способу визначення КП користувача за довільним текстом.

Об’єктом дослідження є процес біометричної ідентифікації особистості за динамікою почерку роботи на клавіатурі.

Предметом дослідження є методи та засоби обробки біометричної інформації, що формуються на виході клавіатури.

1 ОГЛЯД ТА АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ

1.1 Ідентифікація користувачів в сучасних системах

Одним з основних факторів, що визначають стан безпеки конкретної інформаційної інфраструктурної системи, є ефективність системи управління та забезпечення доступу користувачів і захист інформації, що зберігається в ній. Для запобігання значним матеріальним та нематеріальним збиткам необхідні серйозні заходи щодо захисту конфіденційної та цінної інформації від несанкціонованого доступу. Основним питанням у питанні захисту інформації в інформаційних системах від несанкціонованого доступу є питання розподілу функціональних повноважень. Завдання спрямоване на запобігання зловмиснику в зчитуванні або зміні інформації, що зберігається. Дії щодо захисту інформації від несанкціонованого доступу включають:

— запобігання проникненню зловмисника до ІС на основі особи користувача;

— створення спеціального захисту інформації;

— використання спеціальних методів захисту інформації від несанкціонованого доступу.

Визначено такі основні засоби забезпечення захисту від несанкціонованого доступу:

Аналіз правових, організаційних та морально-етичних засобів показав, що вони мають низьку надійність без підтримки фізичної, технічної та програмної інфраструктури. Також було виявлено, що вони сильно залежать від індивідуальних факторів, наприклад, від загальної структури роботи в компанії чи організації.

Виявленими недоліками фізичні, інженерні та технічні засобів є висока вартість, необхідність постійного моніторингу та коригувальних дій, наявність хибних тривог.

Виявленими перевагами апаратних та програмних засобів надійність, відсутність суб'єктивних факторів, можливість змін та вдосконалень, універсальність. Були визначені такі недоліки, що виникають у різних типах цих інструментів: висока вартість, залежність від типу інструменту, відсутність гнучкості.

Однією з областей застосування програмного та апаратного забезпечення є системи контролю та управління доступом. Для успішного впровадження контролю доступу та системного адміністрування для ІТ необхідно вирішити два завдання:створити можливість обходу системи контролю та розмежування доступу; та забезпечити ідентифікацію користувача, який входить до системи.

Ці завдання досягаються шляхом виконання наступних операцій контролю та управління, що застосовуються до користувача:

— створити можливість обходу системи контролю та розмежування доступу;

— забезпечити ідентифікацію користувача, який входить до системи.

Ці завдання досягаються шляхом виконання наступних операцій контролю та управління, що застосовуються до користувача:

— ідентифікація, тобто надання суб'єкту унікального та неповторного логіна;

— автентифікація, тобто підтвердження справжності особистості суб'єкта з метою доведення того, хто є цим суб'єктом.

Таким чином, було зроблено висновок, що забезпечення інформаційної безпеки основної системи залежить від якості операцій ідентифікації та розпізнавання користувача.

1.2 Контроль та управління інформацією сучасних системах

Зазначається, що в сучасних інформаційних системах ідентифікація, автентифікація та доступ до інформації переважно базуються на авторизації, тобто наданні законних прав уповноваженому користувачеві використовувати та

зберігати інформацію в системі. Для перевірки доступу користувача до ІС було визначено такі кроки:

— пароль, що базується на слові або комбінації літер та символів;

— атрибут базується на унікальному пристрої (магнітні картки, смарт-картки, USB-пристрої тощо);

— біометричний, базується на анатомії людини або поведінці людини.

Було проаналізовано поточний стан сучасних систем контролю та управління доступом. За даними IDC, системи ідентифікації та контролю доступу складають 59% від загального ринку засобів безпеки 1Т. Дослідження, проведене у 2017 році Інститутом досліджень комп'ютерних злочинів та безпеки CSI/FBI, показало, що 51% компаній використовують методи паролів для надання доступу користувачам, 35% - атрибутивні методи та лише 20% - біометричні методи. Згідно з соціологічним опитуванням, проведеним Unisys, 68% клієнтів у всьому світі віддають перевагу банкам, платіжним системам та державним установам використовувати біометрію для ідентифікації осіб замість паролів та карток. AtSecurity провела опитування європейських IT-фахівців на початку 2023 року щодо технологій авторизації, що використовуються в банківській галузі (рис. 1.1).

Низька популярність біометричних методів пов'язана з високою вартістю та складністю створення біометричних систем захисту інформації.

На основі аналізу вищезазначених фактів було зроблено висновок, що системи контролю та управління доступом на основі паролів та атрибутів є найпоширенішими. Однак вони мають кілька суттєвих недоліків.

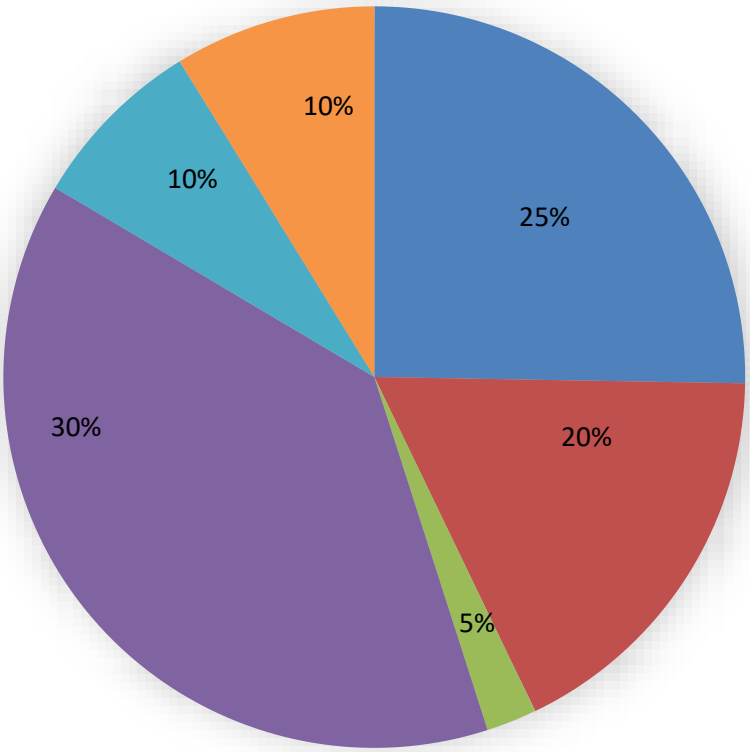


Рисунок 1.1 — Використовувані в європейських банках технологій авторизації за даними опитування AtSecuri

1.3 Переваги та недоліки парольних систем контролю доступом до інформації

Системи контролю та управління доступом за паролями є найпоширенішими засобами захисту даних. Популярність пояснюється тим, що ця система простіше у використанні, ніж інші, але рівень безпеки таких систем низький через наявність низки недоліків:

— можливість підбору пароля;

— недотримання користувачем інструкцій щодо створення надійного пароля (недбалість у процедурі вибору пароля);

— наявність та доступність вільного доступу до спеціалізованих програм для вибору та злому паролів;

— пароль може бути отриманий методом грубої сили проти користувача;

— пароль може бути вкрадений, тобто він може бути збережений, коли його вводить власник.

Було проведено дослідження надійності використання методів виявлення та розпізнавання паролів. Нижче наведено деякі встановлені дані, що підтверджують недоліки сучасних методів контролю та управління.

Далі приведена статистика згідно зі звітом RSA Research Lab:

— 25% користувачів комп'ютерів зберігають свої комп'ютерні дані у звичайному тексті;

— 22% використовують мобільні телефони для відстеження своїх пристроїв;

— 18% ведуть облік своїх рахунків на папері.

Дійсно, експерти (hakykatdanam-id.ua) наводять приклад зберігання даних користувачів в одній з банківських установ, яка оцінила фінансовий стан компанії. Для легкого доступу до своїх додатків на різних платформах банківських систем багато співробітників використовували клавіатури для зберігання інформації замість використання клавіатури.На основі результатів дослідження методів розпізнавання паролів робиться висновок, що можна використовувати методи генерації паролів,посилаючись на право присутності особи, уповноваженої законом. Регулярне введення пароля для підтвердження авторизації під час роботи перешкоджає користувачеві виконувати поставлені завдання. неможливо визначити мінімальну та максимальну довжину пароля.

Дослідження поведінкового розуміння за допомогою іншого інструменту призводить до кращого збереження, ніж стандартний інструмент. Однак, існує кілька ризиків, пов'язаних з моніторингом поведінки за допомогою систем, що відрізняються від «пасивних» та «активних» систем:

— вразливість до крадіжки особистих даних користувачів;

— вимога щодо магнітних карток, смарт-карток тощо;

— можливість створення унікальної копії;

— унікальна креативність.

Існує спеціальний механізм, який запобігає несанкціонованому доступу до контролера, якщо контролер вилучено (спеціально розроблений USB-флеш-

накопичувач). Виробники рекомендують користувачеві брати USB-кабель із собою, коли він залишає робоче місце. У цьому випадку комп'ютер автоматично блокується, доки ключ не буде використано знову. Він використовує алгоритм шифрування AES-256 та захищений PIN-кодом. Людський фактор є основним недоліком цих систем, а саме захист від видавання себе за законного користувача, наприклад, користувач може забути вилучити USB-кабель та залишити робоче місце.

1.4 Методи ідентифікації

Було проведено дослідження біометричних систем контролю та управління доступом. Біометричні системи контролю доступу базуються на розпізнаванні фізіологічних та поведінкових характеристик людини. Ці системи поділяються на групи залежно від типу поведінки людини, що розпізнається (рис. 1.2).

У процесі автентифікації зразок, представлений користувачем, порівнюється з раніше створеним шаблоном з урахуванням деяких помилок. Точність та надійність системи залежить від необхідного оптимального співвідношення помилок хибного прийняття (FAR) та помилок хибного відхилення (FRR).

Було проведено дослідження та аналіз існуючих та активно діючих біометричних систем ідентифікації та розпізнавання користувачів, а також оцінено можливість їх застосування для ідентифікації уповноваженого легального користувача. Результати дослідження представлені в таблиці 1.1.

На основі результатів аналізу було зроблено висновок, що біометричні системи розпізнавання відбитків пальців, райдужних оболонок ока, геометрії руки, вен долоні та геометрії обличчя мало корисні для ідентифікації легального оператора, оскільки мають суттєві обмеження у використанні та вимагають певних умов під час перевірки характеристик сканера. Біометричні системи розпізнавання сітківки не дозволяють постійно контролювати особу

користувача, оскільки для сканування сітківки потрібні певні умови.

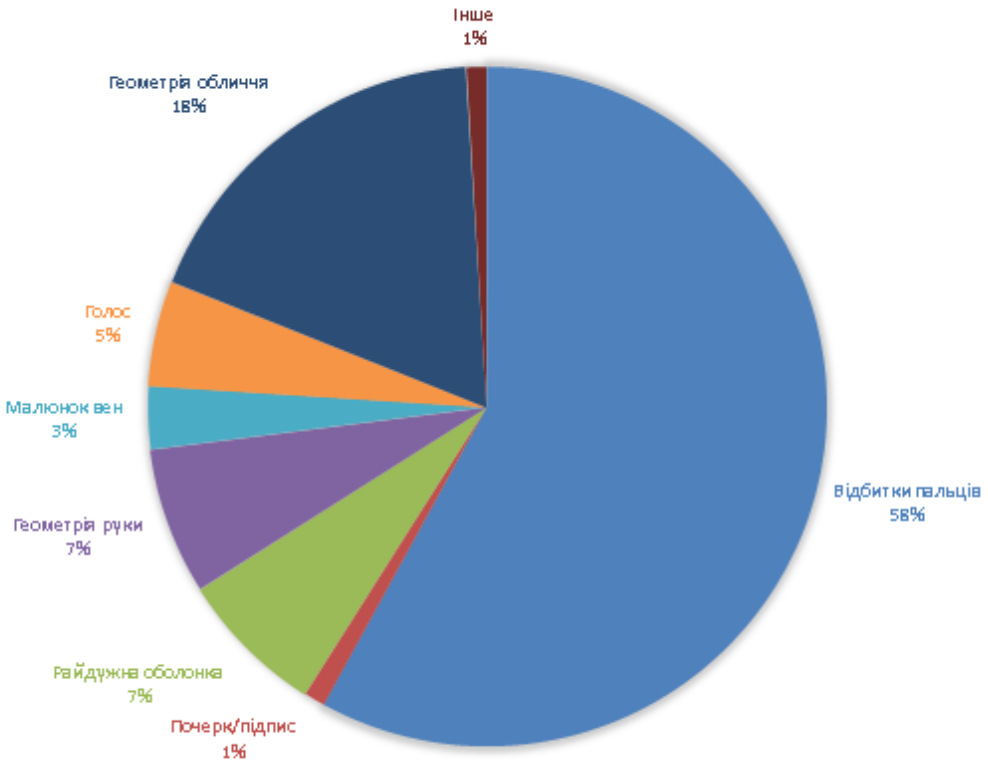


Рисунок 1.2 — Біометричні технології, експлуатовані в промислових масштабах

Таким чином, було зроблено висновок, що для визначення місцезнаходження легітимного користувача необхідно використовувати біометричні параметри, які виникають, коли користувач виконує завдання, безпосередньо пов'язані з його роботою. Найчастіше користувач працює за допомогою миші та набирає текст на клавіатурі. Виходячи з цього припущення, було зроблено висновок, що найзручнішим способом забезпечення процедури безперервного прихованого моніторингу з метою визначення місцезнаходження користувача є почерк на клавіатурі — біометрична характеристика динамічної поведінки людини. Таблиця 1.1 — Аналіз основних біометричних СКУД

Біометричний параметр	Ціна пристро ю (дол.)	Імовірність помилки FAR,%	Переваги	Недоліки	Можливість подати заявку на посаду уповноваженого оператора
Відбиток пальця	100	0.001	Надійність. 1. Стабільність параметрів. 2. Малий ідентифікаційний код. 3. Компактний зчитувач. 4. Низька вартість. 5. Використання додаткових датчиків (температури, живлення, тиску).	1. Безпосередній зв'язок з пристроєм. 2. Складність алгоритмів. 3. Пошкодження папілярного візерунка пальців ускладнює ідентифікацію. 4. Якість зчитування суттєво залежить від стану шкіри. 5. Можливість підробки відбитка пальця.	Сканери відбитків пальців впроваджені в миші, клавіатури та корпуси ноутбуків, але більшість із них служать лише для полегшення процесу авторизації (наприклад, миша BioLink U-Match від BioLink Technologies). Застосування для визначення місцезнаходження оператора неминуче є складними. постійного безпосередньог о контакту пальців зі зчитувачем, що є неможливим.

Продовження таблиці 1.1

Біометричний параметр	Ціна пристрою (дол.)	Імовірність помилки FAR,%	Переваги	Недоліки	Можливість подати заявку на посаду уповноваженого оператора
Райдужна оболонка ока	> 500	0.00001	1. Стабільність параметр 2. Висока точність. 3. Надзвичайно важко підробити. 4. Безконтактні пристрої. 5. Висока швидкість. Сканер можна проводити на відстані кількох сантиметрів 6. кількох метрів.	1. Складність алгоритмів. 2. Висока вартість. 3. Низька доступність високоякісних рішень.	Ускладнений необхідністю для оператора постійно шукати камеру з малими кутами сканування, пристрій EyeLock від Hoyos Group був розроблений для забезпечення процесу авторизації.
Геометрія руки	> 600	0.2	1.Стійкість параметра. 2.Простота алгоритмів.	.1. Пряме підключення до пристрою. .2. Незручна процедура сканування. .3. Великі розміри зчитувача.	Безперервний моніторинг неможливий, якщо руки оператора знаходяться поза зоною дії сканера.

Продовження таблиці 1.1

Біометричний параметр	Ціна пристрою (дол.)	Імовірність помилки FAR,%	Переваги	Недоліки	Можливість застосування для виявлення підміни авторизованого оператора
Біометричний параметр	Ціна пристрою (дол.)	Імовірність помилки FAR,%	Переваги	Недоліки	Можливість подати заявку на посаду уповноваженого оператора
Сітківка ока	4000	0.000001	1. Параметр стає постійним з часом. 2. Висока точність. 3. Відсутність прямого контакту з	1. Складність читання. 2. Складність алгоритмів. 3. Високий час обробки шаблону. 4. Висока вартість системи.	Відсутня в зв'язку з необхідністю виконання
Геометрія особи	>100	От 5 до 0.0047	1. Можливість безперервної перевірки. 2. Пристрої, що не потребують прямого контакту. 3. Низька вартість.	1.Залежність від умов освітлення, положення голови. 2. Залежність від виразу обличчя. 3. Залежність від перешкод (окуляри, головний убір, зміна зачіски).	Його можна використовувати для постійного моніторингу плинності кадрів операторів, але існує кілька обмежень через недоліки методу. Основна програма, процес авторизації,

Вени руки	>300	0.0008	1. Висока точність. 2. Відсутність прямого підключення до пристрою. 3. Приховані функції з	.1.Чутливість сканера до природного та штучного освітлення. .2. Специфічність залежить від стану кровоносної системи людини.	Безперервний моніторинг неможливий, якщо руки оператора знаходяться поза зоною дії сканера. Біометричний зчитувач вен долоні PalmVein, що пропонується компанією Fujitsu, використовуєтьс я для ідентифікації оператора під час авторизації.

1.5 Галузі застосування біометричної ідентифікації особистості

Біометрична ідентифікація особи використовується в широкому спектрі діяльності людини.

До найважливіших сфер належать:

— паспорти, верифікація громадян, що в'їжджають до країни;

— системи ідентифікації корпоративних співробітників;

— системи безпеки;

— платіжні системи;

— медичні системи;

— освіта;

— ігри;

— недоліки методів цифрової ідентифікації.

Біометричні технології вдосконалюються швидкими темпами. Надійність зростає, а вартість традиційних технологій знижується: розпізнавання відбитків

пальців та райдужної оболонки ока. Поряд зі старими технологіями з'являються й нові. Наприклад, розпізнавання за тривимірним зображенням людини може докорінно змінити ситуацію на біометричному ринку в майбутньому.

Звичайно, головною подією в галузі біометрії стане масове впровадження цих технологій для паспортних та візових документів. Ця подія призведе не лише до технологічних змін та вдосконалення систем і пристроїв на ринку, але й до значних змін у житті людей.

Зазвичай при класифікації біометричних технологій виділяють дві групи за типом використовуваних біометричних параметрів. Перша група систем використовує статичні біометричні параметри: відбитки пальців, геометрію руки, сітківку ока тощо. Друга група систем використовує динамічні параметри для ідентифікації: підпис або рукописне ключове слово, голос тощо, динаміку відтворення.

Нижче наведнго приблизний розподіл, використання та попит на технології біометричної ідентифікації на ринку в останні роки (рис. 1.3). У багатьох джерелах такі дані суттєво різняться (різниця становить близько 15-20 відсотків).

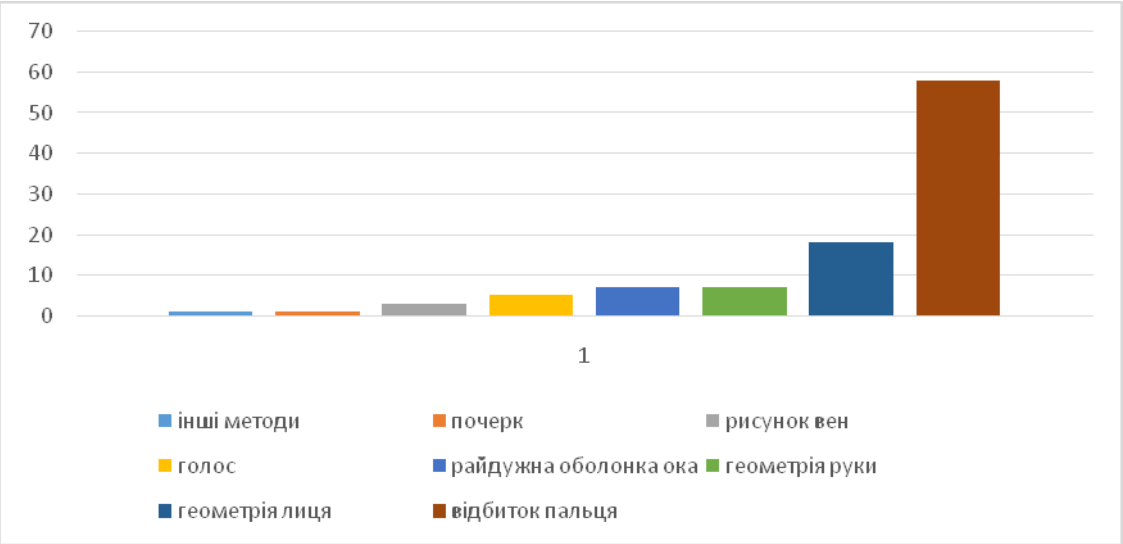


Рисунок 1. 3 — Розподіл у відсотках потреби ринку у технологіях біометричної ідентифікації.

Для біометричної ідентифікації особи використовуються сканери різних пристроїв, що зчитують задані ознаки людини. Наразі поняття «біометричний алгоритм» та «біометричний сканер» не обов'язково пов'язані одне з одним. Найбільша розбіжність виробників сканерів та розробників програмного забезпечення досягнута на ринку біометрії відбитків пальців. Найменша на ринку 3D-сканерів обличчя. Чим більше ви обираєте - тим більше тема розробляється та доводиться до досконалості. Різні сканери мають різні функціональні можливості. В основному, це набір тестів для перевірки, чи є біометричний об'єкт підробленим чи ні.

Нижче подано існуючі види сканерів біометричних характеристик (рис. 1.4).

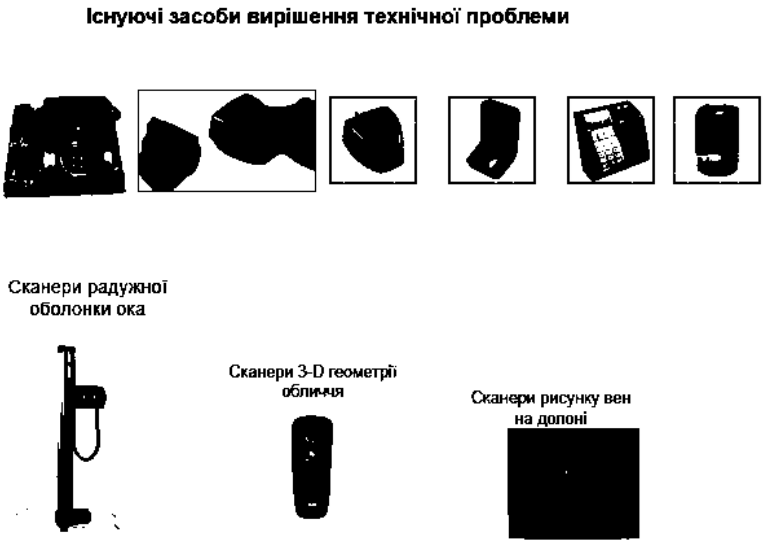


Рисунок 1.4 — Сучасні сканери біометричних характеристик.

1.6 Класифікація методів біометричної ідентифікації особистості

Існуючі процеси біометричної ідентифікації умовно можна поділити на два класи [7].

Перший клас — це статичні методи, засновані на аналізі статичних зображень. Другий клас — це методи ідентифікації особи, що аналізують

динаміку відтворення складних свідомих дій. До них належать, наприклад, методи розпізнавання за голосом, підписом та почерком на клавіатурі.

Для біометричної ідентифікації можуть бути використані різні ознаки та характеристики людини (рис.1. 5).

Найсучаснішими технологіями сьогодні є відбитки пальців, райдужні оболонки ока та двовимірні (плоскі, як на фотографії) зображення людини. Крім того, дактилоскопічна ідентифікація в кілька разів перевершує інші технології за зручністю використання та матеріалодоступністю.

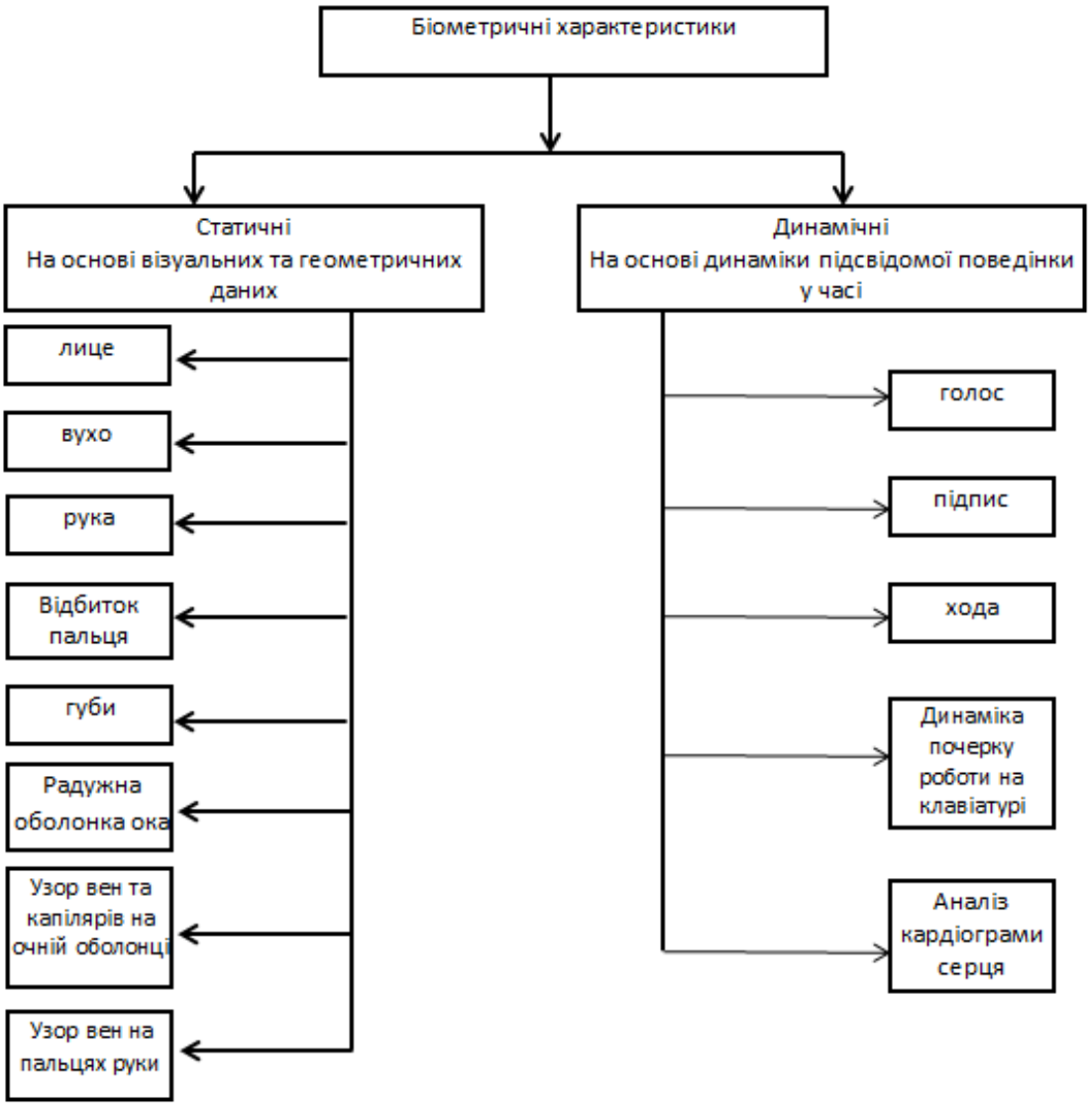


Рисунок 1.5 — Біометричні характеристики і риси людини.

1.6.1 Динамічні методи біометричної ідентифікації

Методи динамічної біометричної ідентифікації базуються на поведінкових характеристиках людини, тобто на особливостях, властивих свідомим діям під час будь-якої дії. Динамічна біометрична ідентифікація людини базується на аналізі підписів, почерку на клавіатурі та інших ознак навмисно контрольованих складних дій.

Системи динамічної ідентифікації здатні оцінювати поточний психічний стан людини паралельно з самою особою. Тому динамічні методи вважаються психологічними. Розглянемо найпопулярніші методи динамічної ідентифікації:

аналіз почерку: для цього типу ідентифікації особи використовується підпис, аналізується сам підпис та динамічні характеристики почерку;

аналіз почерку на клавіатурі: основною характеристикою, призначеною для ідентифікації особи, є динаміка набору кодового слова [8-10];

аналіз голосу: аналізуються різні комбінації частоти голосу та статистичних характеристик [11-13], такі системи ідентифікації є дешевими та інтенсивно розробляються, так як поштовхом до їх розвитку є потреба в таких галузях, як криміналістика, біометричні дослідження, тестування голосу водія та пасажира, а також обмеження потужності за допомогою голосової біометрії.

Крім того слід згадати про менш застосовувані методи біометричної ідентифікації, як аналіз енцефалограм та кардіограм, мікровібрацію пальців, мікрорухи, рухи губ людини.

Під час електроенцефалографічних досліджень визначається площа та інтенсивність електричних імпульсів, що тривають кілька мілісекунд у мозку пацієнта [14, 15]. Система контролює електричну активність мозку та бездротовим способом передає інформацію на комп'ютер. Потім формується цифровий портрет користувача. Під час подальшого аналізу електроенцефалограма витягується та порівнюється з раніше записаною. Комп'ютер робить висновки про особу.

Щодо мікровібрації пальців, то дослідники прогнозують, що вона буде унікальною для кожного користувача, і відповідно, можна отримати унікальний підпис, який буде дуже важко підробити.

Про мікрорухи Нью-Йоркський технологічний інститут розробляє нову біометричну систему ідентифікації, засновану на аналізі мікрорухів та вібрацій руки, що тримає смартфон, яку можна використовувати для ідентифікації користувача. Вивчаються рухи людини під час утримання телефону та паузи між цими рухами під час перегляду контенту.

Рухи губ людини передбачають перевірку деяких параметрів, що характеризують рух губ даної людини. Самонавчальна комп'ютерна система ідентифікує та запам'ятовує візуальні підказки, характерні для конкретної людини, яка вимовляє певне слово.

Інші методи, що використовуються, включають, наприклад, тривимірне моделювання руху. Технологія поєднує зображення, отримані системою відеоспостереження, та фотограмметричне програмне забезпечення PhotoModeler. Метод фотограмметричного вимірювання створює точні 3D-моделі та точні вимірювання розмірів тіла на основі зображень з камер спостереження. Анімація моделей людських ребер дозволяє визначити, чи відповідають тіло та рухи підозрюваного рухам тіла та рухам зловмисника. Програмне забезпечення PhotoModeler дозволяє знаходити та карати злочинців.

1.6.2 Характеристика динамічних методів біометричної аутентифікації

Для методів цього класу характерна більш легка реалізація, аніж реалізація біометричних систем за статичними методами, але водночас динамічні біометричні методи не дають такої точності, як статичні біометричні методи. Характеристику динамічних біометричних методів наведено в таблиці 1.2 [4].

Таблиця 1.2 — Характеристики динамічних біометричних методів

Хар-ки методу / Мет. аутент.	Відносна складність реалізації	Відносна собівартість	Відносна точність
голосом	середня	середня	середня
За клавіатурним почерком	середня	низька	низька
За підписом	складна	висока	середня
За динамікою роботи з комп’ютерною мишею	складна	середня	середня

Огляд характеристик проводився з урахуванням можливості розробки прототипів засобів біометричної ідентифікації та аутентифікації.

1.7 Аналіз методу аутентифікації за клавіатурним почерком

Метод розпізнавання рукописного введення на клавіатурі характеризується наявністю режиму навчання. Користувач може пройти автентифікацію, а потім набрати певний текст. Програма зчитує та зберігає динамічні характеристики користувача. Таким чином, після навчання система збирає дані про час між натисканнями клавіш та паузами для кожного відомого користувача.

Існує три методи розпізнавання рукописного введення на клавіатурі, аналіз алгоритмів наведено в таблиці 1.3:

Таблиця 1.3 — Характеристики алгоритмів аналізу клавіатурного почерку

Алгоритм / Хар-ки алгоритму	Фіксація вихідних даних під час введення паролю	Фіксація вихідних даних під час введення текстового фрагмента	Фіксація вихідних даних під час прихованого моніторингу
Відносна вимогливість до обчислювальної потужності	низька	низька	велика
Відносна точність	низька	середня	висока

Відносна складність реалізації	низька	низька	висока

Перший метод реалізації розпізнавання рукописного тексту на клавіатурі має перевагу в швидкості, оскільки вводиться певний пароль, відомий лише користувачеві. У цьому випадку точність розпізнавання низька, залежно від довжини пароля.

Другий метод реалізації розпізнавання рукописного тексту на клавіатурі має перевагу над першим методом у точності, але користувач повинен вводити фрагменти тексту через незручності у використанні системи.

Третій метод реалізації розпізнавання рукописного тексту на клавіатурі має більшу перевагу в точності, ніж вищезазначений, але вимагає більшої обчислювальної потужності для секретного контролю, особливо якщо використовується складна математична модель статистичної обробки даних (частково вирішується періодичним секретним контролем).

Розроблені засоби виявлення та розпізнавання базуються на алгоритмах другої групи.

Слід зазначити, що всі вищезазначені методи розпізнавання рукописного тексту на клавіатурі діють лише тоді, коли створено рукописний текст користувача на клавіатурі. Користувачі без створеного рукописного тексту на клавіатурі є дуже поширеними, що ускладнює ідентифікацію та розпізнавання особи.

Другий етап після фази навчання системи: ідентифікація або верифікація. На цьому етапі система накопичила достатньо інформації про почерк співробітників організації, тому цю інформацію можна використовувати для підвищення надійності автентифікації.

Порівняння характеристик почерку на клавіатурі можна проводити за допомогою ймовірнісних статистичних методів та нейронних мереж. Вважається, що методи, засновані на використанні нейронних мереж, можуть забезпечити більшу точність. Водночас вони вимагають великої обчислювальної потужності. Можуть виникнути дві додаткові проблеми. Перша полягає в тому,

що розробка такої системи може дещо затриматися. Друга пов'язана з неможливістю забезпечити систему навчальними вибірками для всіх «сторонніх» користувачів.

Ймовірнісно-статистичні методи передбачають обчислення математичного очікування вибірки, а також порівняння отриманих значень динамічних характеристик з посиланнями для заявленого користувача [5]. Одним із способів підвищення точності алгоритму є регулярне оновлення посилання для успішно автентифікованого користувача. Це гарантуватиме, що посилання не застаріє та завжди відповідатиме поточним характеристикам набору тексту користувача.

1.8 Огляд існуючих систем прихованого клавіатурного моніторингу

Витоки аналізу клавіатурного почерку сягають часів широкого поширення радіозв'язку за допомогою азбуки Морзе. Досвідченого радиста, на відміну від новачка, впізнають за швидкістю, стилем та якістю передачі сигналу. Так само, як меломан може впізнати виконавця пісні на слух. Приблизно ті ж принципи використовуються для розпізнавання людини, яка працює на клавіатурі комп'ютера.

Безкоштовна програма "Keyboard Handwriting 1.0". Вона призначена для розрахунку різних характеристик клавіатурного почерку: швидкості введення символів, швидкості натискання, відсотка помилок. Недоліком є те, що деякі користувачі не зберігають інформацію про свій клавіатурний почерк, тому немає можливості порівняти їх для розпізнавання користувачами.

Розпізнавання за допомогою клавіатурного почерку має ряд переваг і недоліків. До переваг належать:

Стабільність клавіатурного почерку конкретного користувача, що дозволяє впевненіше ідентифікувати користувача, який працює з клавіатурою;

Низька вартість впровадження системи розпізнавання;

Можливість контролювати доступ співробітника до ресурсів та фізичний стан.

До недоліка методу належить: використання можливе лише для ідентифікації користувачів з клавіатурним почерком.

Можливості аналізу рукописного введення на клавіатурі дозволяють вирішити такі проблеми:

— моніторинг фізичного стану користувачів;

— уникнення використання паролів;

— надання користувачам простішого способу входу в мережу.

Крім того, наразі це єдина технологія, яку можна використовувати для двох цілей:

— ідентифікація користувача, який стверджує, що увійшов у комп'ютерну систему;

— здійснення таємного моніторингу клавіатури працюючих користувачів.

Системи, що вирішують ці проблеми, відрізняються тим, що в першому випадку особа користувача ідентифікується за короткою парольною фразою, а в другому випадку – за випадковим текстом.

2 МЕХАНІЗМИ РОЗПІЗНАВАННЯ КЛВІАТУРНОГО ПОЧЕРКУ

2.1 Аналіз клавіатурного почерку в процесах аутентифікації, ідентифікації та виявлення підміни користувача

На основі аналізу вищезазначених досліджень пропонується розглядати аналіз почерку на клавіатурі для автентифікації, розпізнавання та ідентифікації користувача.

На основі аналізу цих досліджень рекомендується вважати почерк на клавіатурі індивідуальним та унікальним. Румельхарт і Норман розробили комп'ютерне моделювання користувача, який працює з відеокартами. Вони змоделювали, коли потрібно було натиснути клавішу та коли знову виникала помилка під час набору тексту. Моделі Купера, Солтхауса, Румельхарта та Нормана були першими моделями, розробленими для аналізу структури та властивостей рукописного тексту, створеного користувачем.

Коли користувач друкує, він переживає три події: натискання, утримання та відпускання клавіші. На основі того, як часто використовуються клавіші та коли вони утримуються, розраховується час написання. Наступні характеристики відрізняються від рукописного тексту на клавіатурі, який використовується для ідентифікації користувача: час, що минув між натисканнями клавіш, тобто час від натискання однієї клавіші до натискання наступної клавіші або від першого відпускання однієї клавіші до наступної. Використання цієї методики вимагає тривалого збору статистичних даних. Для об'єднання даних між 33 клавішами з 30 елементів, що відповідають російським літерам, потрібно 32670 одиниць вхідних даних. Тому цей відбиток пальця не може бути використаний для визначення місцезнаходження легітимного користувача. Коли використовуються біграми (наприклад, "АА", "ОЕ", "ЯЯ"), триграми (наприклад, "ААА", "МАМ", "ЭЮЯ"), тобто час від першого натискання до отримання останньої літери N-грами. Цей метод аналізу, як і раніше, вимагає збору великої кількості статистичних даних. Як результат, цієї ознаки недостатньо для виявлення стану користувача. Ступінь часу утримання

відповідає кількості натисканих користувачем клавіш, тобто кількість літер алфавіту відповідає ступеню часу утримання клавіш. Такий тип почерку дозволяє нам планувати періодичний моніторинг стану користувача на приватній клавіатурі для виявлення змін. Стиль, що використовується під час набору тексту, вимагає додавання датчиків (по одному на кожну клавішу) на клавіатурі. Це призводить до збільшення обчислювальної складності, збільшення експлуатаційних витрат та збільшення зносу обладнання. Швидкість, тобто кількість натискань, які користувач вводить за певний час, та якість введення залежать від когнітивного стану користувача та часто можуть змінюватися. Це ускладнює використання цих технологій для відстеження місцезнаходження легітимного користувача. Дійсно, функцію θ(t), яка описує шаблон набору тексту користувачем, можна розглядати як:

$$\vartheta(t) = \gamma(t)+\Theta(t)+\lambda(t) \text{ , де} \qquad (2.1)$$

γ(t) — складова, що характеризує підсвідомі процеси мислення при наборі тексту;

Θ(t) — складова свідомих процесів мислення;

λ(t) — механічні характеристики клавіатури, що впливають на процес набору тексту.

Головним завданням біометричної системи ідентифікації користувача на основі шаблону натискання клавіш є виділення та вдосконалення функції θ(t), яка визначає початкову інформацію, що підлягає ідентифікації після моменту натискання клавіші. Для цього компоненти Θ(t) та λ(t) необхідно поділити на перший компонент θ(t). Оскільки неможливо створити роботизовану симуляцію руху людини під час набору тексту, одним із прийнятних підходів є збір статистики щодо почерку великої кількості користувачів. Здатність користувача контролювати довжину ключового слова є більш послідовною характеристикою досвіду набору тексту користувачем, ніж час між

натисканнями клавіш, який збільшується зі збільшенням довжини натискання клавіші. Це пояснюється тим, що натискання клавіші на клавіатурі є справді емоційним досвідом. Цей робочий процес не змінюється для більшості користувачів, навіть якщо вони досвідчені та знайомі з клавіатурою. Це призводить до більш точної оцінки компонента γ(t) на основі часу, який користувач утримує клавіші під час набору тексту. Час утримання клавіші розраховується за допомогою рівняння (2.2):

$$T_i^{\text{утр.кл.}} = T_i^{\text{відп.кл.}} - T_i^{\text{натиск.кл.}} \quad \text{де} \qquad (2.2)$$

$T_i^{\text{утр.кл.}}$ – час утримання клавіші;

$T_i^{\text{відп.кл.}}$ – час відпускання клавіші;

$T_i^{\text{натиск.кл.}}$ – час натискання клавіші.

За підсумками аналізу характеристик клавіатурного почерку запропоновано використовувати час утримання клавіш в процесі виявлення підміни законного користувача. У шаблон почерку користувача запропоновано зберігати усереднені значення часу утримання клавіш. Маючи такий шаблон, стає можливо ідентифікувати користувача ключової системи. Далі наведено аналіз відомих методів ідентифікації і аутентифікації користувачів за клавіатурним почерком: статистичних методів, методів заснованих на застосуванні нейронних мереж, розпізнаванні образів і генетичних алгоритмах.

Статистичні методи полягають в обчисленні відхилень характеристик поточного почерку користувача, який претендує на доступ до ІС і характеристик почерку в шаблоні, збереженого в системі для даного користувача. Для порівняння можуть використовуватися t-тести, Евклідова відстань, Хеммінгово відстань та інші. Joyce і Gupta використовуючи

статистичні методи отримання точності аутентифікації користувача досягли FAR 0.25% і FRR 16.36%. У своїй роботі вони використовували Хеммінгову відстань (2.3) і відстань Махаланобіса (2.4):

$$M = \sum_{i=1}^{N} (|A_i| - |B_i|) \tag{2.3}$$

$$M = \sqrt{\sum_{i=1}^{N} \frac{(A_i - B_i)^2}{\sigma_i^2}} \tag{2.4}$$

i — номер клавіші;

N — кількість аналізованих клавіш;

A_i — тимчасова характеристика для клавіші з шаблону оператора, який претендує на доступ;

B_i — тимчасова характеристика для клавіші з шаблону, що зберігається в базі шаблонів і відповідного оператору;

σ — середньоквадратичне відхилення A_i від B_i.

Guven і Sogukpinar базуючись на векторному аналізі досягли точності ідентифікації оператора в 95%. Аналіз робіт зазначених дослідників дозволив зробити висновок, що головною проблемою статистичних методів є недолік даних на стадії навчання, тобто при отриманні шаблону почерку оператора.

Метод заснований на нейронних мережах вперше був застосований Obaidat і Macchiarolo для аутентифікації і ідентифікації користувачів за часом між натисканнями клавіш. Вони досягли точності ідентифікації оператора в 96.8%, використовуючи нейронну мережу, засновану на сумі творів. Yong та його колеги запропонували використовувати динамічну нейронну мережу. За

аналізом даних досліджень зроблено висновок про те, що головна перевага нейронних мереж полягає в тому, що вони можуть обробляти відразу декілька параметрів почерку. Виділено основні недоліки застосування нейронних мереж при розпізнаванні клавіатурного почерку: потрібно чимало часу для процедур навчання та аутентифікації, присутність ситуацій, коли нейронна мережа не може навчиться через особливості вхідної вибірки. Так як даний метод використовується тільки в якості «чорного ящика», неможливо визначення достатнього для отримання шаблону почерку і подальшої успішної роботи обсягу і складу вхідної вибірки. Також, у разі додавання шаблону нового користувача до системи доведеться перенавчати всю нейронну мережу.

Для методу розпізнавання образів, Giot та його колеги запропонували використовувати метод опорних векторів для розпізнавання клавіатурного почерку. Вони досягли рівня ідентифікації в 95%. Виявлено головна перевага даного методу – висока точність, яка призведена ігноруванням помилок і похибок вимірювань часу утримання клавіш. Недоліком методу є те, що ідентифікація проводиться не за всіма шаблонами, а лише з тієї частини шаблонів, яка знаходиться на кордонах.

Revett та інші використовуючи генетичні алгоритми досягли ймовірності виникнення помилок FAR в 0.43% і FRR в 4.75%. Виявлено основна перевага використання генетичних алгоритмів – вони можуть легко взаємодіяти з великими базами даних та обробляти багатовимірні, недиференціальні, безперервні і непараметричні дані. Виділено головні недоліки генетичних алгоритмів: висока трудомісткість, що обмежує сферу застосування, низька стійкість до відхилень тимчасових характеристик почерку, даний метод не гарантує знаходження оптимального рішення.

2.2 Реалізація механізмів систем постійного клавіатурного

моніторингу з метою виявлення підміни користувача

На основі зробленого аналізу пропонується наступна архітектура біометричної підсистеми виявлення підміни законного користувача (рисунок 2.1), що забезпечує процес отримання шаблону почерку і порівняння почерків.

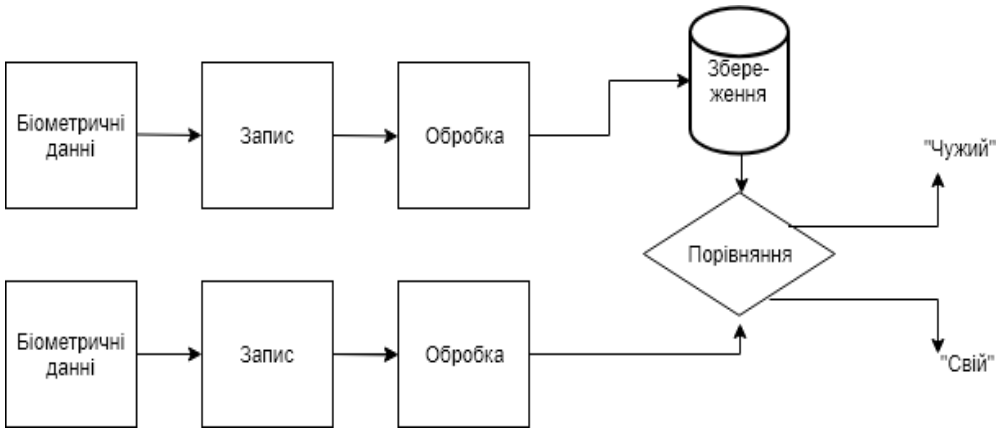


Рисунок 2.1 — Спрощена архітектура біометричної системи виявлення підміни законного оператора

Блок отримання і запису клавіатурного почерку користувача відповідає за отримання тимчасових міток подій натискання і відпускання клавіш, та зазначає до якої клавіші відносяться ці події. Для отримання часу виникнення подій використовується таймер. Даний блок містить так само фільтр довгих натискань на клавіші. Важливим моментом є точність визначення моменту виникнення подій клавіатури. Отже, системи повинні бути зроблені стійкими до похибок вибірки часу.

Блок обробки вибірки подій клавіатури відповідає за обчислення усереднених значень часу утримання клавіш.

Блок зберігання клавіатурного почерку дозволяє зберегти шаблонні значення клавіатурного почерку користувачів в базу шаблонів.

Блок порівняння поточного клавіатурного почерку і шаблонного служить для порівняння почерків і прийняття рішення про аутентифікації і ідентифікації користувача за результатами порівняння.

2.3 Математична модель часу утримання клавіш

Аналіз клавіатурного почерку ґрунтуються на припущенні, що клавіатурний почерк представляється у вигляді усереднених значень подій клавіатури. У системах Microsoft Windows виділяють три види подій клавіатури:

Подія KeyDown, яка відбувається один раз. Спрацьовує під час натискання фізичної клавіші. Подія нижчого рівня – реагує на натискання будь-якої клавіші на клавіатурі. Повертає код натиснутою клавіші.

Подія KeyUp, яка виникає один раз після того, як користувач відпускає фізичну клавішу. В усьому іншому подія аналогічна до KeyDown.

Подія KeyPress, яка може виникати кілька разів, коли користувач утримує натиснуту клавішу. Ця подія виникає при натисканні клавіші, що призводить до введення знаку.

У системах розпізнавання клавіатурного почерку статистичними даними є значення часу подій клавіатури. Обраною ознакою клавіатурного почерку є час утримання клавіш, яке відповідає часовому інтервалу між подіями KeyDown(A) і KeyUp(A), де A — одна з клавіш клавіатури. У зв'язку з використанням даного методу необхідний збір статистики, що складається з вибірки тимчасових значень, де елементом вибірки буде час утримання клавіші.

У ймовірно-статистичному формулюванні виникає необхідність побудови середньостатистичних шаблонів на основі зразків, пред'явлених системі в режимі навчання. При цьому слід враховувати, що на характеристики клавіатурного почерку людини впливає безліч факторів: програмні і апаратні затримки, які теж є випадковими величинами, рух нервового імпульсу по нейронам, час відгуку м'язів людини на сигнал посланий мозком та інші. Значить, на клавіатурний почерк впливає безліч незалежних випадкових величин. Ефект їх складання описується формулою Гауса. Відповідно для зменшення впливу випадкових помилок необхідно провести вимірювання досліджуваної величини кілька разів.

Розглянемо застосування формули Гауса в процесі обробки результатів вимірювання характеристик клавіатурного почерку. Припустимо, що ми вимірюємо час утримання якоїсь конкретної клавіші, позначимо цю величину X. В результаті проведених вимірювань ми отримали вибірку значень величини (2.5):

$$X_1,\ X_2,\ X_3 \ldots X_N \qquad (2.5)$$

Цей ряд значень величини X складе нашу вибірку часу утримання клавіші. По даній вибірці дається оцінка результату вимірювань, тобто усереднене значення ЧУК, в яке прагне укластися користувач при натисканні на клавішу. Величину, яка буде такою оцінкою, ми позначимо $\bar{X}$. Але так як це значення оцінки результатів вимірів не буде являти собою істинного значення вимірюваної величини часу утримання клавіші, необхідно оцінити помилку вимірювання. Припустимо, що ми зуміємо визначити оцінку помилки ΔX. У такому випадку ми можемо записати результат вимірювань у вигляді (2.8):

$$\mu = \bar{X} \pm \Delta X\,. \qquad (2.6)$$

Таким чином, маючи вибірку, необхідно знайти оцінку результату вимірювань $\bar{X}$, його помилку ΔX і надійність P. Це завдання вирішується застосуванням математичної статистики. Запропоновано в якості оцінки результатів вимірювань ЧУК розраховувати середнє значення всіх елементів зібраної для конкретної клавіші вибірки (2.7):

$$\bar{X} = \frac{\sum_{i=1}^{N} X_i}{N} \qquad (2.7)$$

де

N — число вимірювань.

Значить, для вибірки в N вимірювань часу утримання, найбільш імовірним значенням вимірюваної величини буде її середнє арифметичне значення. Отримане середнє значення ЧУК прагне до істинного значення μ вимірюваної величини $\bar{X}$ при збільшенні числа вимірювань, тобто $N \to \infty$.

Середньоквадратичної помилкою середнього арифметичного називається величина:

$$S_{\bar{x}} = \sqrt{\frac{\sum(X - X_i)^2}{N(N-1)}} = \frac{S}{\sqrt{N}} \qquad (2.8)$$

Точність оцінки зростає при збільшенні числа вимірювань. Помилка $S_{\bar{X}}$ дозволяє оцінити точність, з якою розраховано середнє значення ЧУК.

Отже, можна визначити, скільки разів повинна бути натиснута конкретна клавіша, для того щоб зібрати статистику, що характеризує усереднений ЧУК. Відповідно, для того щоб визначити клавіатурний почерк користувача, потрібно зібрати дані про середні значення часу утримання всіх використовуваних клавіш.

2.4 Аналітична модель клавіатурного почерку

Маючи шаблон клавіатурного почерку користувача стає можливо провести його аутентифікацію та ідентифікацію. Для цього необхідно провести процедуру порівняння поточного зразка почерку і збереженого раніше шаблона. Запропоновано використовувати Евклідова відстань для порівняння часу утримання клавіш поточного зразка і шаблону (2.9):

$$M = \sqrt{\sum_{i=1}^{V}(A_i - B_i)^2}\text{, де} \qquad (2.9)$$

M — розраховане значення Евклідової відстані,

V — кількість вибірок часу утримання клавіші, що відповідає кількості аналізованих клавіш,

A_i — час утримання клавіші з поточного зразка клавіатурного почерку користувача, який претендує на доступ,

B_i — час утримання клавіші, що зберігається в шаблоні почерку.

Користувач буде успішно ідентифікований або його особистість буде підтверджена, якщо розраховані значення Евклідова відстані менше встановленого в системі порога доступу. Поріг доступу підбирається в залежності від вимог до розроблюваної системи. Основними вимогами для систем захисту інформації є ймовірності виникнення помилок першого і другого роду.

2.5 Розроблення методу розпізнавання клавіатурного почерку користувача

Пропонується розраховувати почерк на клавіатурі за часом натискання клавіш та відстанню між клавішами. Це дозволить отримати шаблон почерку, який не залежить від набраного тексту та порядку введення символів. Таким чином, з'являється можливість визначити почерк на клавіатурі користувача ключової системи за вільним контрольним текстом. Це дозволяє використовувати метод для задач безперервного секретного моніторингу клавіатури, для визначення місцезнаходження авторизованого легітимного користувача, для визначення відхилень психофізіологічного стану користувача ключової системи від норми.

Основним параметром, який використовується при аналізі клавіатурного почерку, є час між подіями клавіш клавіатури. Ідентифікація користувача будується на аналізі тривалості інтервалів, відповідних кожної

комбінації клавіш Чутливість до натискання клавіш аналізували, припускаючи, що чутливість до натискання клавіш виражається як середнє значення подій натискання клавіш. Microsoft Windows має три варіанти:

Подія KeyDown виникає лише один раз. Вона виникає, коли людину змушують щось робити. Клавіша має реагувати на все, що ви пишете. Відображає код введеного коду.

Подія KeyUp виникає лише один раз, коли користувач відпускає клавішу. В іншому випадку ця поведінка така ж, як і KeyDown.

Подія KeyPress виникає кілька разів, коли користувач натискає клавішу. Це відбувається, коли клавіша натискається і вводиться текст (рис.2.2).

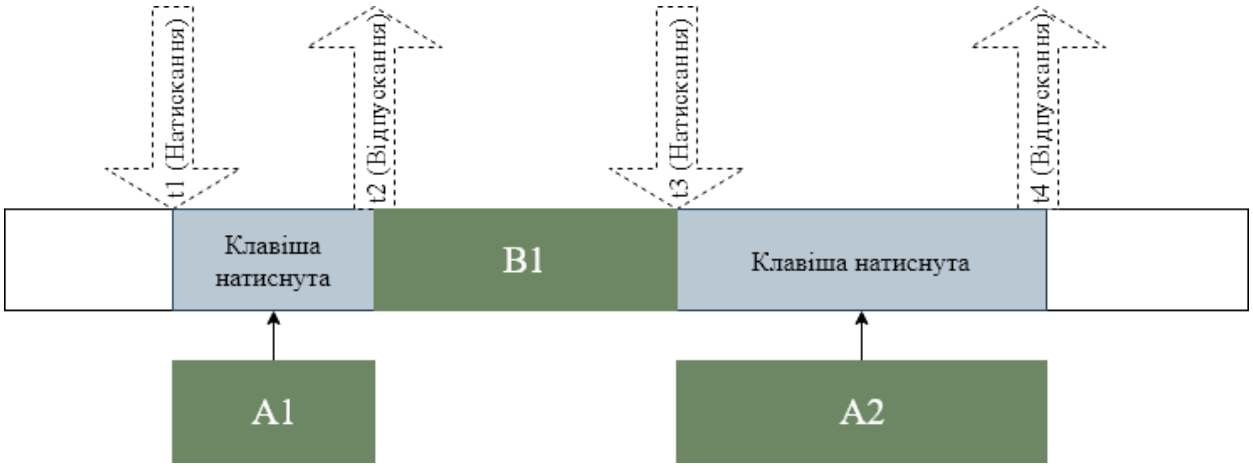


Рисунок 2.2 — Часова діаграма клавіатурного почерку

Для реалізації схеми зміни клавіатурного почерку пропонується використання програмного або апаратного модуля. Можливі такі основні місця вбудовування такого модуля:

— безпосередньо в клавіатуру (програмно-апаратний або апаратний модуль);

— безпосередньо в обробник подій клавіатури операційної системи (програмний модуль);

— між клавіатурою і комп'ютером (апаратний модуль у розриві кабелю).

Вбудовування модуля безпосередньо в клавіатуру вимагає внесення змін у конструкцію клавіатури і, можливо, в її драйвер. Будь-яких принципових переваг, крім візуальної скритності, таке розміщення модуля не несе.

Програмний модуль обробки подій клавіатури не вимагає яких-небудь апаратних компонентів, проте його функціонування залежить від операційної системи. По суті, кожна операційна система вимагає свого програмного модуля. Такий модуль не залежить від того, через який порт підключається клавіатура.

Установка модуля зміни клавіатурного почерку в розрив кабелю дозволяє використовувати його на будь-який ОС. Недоліком же такого рішення є залежність від порту підключення (найбільш часто використовуються PS / 2 або USB). В даній роботі розглянемо програмний модуль.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ

3.1 Сценарій використання системи

На зображенні нижче показано UML-діаграму сценаріїв використання системи ідентифікації на основі рукописного введення з описом кожного випадку використання.

3.1.1 Запис даних у кільцевий стек

Натискання клавіш та події, пов'язані з натисканнями клавіш, використовуються для запису часу. Для цього програма має два обробники:

Sign_OnKeyDown (); — призначений для запису натискань клавіш;

Sign_OnKeyUp (); — створений для реєстрації відпускання клавіші, кільцеві стеки реалізовані як двовимірні масиви KeyPress;

array [1..MAX_KEY_CODE, 1..MAX_SER_LEN] of integer; — масив, в якому зберігається час утримання клавіші;

KeyInt: array [1..MAX_KEY_CODE, 1..MAX_SER_LEN] of integer; — масив, в якому зберігається час перед натисканням клавіші, тобто інтервал між натисканням;

KeyDown: array [1..MAX_KEY_CODE] of TTime; — масив, у котрому зберігається момент натиснення клавіші;

KeyIndex: array [1..MAX_KEY_CODE] of integer; — даний масив використовується як індекс для зберігання серії даних і організації кільцевого стека зберігання;

KeyCount: array [1..MAX_KEY_CODE] of integer; — останній масив, у якому зберігаються лічильники натискань клавіш.

Тривалість натискання клавіші вимірюється наступним чином: коли клавіша натискається, масив KeyDown[] зберігає час, витрачений на натискання цієї клавіші. Коли клавіша відпускається, збережене значення використовується для визначення часу утримання в мілісекундах як різниця між часом натискання та часом утримання. Час утримання зберігається у двовимірному масиві

KeyPress[], де перший вказівник відповідає коду клавіші, а другий - вказівнику кільцевого регістра, що зберігається в масиві KeyIndex[]. Таким чином, можна зберігати кілька виміряних значень часу для кожної клавіші. Кількість фактично виконаних вимірювань зберігається в масиві KeyCount[]. Якщо кількість вимірювань перевищує максимальну ємність стеку, задану константою MAX_SER_LEN, вказівник переміщується на початок масиву. Для вимірювання інтервалів між натисканнями використовується час попереднього натискання клавіші, що зберігається в глобальній змінній “PredPress: TTime”; та час поточного натискання. Результат зберігається у двовимірному масиві KeyInt[], записаному як у масиві KeyPress[]. Щоб запобігти надмірним перервам у наборі даних, які можуть виникнути через якусь зовнішню подію, таку як телефонний дзвінок або повідомлення, перед записом значення воно порівнюється з пороговим значенням, і, якщо воно перевищено, записується фіксоване значення 50 мс.

3.1.2 Отримання шаблону

При створенні однієї з спеціальних подій натиснення клавіш або відпускання клавіш, викликається процедура CalcStatistic; в якій проводяться обчислення середніх величин таймінгів. Для цього перебирається масив KeyCount [] для всіх клавіш, але для обчислення використовуються тільки ті елементи, які відповідають натисненні тих клавіш, які були використані користувачем в поточному сеансі. Для підрахунку середніх арифметичних значень часу утримання кожної клавіші і часу перед натисканням кожної клавіші, тобто пошуку її, використовується найменша величина з двох – або лічильник числа натискань KeyCount [], або розмір кільцевого стека. Результат зберігається в масиви KeyPressOvr [] та KeyIntOvr [], після чого обчислюються ще дві величини: середній час утримання (KeyPressTOvr — характеризує силу натискання на клавіші) і середній час між натисненням (KeyIntTOvr–темп набору тексту), які також беруть участь в ідентифікації (рис.3.1).

Збереження шаблону в базі даних здійснюється за допомогою процедури SaveTiming(), яка приймає тип шаблону як параметр. Існує два типи шаблонів: для пароля та введення тексту. Це пояснюється тим, що ключі в режимі введення пароля та режимі введення тексту різні, тому, якщо для визначення двох процесів використовується лише один тип шаблону, конвергенція буде дуже низькою

Рисунок 3.1 — Отримання шаблону

Дані зберігаються в таблицях "час" та "користувач". Процедура LoadTiming() використовується для завантаження часу поточного користувача;

3.2 Схема бази даних

Схема бази даних, (рис. 4.1), показує таблиці, які зберігають шаблони часу, інформацію про користувача, налаштування програми та інші дані.

Таблиця 4.1 — Опис таблиць бази даних

user	Дані про користувачів: 1. id – ключове поле; 2. login – логін користувача; 3. password – пароль користувача; 4. is_admin – ознака того, що користувач являється адміністратором; 5. is_getident – ознака проходження авторизації; 6. pretime – середній час між натисканням клавіш; 7. holdtime – середній час утримання клавіш;
timing	Шаблон таймінгів: 1. id – ключове поле; 2. key – код клавіши; 3. pretime – середній час між натисканням клавіші; 4. holdtime – середній час утримання клавіші; 5. id_user – користувач; 6. type – тип шаблону 0 – для пароля, 1 – для тексту;
param	Параметри програми: 1. id – ключове поле; 2. k_dev – коефіцієнт максимального відхилення прпорівнянні шаблонів; 3. ValidPassKey – допустимі символи для пароля; 4. PassEnterCount – кількість повторень пароля

Продовження таблиці 4.1 — Опис таблиць бази даних	
data	Дані, що використовуються (набираються) користувачами - щоденники спостережень: 1. id – ключове поле; 2. id_user – користувач; 3. create_date – дата створення запису; 4. caption – заголовок запису; 5. data – вміст запису;
log	Журнал подій: 1. id – ключове поле; 2. event_time – дата події; 3. event_desc – опис події;
testdata	Тестові дані для отримання шаблонів таймінгів набору тексту 1. id – ключове поле; 2. data – текст для набору; 3. order_num – порядковий номер;

Рисунок 3.2 — Схема бази даних

3.4 Огляд та пояснення основних частин коду програми

На початку файлу є секція Const (рис. 3.3) – секція, яка описує таку послідовність:

Each — обсяг статистики для кожного збереженого ключа;

Code — максимальне значення коду;

Log — тип часу запису в журнал;

Text — тип часу запису тексту;

Password — зміна довжини пароля.

```
const
  MAX_SER_LEN = 20;
  MAX_KEY_CODE = 230;
  TT_LOGIN = 0;
  TT_TEXT = 1;
  MIN_PASS_LENGTH = 5;
  VAR_PASS_LENGTH = 3;
```

Рисунок 3.3 — Розділ з описаними константами

Його слід розмістити перед розділом Var, як показано на рисунку 3.4. Ця секція використовується для позначення секції, де оголошуються змінні та типи. Змінні зазвичай оголошуються на початку програми, процедури, функції або модуля.

```
var
  ValidPassKey: string;
  EnterPassCount: integer;
  UserID: integer;
  PredPress: TTime;
  KeyDown : array[1..MAX_KEY_CODE] of TTime;
  KeyIndex: array[1..MAX_KEY_CODE] of integer;
  KeyCount: array[1..MAX_KEY_CODE] of integer;
  KeyPress: array[1..MAX_KEY_CODE,1..MAX_SER_LEN] of integer;
  KeyInt: array[1..MAX_KEY_CODE,1..MAX_SER_LEN] of integer;
  KeyPressOvr: array[1..MAX_KEY_CODE] of integer;
  KeyIntOvr: array[1..MAX_KEY_CODE] of integer;
  KeyPressTOvr: integer;
  KeyIntTOvr: integer;
  UserKeyPressOvr: array[1..MAX_KEY_CODE] of integer;
  UserKeyIntOvr: array[1..MAX_KEY_CODE] of integer;
  UserKeyPressTOvr: integer;
  UserKeyIntTOvr: integer;

procedure frmTiming_OnShow (Sender: TObject; Action: string);
```

Рисунок 3.4 — Секція з оголошенням змінних

Нижче на рисунку 3.5 показано кроки для отримання ключових прес-релізів, на рисунку 3.6 показано кроки для отримання ключових прес-релізів, а на рисунку 3.7 показано кроки для отримання ключових прес-релізів.

```
82  procedure Sign_OnKeyDown (Key: Word);
83  var
84    tmpPressTime:TTime;
85    tmpInterval: integer;
86  begin
87    if (Key >= 1) and (Key <= MAX_KEY_CODE) then
88    begin
89      tmpPressTime := Time();
90      KeyDown[Key] := tmpPressTime;
91      inc( KeyCount[Key] );
92      try
93        tmpInterval := MilliSecondsBetween(tmpPressTime,PredPress);
94      except
95        tmpInterval := 50;
96      end;
97      KeyInt[Key,KeyIndex[Key]] := tmpInterval;
98      PredPress := tmpPressTime;
99    end;
100 end;
```

Рисунок 3.5 — Облік таймінгу зняття сигнатур натискання клавіші

```
105 procedure Sign_OnKeyUp (Key: Word);
106 var
107   tmpInterval: integer;
108 begin
109   if (Key >= 1) and (Key <= MAX_KEY_CODE) then
110   begin
111     tmpInterval := MilliSecondsBetween(Time(),KeyDown[Key]);
112     KeyPress[Key,KeyIndex[Key]] := tmpInterval;
113     inc(KeyIndex[Key]);
114     if KeyIndex[Key] > MAX_SER_LEN then
115       KeyIndex[Key] := 1;
116   end;
117 end;
```

Рисунок 3.6 — Облік таймінгу для зняття сигнатур відпускання клавіші

У фрагменті коду на рисунку 3 .7 зображено обчислення статистики, де розраховується середньоарифметичне:

— час до натиснення певної клавіші;

— час до утримання певної клавіші;

— час до натискання клавіші;час утримання клавіші.

```
121 procedure CalcStatistic;
122 var
123   tmpKey:integer;
124   i: integer;
125   tmpKeyCount: integer;
126 begin
127   tmpKeyCount := 0;
128   KeyPressTOvr := 0;
129   for tmpKey := 1 to MAX_KEY_CODE do
130   begin
131     KeyPressOvr[tmpKey] := 0;
132     KeyIntOvr[tmpKey] := 0;
133     if KeyCount[tmpKey] > 0 then
134     begin
135       i := 1;
136       while (i <= KeyCount[tmpKey]) and (i<=MAX_SER_LEN) do
137       begin
138         KeyPressOvr[tmpKey] := KeyPressOvr[tmpKey] + KeyPress[tmpKey,i];
139         KeyIntOvr[tmpKey] := KeyIntOvr[tmpKey] + KeyInt[tmpKey,i];
140         inc(i);
141       end;
142       dec(i);
143       KeyPressOvr[tmpKey] := KeyPressOvr[tmpKey] div i;
144       KeyIntOvr[tmpKey] := KeyIntOvr[tmpKey] div i;
145       KeyPressTOvr := KeyPressTOvr + KeyPressOvr[tmpKey];
146       KeyIntTOvr := KeyIntTOvr + KeyIntOvr[tmpKey];
147       inc( tmpKeyCount );
148     end;
149   end;
150   if tmpKeyCount<>0 then
151   begin
152     KeyPressTOvr := KeyPressTOvr div tmpKeyCount;
153     KeyIntTOvr := KeyIntTOvr div tmpKeyCount;
154   end;
155 end;
```

Рисунок 3.7 — Обчислення статистики

Після розрахунку дані зберігаються в базі даних у таблицях «час» та «користувач» і можуть бути завантажені для поточного користувача. Основним завданням програми є порівняння підписів, де окремо порівнюються підписи

для паролів та підписи під час набору тексту, оскільки склад символів у цьому випадку різний, що може впливати на динаміку набору тексту (рис. 3.8) .

```
function CheckSign(AType:integer):boolean;
var
  tmpDiv: double;
  tmpDiv2: double;
  tmpDivMax: double;
  tmpCount: integer;
  tmpKey:integer;
begin
  CalcStatistic;
  tmpDivMax := 0;
  AddToLog('Перевірка сигнатур. Тип перевірки: '+inttostr(AType));
  tmpDiv := abs(UserKeyPressTOvr - KeyPressTOvr) / UserKeyPressTOvr;
  if tmpDiv > tmpDivMax then
    tmpDivMax := tmpDiv;
  AddToLog('Відхилення по утриманню: '+FloatToStr(tmpDiv));
  tmpDiv := abs(UserKeyIntTOvr - KeyIntTOvr) / UserKeyIntTOvr;
  if tmpDiv > tmpDivMax then
    tmpDivMax := tmpDiv;
  AddToLog('Відхилення по темпу: '+FloatToStr(tmpDiv));
  tmpDiv := 0;
  tmpDiv2 := 0;
  tmpCount := 0;
  for tmpKey := 1 to MAX_KEY_CODE do
  begin
    if (KeyPressOvr[tmpKey]<>0) and (KeyIntOvr[tmpKey]<>0) and (UserKeyPressOvr[tmpKey]<>0) and (UserKeyIntOvr[tmpKey]<>0) then
    begin
      tmpDiv := tmpDiv + abs(UserKeyIntOvr[tmpKey] - KeyIntOvr[tmpKey]) / UserKeyIntOvr[tmpKey];
      tmpDiv2 := tmpDiv2 + abs(UserKeyPressOvr[tmpKey] - KeyPressOvr[tmpKey]) / UserKeyPressOvr[tmpKey];
      inc(tmpCount);
    end
  end;
  if tmpCount>0 then
  begin
    tmpDiv := tmpDiv / tmpCount;
    tmpDiv2 := tmpDiv2 / tmpCount;
  end;
  AddToLog('Середнє відхилення по утриманню по клавішах: '+FloatToStr(tmpDiv));
  AddToLog('Середнє відхилення по темпу по клавішах: '+FloatToStr(tmpDiv2));
  if tmpDiv > tmpDivMax then
    tmpDivMax := tmpDiv;
  if tmpDiv2 > tmpDivMax then
    tmpDivMax := tmpDiv2;
  result := tmpDivMax < SQLExecute('select coalesce(k_dev,0) from param');
  if not result then
    AddToLog('Виявлено невідповідність психомоторних характеристик поточного користувача і реєстраційних даних');
end;
```

Рисунок 3.8 — Порівняння сигнатур

При порівнянні розраховуються середні значення на основі поточних даних про поведінку користувачів. Максимальне відхилення характеристик виявляється в процесі порівняння. Максимальне відхилення порівнюється з максимально допустимим відхиленням, що зберігається в налаштуваннях програми.

Формування випадкового пароля показано на рисунку 3.9, де зазначено, що довжина пароля не може бути меншою за мінімальну, але може змінюватися випадковим чином.

Від 0 до VAR_PASS_LENGTH. Для побудови пароля використовується набір допустимих символів, що зберігаються в налаштуваннях програми та в таблиці "param"

```
287 procedure frmChangePass_brnCreatePass_OnClick (Sender: TObject; var Cancel: boolean);
288 var
289   tmpPassLength: integer;
290   tmpPass: string;
291   tmpValidKeys: string;
292   i: integer;
293   j: integer;
294 begin
295   tmpPassLength := MIN_PASS_LENGTH + trunc(Random()*(VAR_PASS_LENGTH+1));
296   tmpValidKeys := SQLExecute('select coalesce(ValidPasskey,''!'') from param');
297   tmpPass := '';
298   for i:=1 to tmpPassLength do
299   begin
300     tmpPass := tmpPass + tmpValidKeys[ trunc(Random()*length(tmpValidKeys))+1 ];
301   end;
302   frmChangePass.edtPassword.Text := tmpPass;
303   frmChangePass.edtEnterPass.Text := '';
304   frmChangePass.btnConfirm.Enabled := true;
305   InitTimings;
306 end;
```

Рисунок 3.9 — Генерація випадкового пароля

```
313 procedure frmDataEdit_Button1_OnAfterClick (Sender: TObject);
314 begin
315   if not CheckSign(TT_TEXT) then
316   begin
317     ShowMessage('Виявлено розбіжність психомоторних характеристик поточного користувача і реєстраційних даних. Доступ до програми заблокований. Будь ласка, пройдіть повторну авторизацію!');
318     frmMain.Close;
319   end;
320 end;
```

Рисунок 3.10 — Контроль збереження даних

Для перевірки були використані зразки клавіатурного почерку п’яти людей. Час утримання клавіши у першого користувача для першого зразка варіюється від 85 мс до 114 мс, час між натисканнями клавіш – від 92 мс до 481 мс. При цьому середнє утримання клавіш 98,6 мс, а середній час між натисканням клавіш складає 208,5 мс (рисунок 3.11).

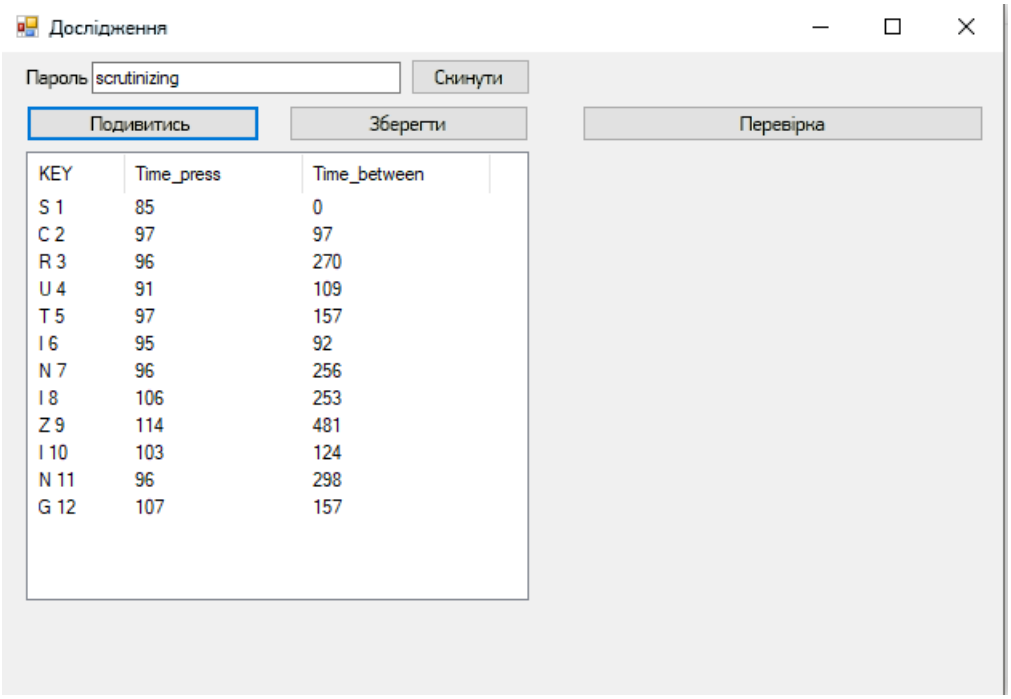


Рисунок 3.11 – Результат КП для першого зразка першого користувача

Час утримання клавіши у першого користувача для другого зразка варіюється від 75 мс до 112 мс, час між натисканнями клавіш – від 28 мс до 143 мс. При цьому середнє утримання клавіш 88,3 мс, а середній час між натисканням клавіш складає 93,6 мс, тобто менше, аніж в першому зразку (рисунок 3.12).

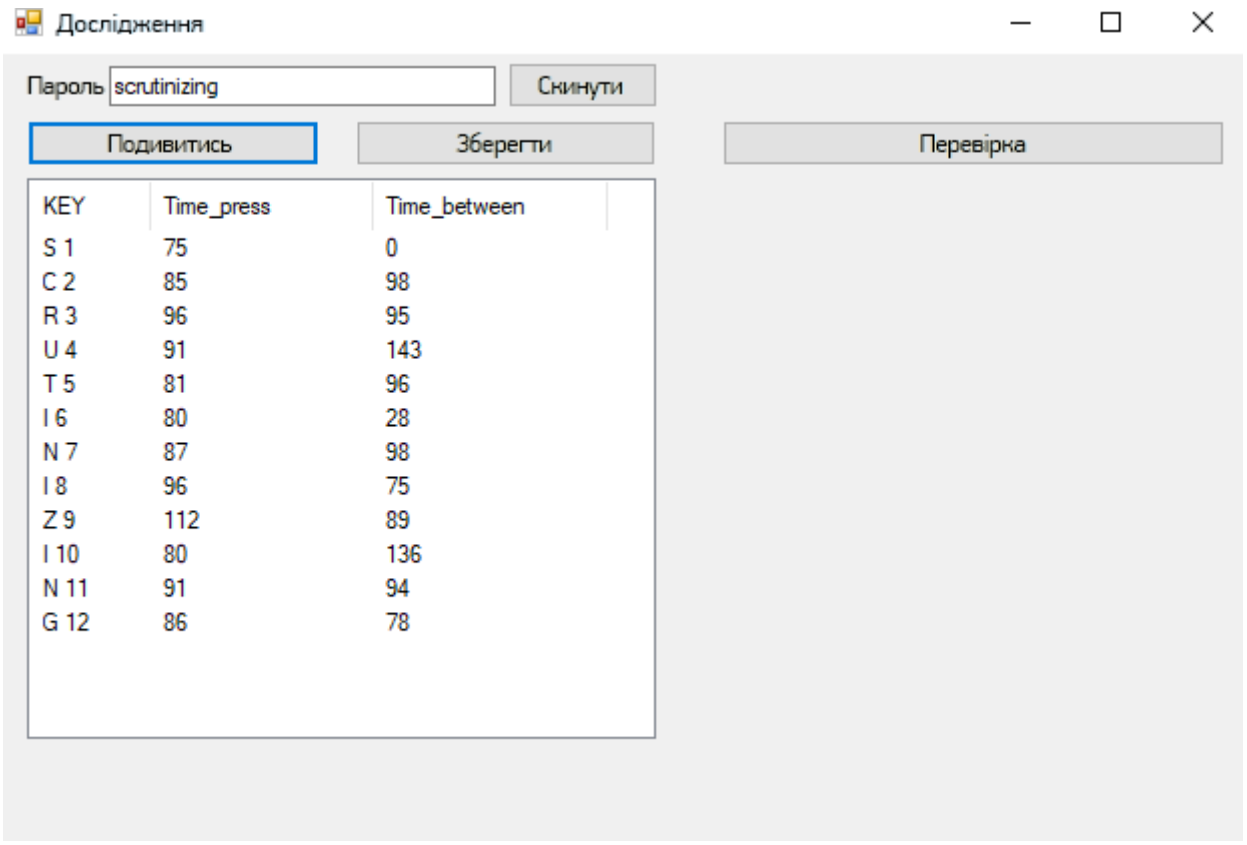


Рисунок 3.12 — Результат КП для другого зразка першого користувача

Час утримання клавіши у другого користувача варіюється від 75 мс до 107 мс, час між натисканнями клавіш – від 31 мс до 234 мс. При цьому середнє утримання клавіш 91 мс, а середній час між натисканням клавіш складає 91,8 мс (рисунок 3.12).

Час утримання клавіши у третього користувача варіюється від 95 мс до 160 мс, час між натисканнями клавіш – від 55 мс до 736 мс. При цьому середнє утримання клавіш 111,3 мс, а середній час між натисканням клавіш складає 327 мс (рисунок 3.13).

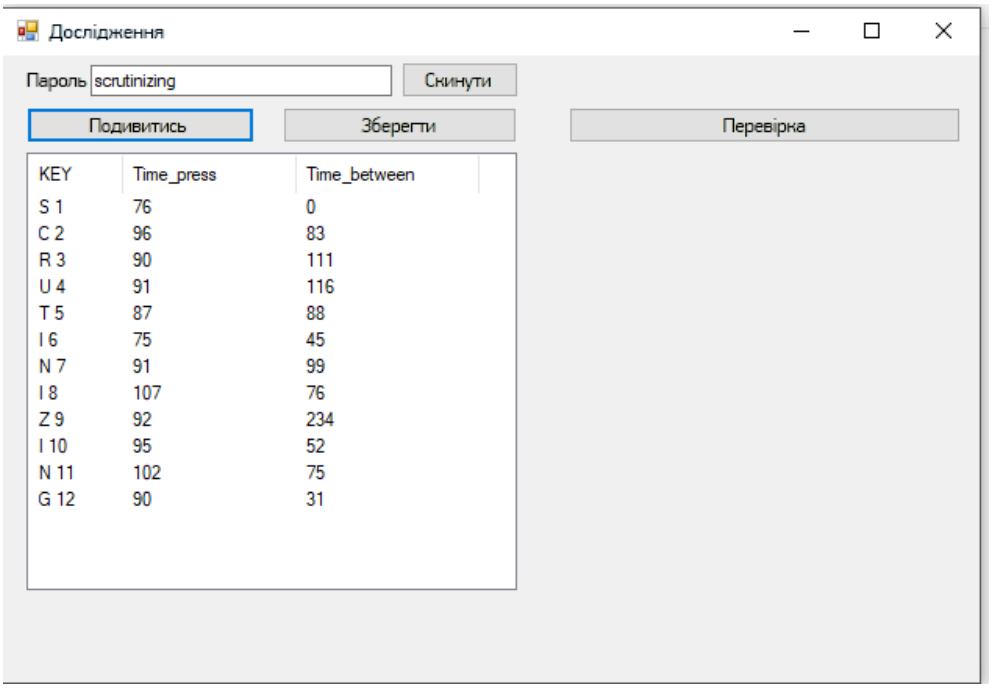


Рисунок 3.14 — Результат КП другого користувача

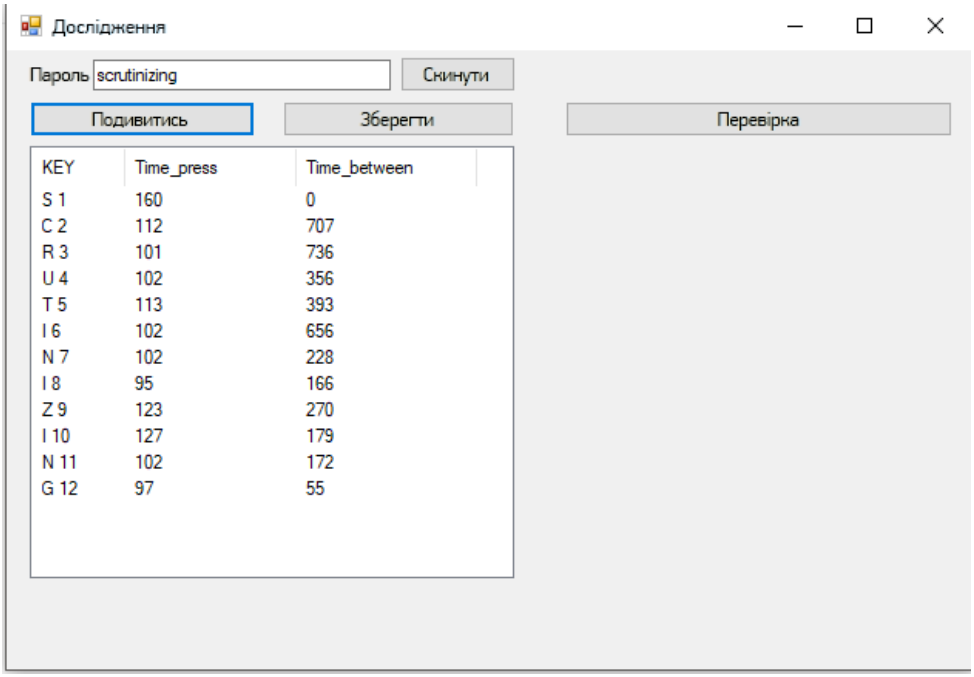


Рисунок 3.15 — Результат КП третього користувача

Час утримання клавіши у четвертого користувача варіюється від 91 мс до 128 мс, час між натисканнями клавіш – від 145 мс до 1287 мс. При цьому середнє утримання клавіш 104,8 мс, а середній час між натисканням клавіш складає 615,5 мс (рисунок 3.16).

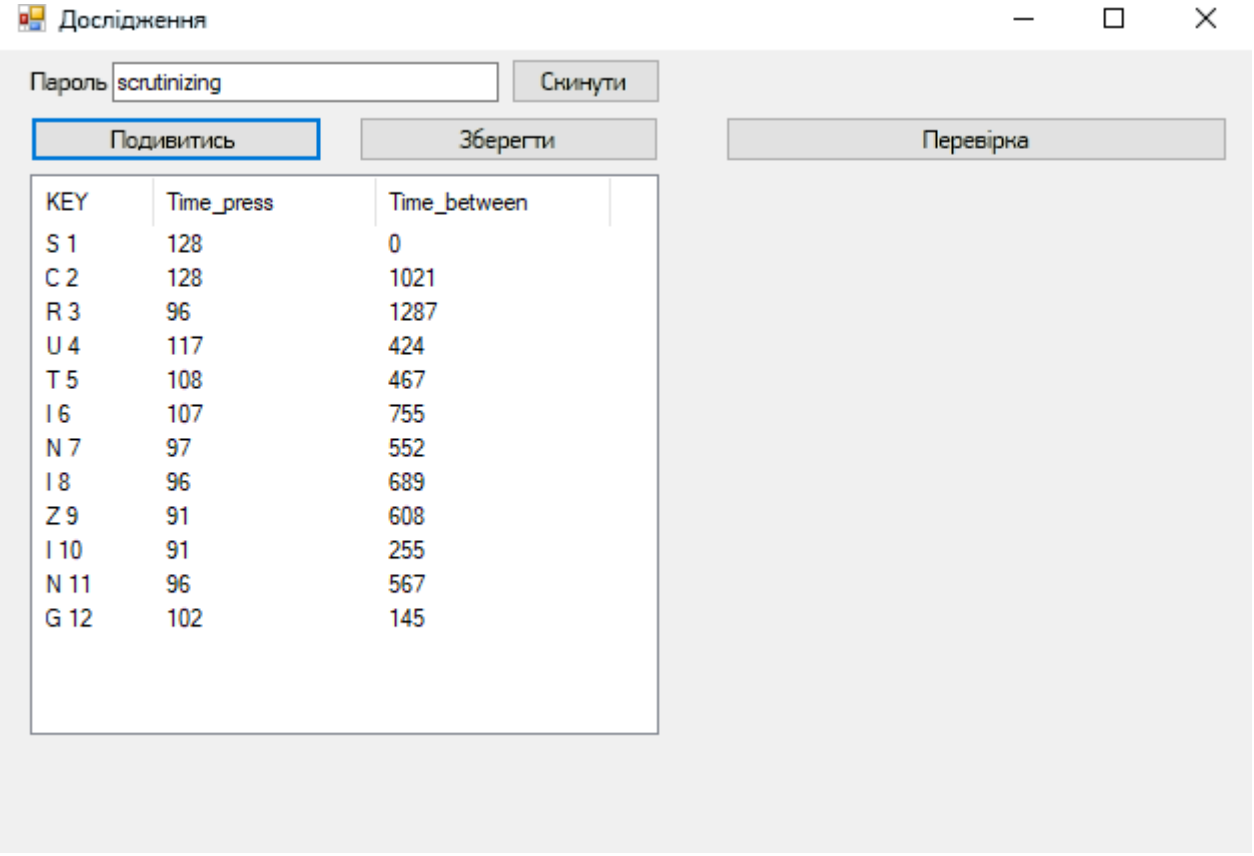


Рисунок 3.16 — Результат КП четвертого користувача

Час утримання клавіши у п’ятого користувача варіюється від 68 мс до 102 мс, час між натисканнями клавіш – від 51 мс до 507 мс. При цьому середнє утримання клавіш 82 мс, а середній час між натисканням клавіш складає 233,2 мс (рисунок 3.17).

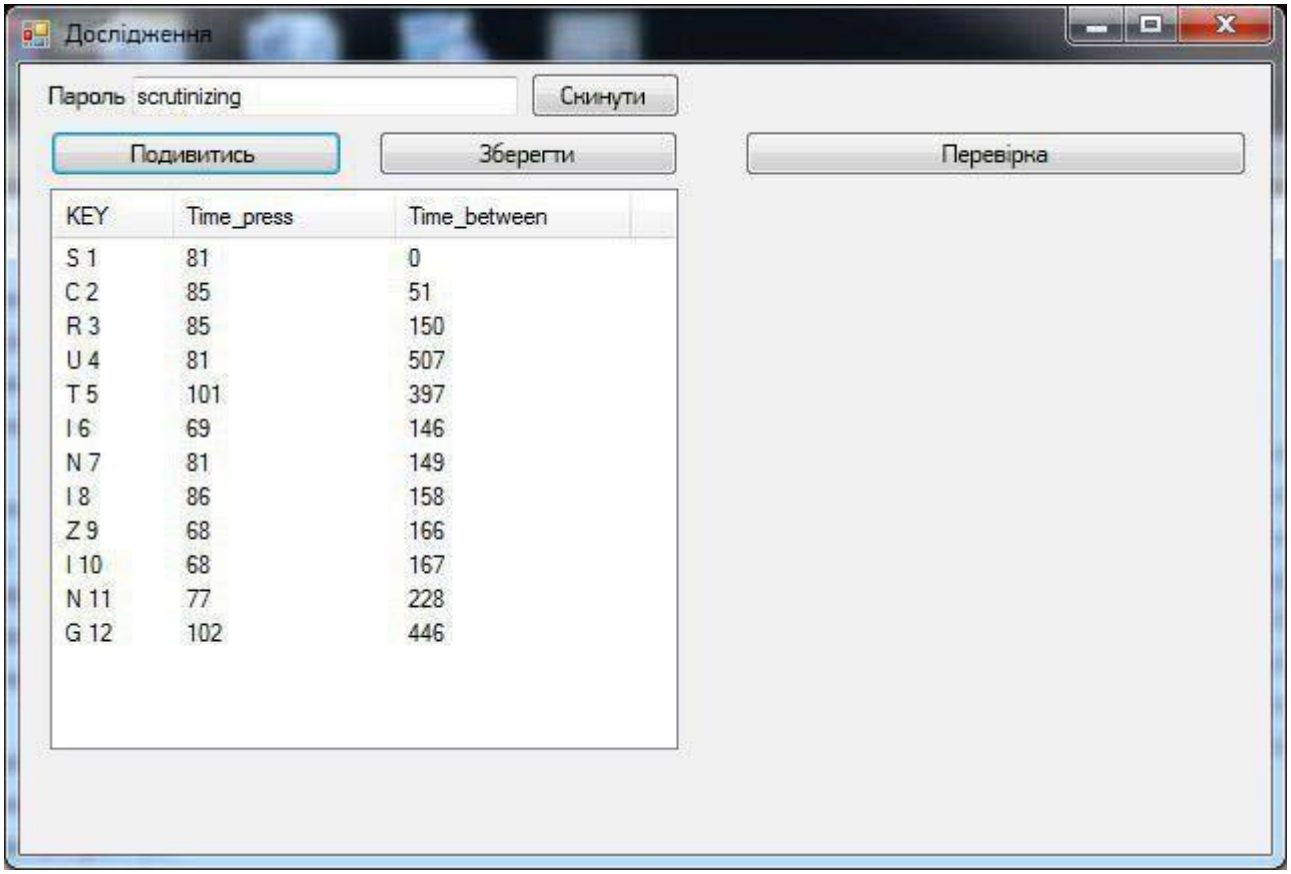


Рисунок 3.17 – Результат КП п’ятого користувача

Після закінчення тестування з отриманих даних було побудовано графіки:

— порівнянь часу утримання клавіш двох зразків першого користувача (рисунок 3.18);

— порівняння часу між натисканням клавіш двох зразків у першого користувача (рисунок 3.19);

— порівняння часу утримання клавіш двох користувачів (рисунок 3.10);

— порівняння часу між натисканням клавіш у двох користувачів (рисунок 3.20);

— порівняння часу утримання клавіши у п’яти користувачів, порівняння часу між натисканням клавіш у п’яти користувачів зображено на рисунках 3.21 та 3.22.

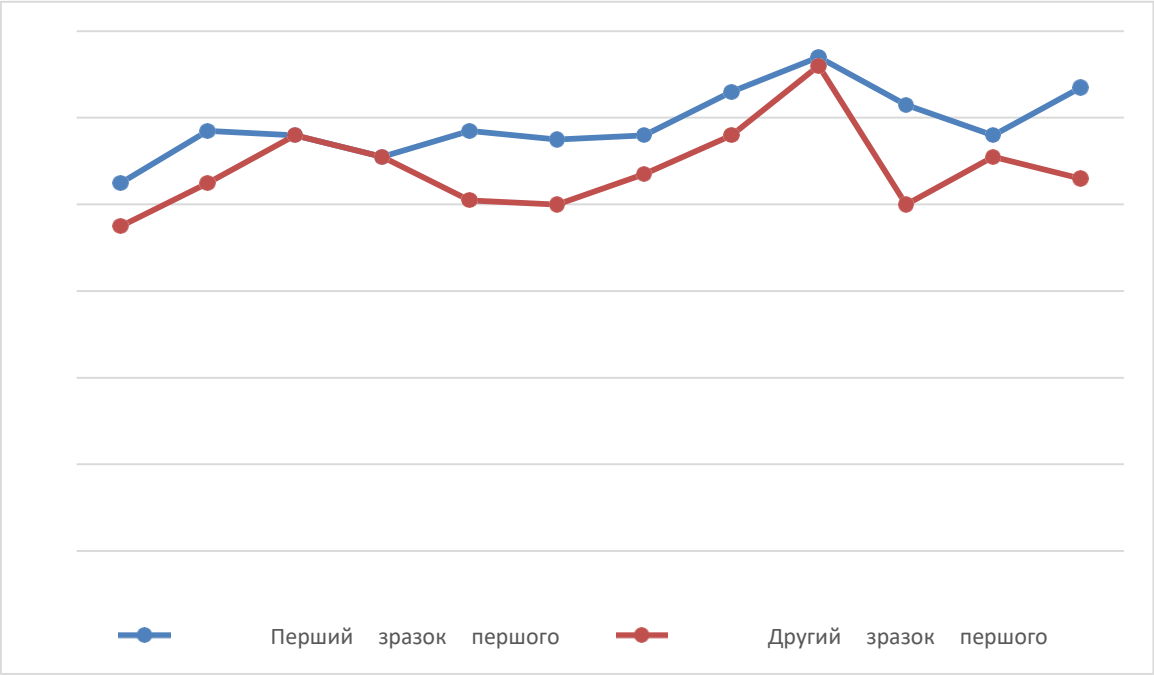


Рисунок 3.18 — Порівняння часу утримання клавіш двох зразків у першого користувача

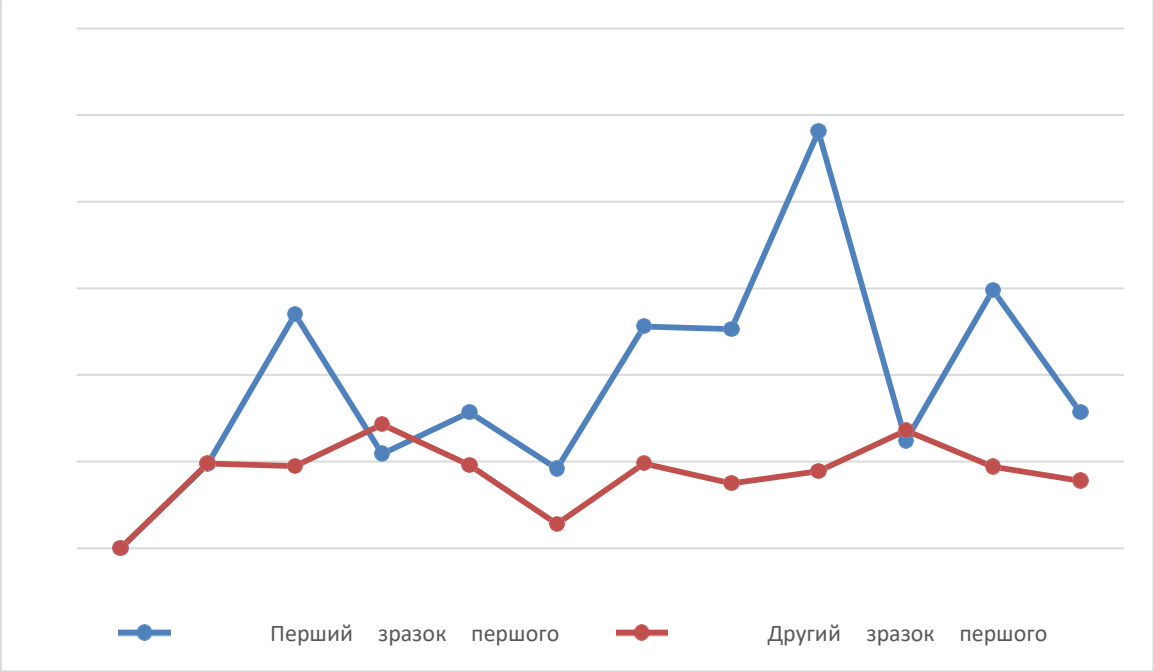


Рисунок 3.19 — Порівняння часу між натисканням клавіш двох зразків у першого користувача

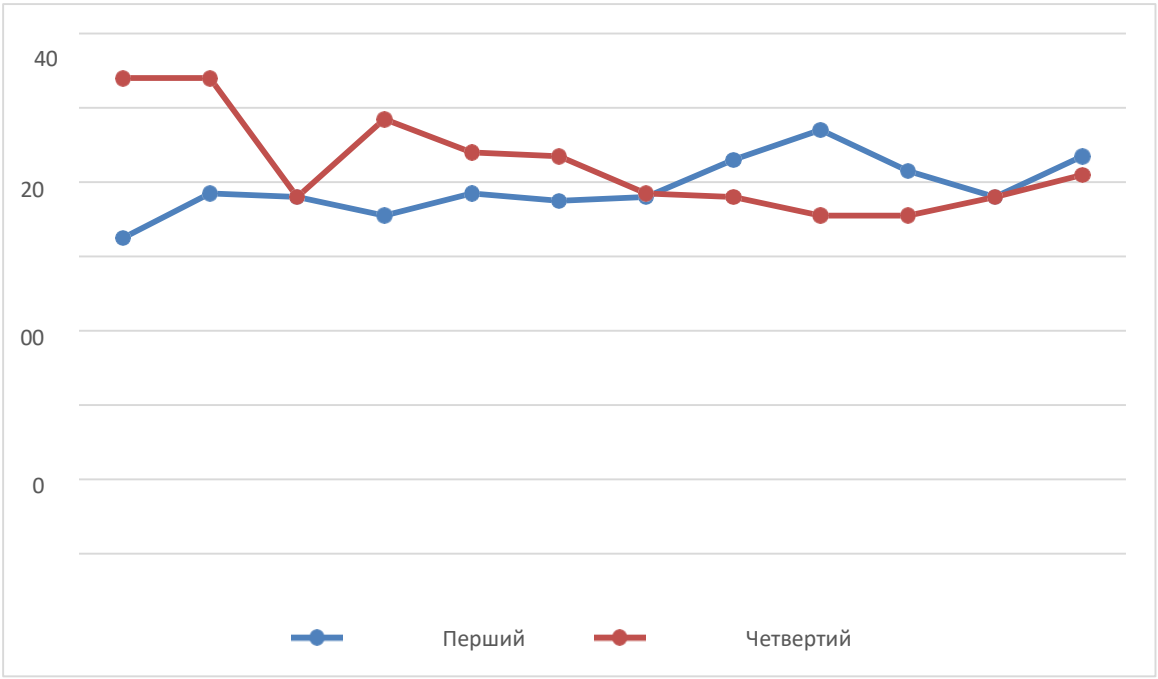


Рисунок 3.20 — Порівняння часу утримання клавіш двох користувачів

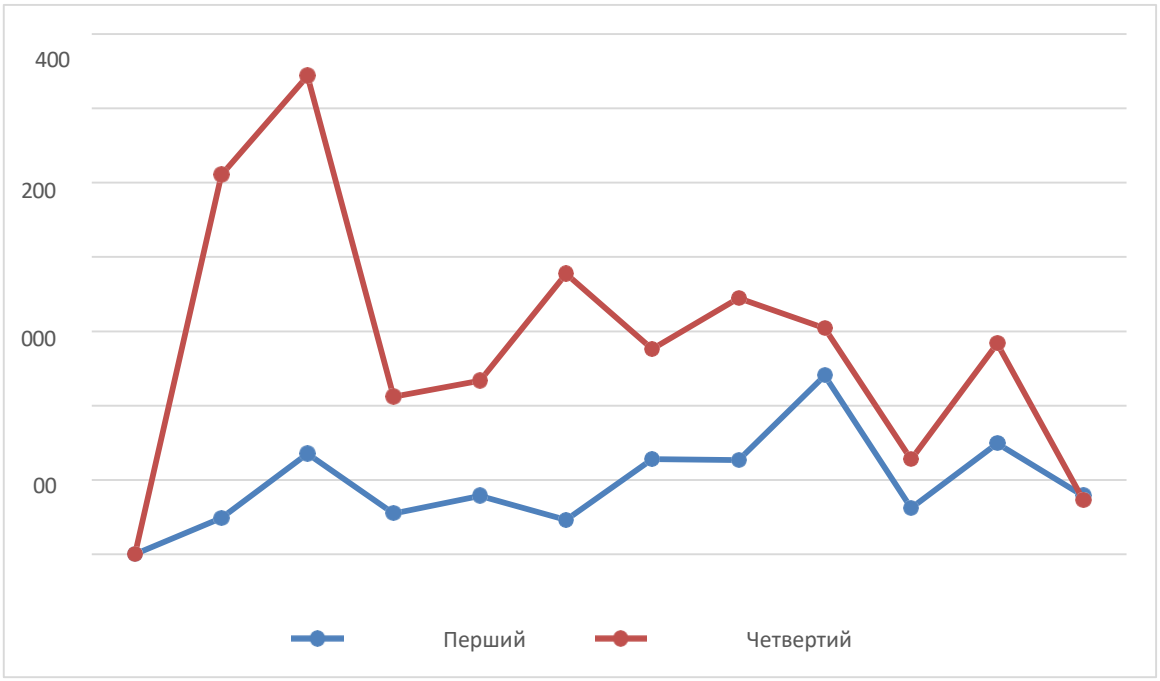


Рисунок 3.21 — Порівняння часу між натисканням клавіш у двох користувачів

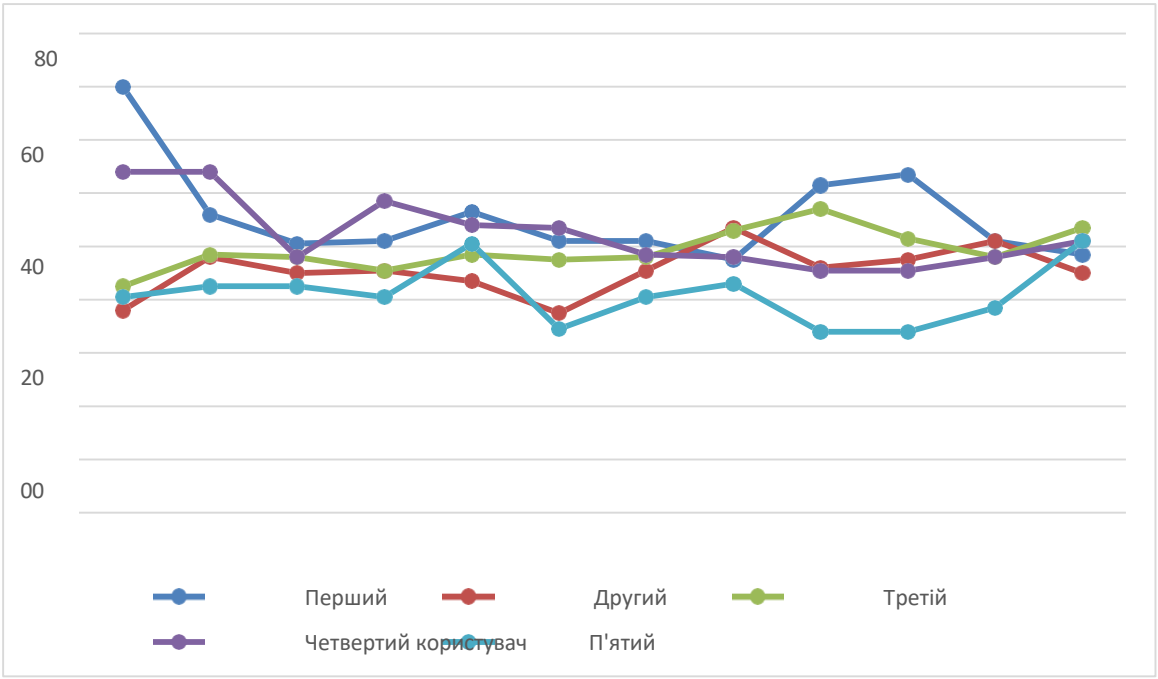
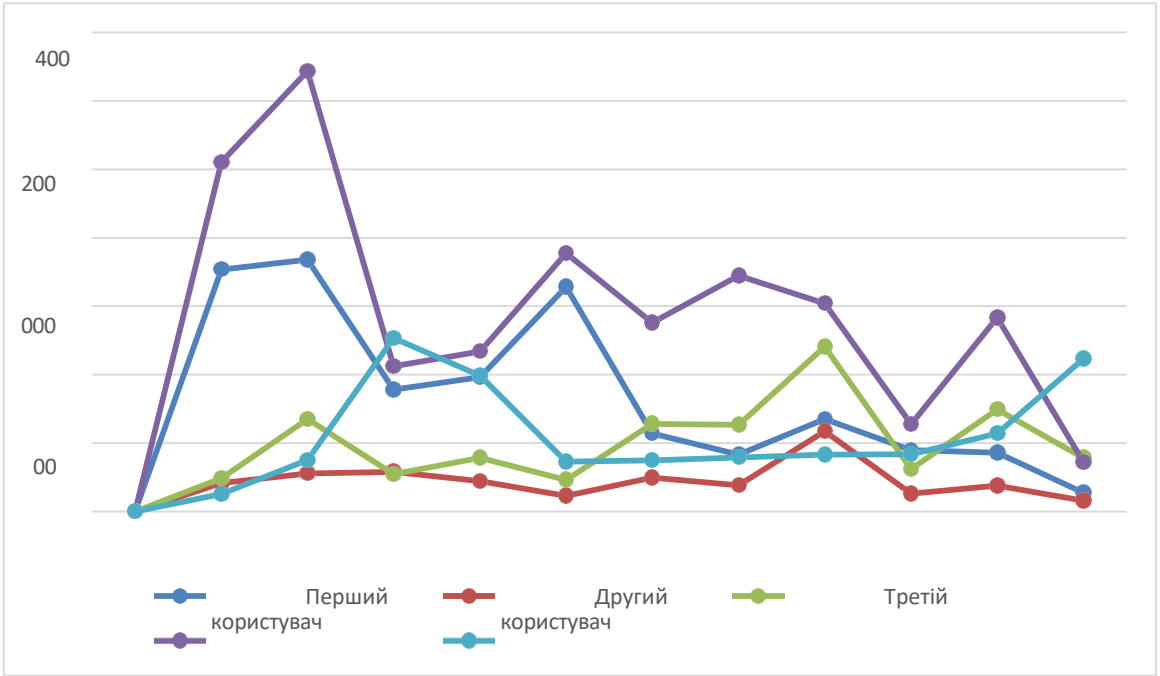


Рисунок 3.22 — Порівняння часу утримання клавіши у п’яти користувачів

Рисунок 3.23 — Порівняння часу між натисканням клавіш у п’яти



користувачів

Таким чином, отримані в ході тестування дані дають змогу зробити висновок, що кожній людині притаманний свій клавіатурний почерк, а

почерки різних людей відрізняються між собою. Виходячи з цього, аутентифікацію на основі аналізу клавіатурного почерку має свою ефективність та може бути використана.

ВИСНОВКИ

У бакалаврській кваліфікаційній роботі проаналізовано характеристики клавіатурного почерку, існуючі методи, моделі та засоби отримання користувацьких КП. Запропоновано визначення отримання клавіатурного почерку користувача, яке відрізняється від існуючих тим, що розпізнає КП не лише методом пароля, а й вільним, згенерованим текстом, причому отриманий шаблон не залежить від порядку символів, що вводяться користувачем, що дозволяє за допомогою цього методу визначити правовий статус користувача та визначити стан нормальної психіки для постійного секретного контролю.

Аналітична модель дозволяє порівнювати отриманий шаблон та поточний шаблон користувача під час реєстрації. Шаблон клавіатурного почерку користувача використовувався для визначення часу натискання певної клавіші, часу натискання клавіш, часу утримання клавіш та часу між натисканнями клавіш. Також побудовано алгоритм отримання шаблону, авторизації, автентифікації та постійного секретного контролю за допомогою клавіатурних почерків.

Реалізовано програму, що використовує алгоритми та методи розпізнавання клавіатурних почерків, які можуть бути використані в інформаційних системах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Білан С.М., Демаш А. А., Іваськів Т. В. Система біометричної ідентифікації особистості з довільною ключовою послідовністю. Збірник наукових праць Державного економіко-технологічного університету транспорту Міністерства освіти і науки України: Серія «Транспортні системи і технології». Київ:ДЕТУТ, 2016.Вип. 28. С. 170-176.

2. Захаров, В. П. Біометричні технології в XXI столітті та їх використання правоохоронними органами [Текст] : посібник / В. П. Захаров, В. І. Рудешко. – 2- ге вид., доп. – Львів: ЛьвДУВС, 2015. – 492 с.

3. Бідюк, П. Сучасні методи біометричної ідентифікації [Текст] / П. Бідюк, В. Бондарчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2009. – Вип. 1(18). – С. 137-146.

4. Yevetskyi, V. Analysis of stability of the user's keyboard handwriting characteristics in the biometric authentication systems / V. Yevetskyi, I. Horniichuk // Information Technology and Security. – 2018. – Vol. 6, Iss. 2 (11). – Pp. 19–28.

5. Теорія імовірностей і математична статистика [Текст]. У 2 ч. Ч. І. Теорія ймовірностей / В. І. Жлуктенко, С.І. Наконечний; за ред. О.П. Бондаренко. – К.: КНЕУ, 2000. – 304 с.

6. ISO/IEC 14882 Fifth edition 2017-12 [Електроний рисурс] / Режим доступу: https://webstore.iec.ch/preview/info_isoiec14882%7Bed5.0%7Den.pdf

7. Dr. R. SatyaPrasad, Muzhir Shaban Al-Ani, Salwa Mohammed Nejres. An Efficient Approach for Human Face Recognition. /International Journal of Advanced Researchin Computer Science and Software Engineering, Volume 5, Issue 9, September, 2015.

8. B. Mathivanan, V. Palanisamyand S. Selvarajan. A Hybrid Model For Human Recognition System Using Hand Dorsum Geometry and Finger-Knuckle-Print. Journal of Computer Science. 2012.No 8 (11).P. 1814-1821.

9. Основн іметоди динамічної біометричної ідентифікації URL: www.biometrics.org/ (дата звернення: 17.07.2018).

10. Біометрія.URL: https://uk.wikipedia.org/wiki/Біометрія. (дата звернення 18.11.2018).

11. Пристрій біометричної ідентифікації особистості по почерку роботи на клавіатурі:пат. на корисну модель100843 Україна: МПК (2015.01) G06K 9/00. № 201502043; заявл.06.03.2015; опубл. 10.08.2015,Бюл. №15.

12. Syed Zahurul Islam, Syed Zahidul Islam, Razali Jidin. Performance Study of Adaptive Filtering Algorithms for Noise Cancellation of EGG Signal, IEEE, 2009.URL: https://www.researchgate.net/publication/224107544_Performance_study_of_adaptive_filtering_algorithms_for_noise_cancellation_of_ECG_signal.(дата звернення 21.11.2018).

13. E. Farahabadi. Noise Removal from Electrocar diogramsignal Employ inganartificial Neural Networkin Wawelet Domain. IEEE, 2009. URL: https://www.researchgate.net/publication/251909703_Noise_Removal_from_Electrocardiogram_Signal_Employing_an_Artificial_Neural_Network_in_Wavelet_Domain.(дата звернення 25.11.2018).

ДОДАТОК А

Технічне завдання

Міністерство освіти та науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ ВНТУ

д.т.н., проф.

_____О. Д. Азаров

"_21_" березня_____ 2025 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання бакалаврської кваліфікаційної роботи

Біометрична ідентифікація особистості на основі аналізу динаміки почерку роботи на клавіатурі

08-54.БКР.003.00.000 ТЗ

Науковий керівник к.т.н., доц. каф. ОТ

_____ Колесник І.С.

Студент групи 1КІ-23мс

_____ Болденюк Н.А.

Вінниця 2025

1 Підстава виконання бакалаврської кваліфікаційної роботи

Наказ про затвердження теми бакалаврської кваліфікаційної роботи від 20.03.2025 р. №97.

2 Мета та призначення БКР

2.1 Мета роботи — створення системи біометричної ідентифікації особистості на основі аналізу динаміки почерку роботи на клавіатурі

3 Вимоги до виконання БКР

БКР повинна задовольняти такі вимоги:

— визначення характеристик комп'ютерного почерку;

— дослідження алгоритмів, методів, моделей та засобів визначення КП користувача інформаційної системи;

— дослідження та створення математичних моделей визначення КП користувача інформаційної системи;

— розробка алгоритму дослідження КП користувача за тривалістю утримання клавіш;

— розробка алгоритму дослідження КП користувача за часом між натисненням клавіш;

— розробка способу визначення КП користувача за довільним текстом.

4 Етапи БКР та очікувані результати

Робота виконується у вісім етапів, що наведені в таблиці А.1.

5 Матеріали, що подаються до захисту БКР

До захисту подаються: пояснювальна записка БКР, графічні і ілюстративні матеріали, протокол попереднього захисту БКР на кафедрі, відзив наукового керівника, рецензія опонента, протоколи складання державних екзаменів, анотації до БКР українською та іноземною мовами, довідка про відповідність оформлення БКР діючим вимогам.

Таблиця А.1 – Етапи виконання роботи

№ з/п	Назва етапів дипломної Роботи	Строк виконання	Підпис
1	Постановка задачі роботи	21.03.25	
2	Огляд предметної області	21.03.25— 29.03.25	
3	Розробка моделей розпізнавання	21.03.25— 29.03.25	
4	Дослідження основних підходів до ідентифікації на основі клавіатурного почерку	30.03.25— 11.04.25	
5	Дослідження основних підходів до ідентифікації на основі клавіатурного почерку	12.04.25— 26.04.25	
6	Тестування та демонстрація роботи системи	27.04.25— 07.05.25	
7	Оформлення пояснювальної записки та ілюстративного матеріалу	08.05.25	
8	Перевірка якості виконання бакалаврської роботи та усунення недоліків	14.05.25	

6 Порядок контролю виконання та захисту БКР

Виконання етапів графічної та розрахункової документації БКР контролюється науковим керівником згідно зі встановленими термінами. Захист БКР відбувається на засіданні Державної екзаменаційної комісії, затвердженою наказом ректора.

7 Вимоги до оформлювання та порядок виконання БКР

7.1 При оформлювання БДР використовуються:

— ДСТУ 3008: 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302: 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— міждержавний ГОСТ 2.104-2006 «Єдина система конструкторської документації. Основні написи»;

— Методичні вказівки до виконання бакалаврських кваліфікаційних робіт зі спеціальності 123 «Комп’ютерна інженерія» (освітня програма «Комп’ютерна інженерія»). Кафедра обчислювальної техніки ВНТУ 2022;

— документами на які посилаються у вище вказаних.

7.2 Порядок виконання БКР викладено в «Положення про кваліфікаційні роботи на першому (бакалаврському) рівні вищої освіти СУЯ ВНТУ-03.02.02-П.001.01:21»

Д О Д А Т О К Б

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: _ Біометрична ідентифікація особистості на основі аналізу динаміки почерку роботи на клавіатурі _

Тип роботи: _____ бакалаврська кваліфікаційна робота _____

(бакалаврська кваліфікаційна робота / магістерська кваліфікаційна робота)

Підрозділ _____кафедра обчислювальної техніки_____

(кафедра, факультет, навчальна група)

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism __30___%

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

✓ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту

☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

Експертна комісія:

_____Азаров О.Д., зав. каф. ОТ _____ _____

(прізвище, ініціали, посада) (підпис)

____Крупельницький Л.В., доц. каф ОТ_____ _____

(прізвище, ініціали, посада) (підпис)

Особа, відповідальна за перевірку _____ ___Захарченко С.М.____

(підпис) (прізвище, ініціали)

З висновком експертної комісії ознайомлений(-на)

Керівник _____ _____Колесник І.С._____

(підпис) (прізвище, ініціали, посада)

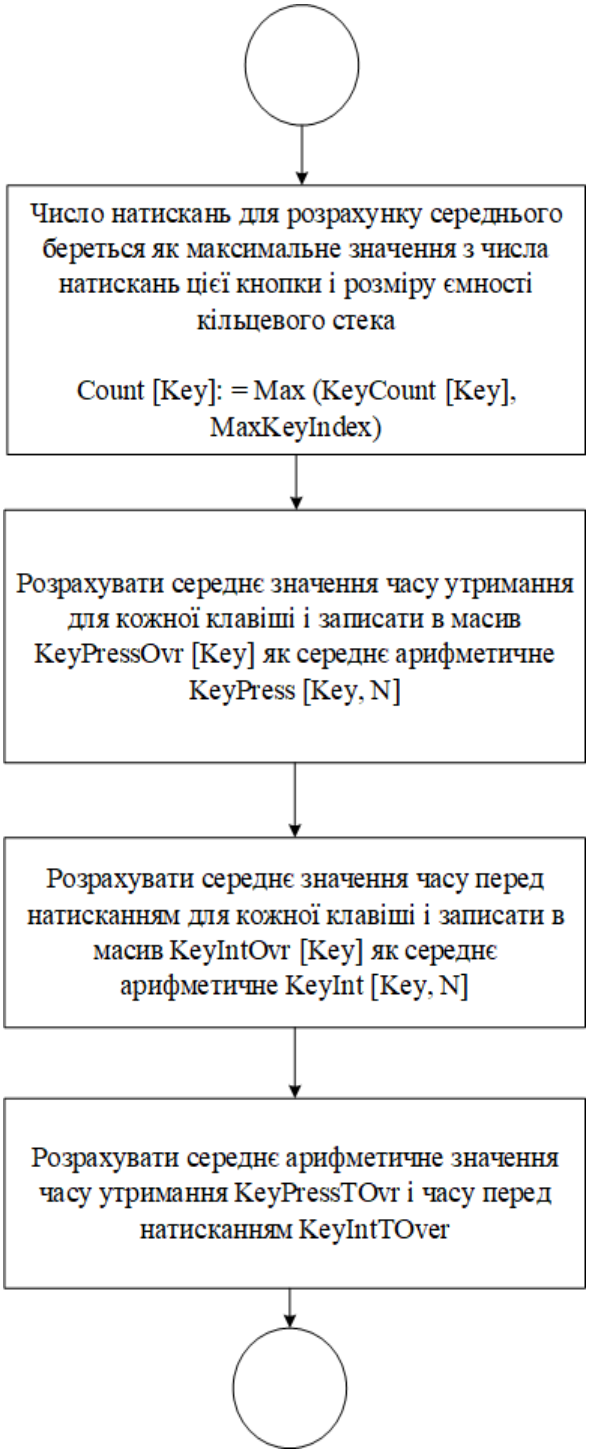
Здобувач _____ _____Болденюк Н.А._____

(підпис) (прізвище, ініціали)

ДОДАТОК В

Графічна частина

АЛГОРИТМ ОТМАННЯ ШАБЛОНУ


Число натискань для розрахунку середнього береться як максимальне значення з числа натискань цієї кнопки і розміру ємності кільцевого стека
Count [Key]: = Max (KeyCount [Key], MaxKeyIndex)
Розрахувати середнє значення часу утримання для кожної клавіші і записати в масив KeyPressOvr [Key] як середнє арифметичне KeyPress [Key, N]
Розрахувати середнє значення часу перед натисканням для кожної клавіші і записати в масив KeyIntOvr [Key] як середнє арифметичне KeyInt [Key, N]
Розрахувати середнє арифметичне значення часу утримання KeyPressTOvr і часу перед натисканням KeyIntTOver

ДОДАТОК Г

ілюстративна частина

ПОРІВНЯННЯ ЧАСУ МІЖ НАТИСКАННЯМ КЛАВІШ ДВОХ ЗРАЗКІВ У ПЕРШОГО КОРИСТУВАЧА

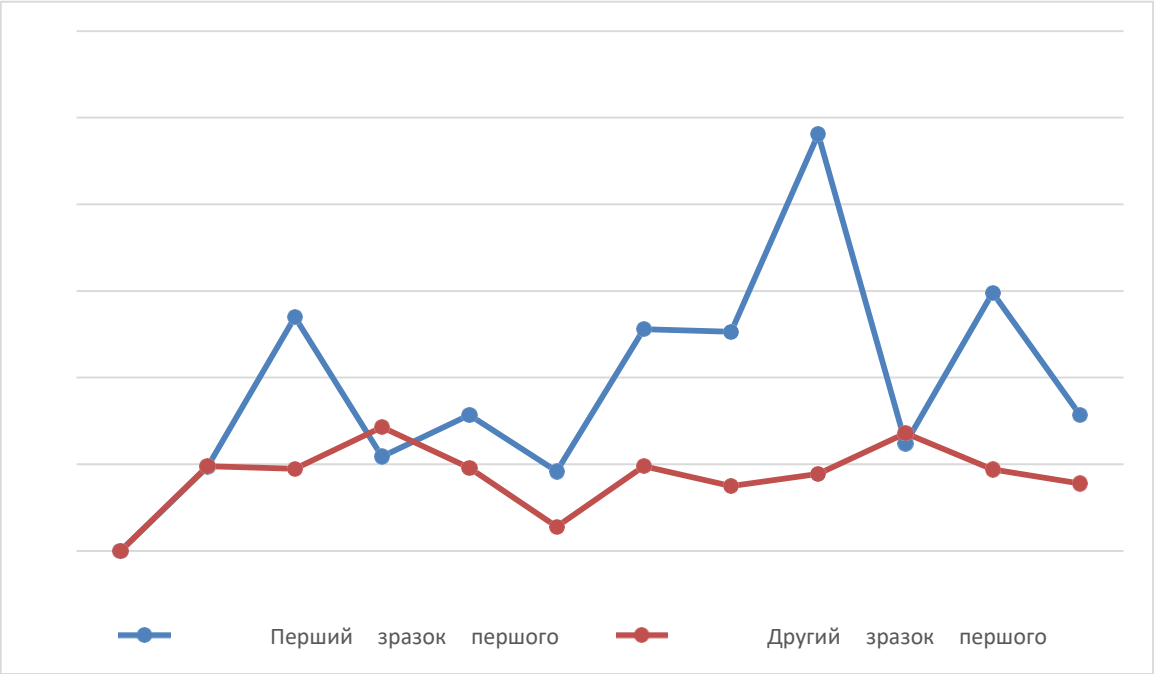


Рисунок Г.1 — Порівняння часу між натисканням клавіш двох зразків у першого користувача

ДОДАТОК Г

Основний лістинг

```
--------------------------------------------------------------------------------

--
-- Title       : NoTitle
-- Design      : key_1
-- Author      : tmp
-- Company     : 111
--
--------------------------------------------------------------------------------
--
-- File        : c:\My_Designs\biometryk_key\key_1\compile\digital_biometry.vhd
-- Generated   : FriJan  2 15:56:34 2015
-- From        : c:\My_Designs\biometryk_key\key_1\src\digital_biometry.bde
-- By          : Bde2Vhdl ver. 2.6
--
--------------------------------------------------------------------------------
--
-- Description :
--
--------------------------------------------------------------------------------
-- Designunitheader --
library IEEE;
use IEEE.std_logic_1164.all;
entitydigital_biometryis
port(
      Input0 : in STD_LOGIC;
      Input1 : in STD_LOGIC;
      Input2 : in STD_LOGIC;
      Input3 : in STD_LOGIC;
      Input4 : in STD_LOGIC;
      Input5 : in STD_LOGIC;
      Input6 : in STD_LOGIC;
      Input7 : in STD_LOGIC;
      Input8 : in STD_LOGIC;
      Input9 : in STD_LOGIC;
      BusOutput0 : out STD_LOGIC_VECTOR(2 downto 0);
      BusOutput1 : out STD_LOGIC_VECTOR(7 downto 0)
  );
enddigital_biometry;

architecturedigital_biometryofdigital_biometryis
```

```
---- Componentdeclarations -----

component Counter3
port (
clk : in STD_LOGIC;
      Q : out STD_LOGIC_VECTOR(2 downto 0)
  );
endcomponent;
componentdecode
port (
Ain : in STD_LOGIC_VECTOR(2 downto 0);
En : in STD_LOGIC;
Yout : out STD_LOGIC_VECTOR(7 downto 0)
  );
endcomponent;
component or_8
port (
      In_00 : in STD_LOGIC;
      In_01 : in STD_LOGIC;
      In_02 : in STD_LOGIC;
      In_03 : in STD_LOGIC;
      In_04 : in STD_LOGIC;
      In_05 : in STD_LOGIC;
      In_06 : in STD_LOGIC;
      In_07 : in STD_LOGIC;
      Out00 : out STD_LOGIC
  );
endcomponent;
---- Signaldeclarationsusedonthediagram ----

signal NET73 : STD_LOGIC;
signal NET82 : STD_LOGIC;
signal BUS91 : STD_LOGIC_VECTOR (2 downto 0);
begin

----  Componentinstantiations  ----
NET73 <= Input8 and NET82;

U2 : or_8
portmap(
      In_00 => Input0,
      In_01 => Input1,
      In_02 => Input2,
      In_03 => Input3,
      In_04 => Input4,
```

```
      In_05 => Input5,
      In_06 => Input6,
      In_07 => Input7,
      Out00 => NET82
  );
U3 : Counter3
portmap(
      Q => BusOutput0,
clk => NET73
  );

U4 : Counter3
portmap(
      Q => BUS91,
clk => NET82
  );
U5 : decode
portmap(
Ain => BUS91,
En => Input9,
Yout => BusOutput1
  );


enddigital_biometry;
```