МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ДОСЛІДЖЕННЯ МЕТОДІВ АВТЕНТИФІКАЦІЇ БІОМЕТРИЧНИМИ ДАНИМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Микита М'ЯСНИКОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти групи УБД-41

Микита М'ЯСНИКОВ
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЩАВІНСЬКИЙ
к. т. н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: _____

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти Бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____Світлана Легомінова
"___" _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

М'ясников Микита Сергійович
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: "Дослідження методів автентифікації біометричними даними для забезпечення інформаційної безпеки"
керівник кваліфікаційної роботи: Юрій ЩАВІНСЬКИЙ, *к. т. н., доц.*
(прізвище, ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024 року № 36.

2. Строк подання кваліфікаційної роботи: 20.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи: методи автентифікації – аналіз та порівняння; розробка інтегрованої системи безпеки; наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Перелік питань, які бути розроблені:

4.1. Аналіз сучасних методів автентифікації за допомогою біометричних даних.

4.2. Порівняльний аналіз різних методів біометричної автентифікації.

4.3. Розроблення та впровадження рекомендацій щодо вибору найбільш оптимальних біометричних методів для конкретних ситуацій та систем.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint.*

6. Дата видачі завдання: "11" березня 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз сучасних методів автентифікації за допомогою біометричних даних	08.04.2024	
4.	Проведення порівняльного аналізу різних методів біометричної автентифікації.	22.04.2024	
5.	Розроблення рекомендацій щодо вибору та впровадження найбільш оптимальних біометричних методів для конкретних ситуацій та систем	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Микита М'ЯСНИКОВ
(підпис) *(ім’я, прізвище)*

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач М’ясников М.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Дослідження методів автентифікації біометричними даними для забезпечення інформаційної безпеки ”

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач М’ЯСНИКОВ Микита у кваліфікаційній роботі проаналізував методи біометричної автентифікації, дослідив біометричні техніки для забезпечення інформаційної безпеки, розробив метод автентифікації біометричними даними та оцінив його ефективність і відпрацював рекомендації щодо вибору та впровадження найбільш оптимальних біометричних методів для конкретних ситуацій та систем.

М’ЯСНИКОВ Микита показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів здатність самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичній конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача М’ЯСНИКОВА Микити на оцінку “відмінно” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач М’ясников М.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти М'ЯСНИКОВА Микити

на тему "Дослідження методів автентифікації біометричними даними для забезпечення інформаційної безпеки"

Актуальність. У сучасному світі кількість кіберзагроз постійно зростає, і традиційні методи автентифікації, такі як паролі та PIN-коди, стають менш ефективними. Необхідність дослідження методів біометричної автентифікації обумовлена потребою у підвищенні рівня безпеки, зручності для користувачів, інтеграції новітніх технологій та забезпеченні відповідності нормативним вимогам і етичним стандартам. Біометричні дані, як відбитки пальців, сканування обличчя, райдужної оболонки ока та голосу, надають більш високий рівень безпеки завдяки своїй унікальності та складності для підробки. Дослідження в галузі біометричної автентифікації мають великий потенціал для інновацій. Зокрема, нові методи та алгоритми можуть забезпечити ще вищий рівень безпеки та надійності, а також відкрити нові можливості для інтеграції біометричних систем у різні сфери життя.

Позитивні сторони.

1. У роботі досліджені сучасні методи автентифікації, визначені їх позитивні сторони та властивості а також недоліки кожного окремого методу та визначена потреба в комплексному застосуванні методів для зниження коефіцієнтів хибного доступу та хибної відмови в доступі, розроблені рекомендації з впровадження оптимальних біометричних методів для конкретних ситуацій та систем .
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Автор опрацював значну джерельну базу наукових публікацій, в тому числі англомовних.
4. За результатами дослідження розроблені рекомендації з впровадження оптимальних біометричних методів для конкретних ситуацій та систем .

Недоліки.

Доцільно було б приділити більше уваги вивченню і класифікації програмних інструментів для оцінки ефективності біометричних методів автентифікації

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки "відмінно", а здобувач М'ЯСНИКОВ Микита заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____ _____

підпис Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена аналізу методів автентифікації біометричними даними, їх порівнянню та розробці рекомендацій застосування цих методів для забезпечення інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 22 рисунки, висновків і списку використаних джерел із 41 найменувань. Загальний обсяг роботи становить 72 аркуші, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є аналіз методів біометричної автентифікації, їх порівняння та розроблення рекомендацій щодо впровадження біометричної автентифікації в системи та процеси.

Об'єктом дослідження є процеси автентифікації та розпізнавання користувача, використовуючи біометричні дані для забезпечення інформаційної безпеки.

Предметом дослідження є методи автентифікації з використанням біометричних даних для забезпечення інформаційної безпеки.

Методи дослідження. В ході проведення дослідження застосований аналіз при огляді наукових джерел та методів автентифікації; мета-аналіз і контент-аналіз наукових публікацій, аналіз журналів та логів для виявлення підозрілих активностей та інцидентів, міжнародні стандарти та їх порівняння.

Як результат у роботі проаналізовані сучасні методи автентифікації, їх позитивні сторони та недоліки, за результатами аналізу встановлена потреба у їх удосконаленні, розроблено комплексну систему автентифікації на основі біометричних даних, яка враховує високу точність і швидкість в роботі, а також забезпечує захист приватності користувачів.

Галузь застосування. Рекомендації по застосуванню комплексної системи автентифікації за допомогою біометричних даних можуть бути використані при розробці та впровадженні систем автентифікації у різних структурах де важливий високий рівень інформаційної безпеки.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, АВТЕНТИФІКАЦІЯ, БІОМЕТРИЧНІ ДАНІ, БІОМЕТРИЧНІ ТЕХНОЛОГІЇ.

ABSTRACT

The qualification work is dedicated to the analysis of methods of authentication using biometric data, their comparison, and the development of recommendations for the application of these methods to ensure information security. The work consists of an introduction, three chapters containing 22 figures, conclusions, and a list of used sources with 41 titles. The total volume of the work is 72 pages, of which 6 pages are occupied by a list of abbreviations and a list of used sources.

The purpose of the study is to analyze methods of biometric authentication, their comparison, and the development of recommendations for the implementation of biometric authentication in systems and processes.

The object of the study is the processes of authentication and user recognition using biometric data to ensure information security.

The subject of the study is methods of authentication using biometric data to ensure information security.

Research methods. In the course of the research, the analysis was applied in the review of scientific sources and methods of authentication; meta-analysis and content-analysis of scientific publications, analysis of journals and logs to identify suspicious activities and incidents, international standards and their comparison.

As a result, the work analyzed modern authentication methods, their positive sides and shortcomings, based on the results of the analysis, the need for their improvement was established, a complex authentication system based on biometric data was developed, which takes into account high accuracy and speed of work, and also ensures the protection of user privacy.

Field of application. Recommendations for the application of a complex authentication system using biometric data can be used in the development and implementation of authentication systems in various structures where a high level of information security is important.

Keywords: INFORMATION SECURITY, AUTHENTICATION, BIOMETRIC DATA, BIOMETRIC TECHNOLOGIES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

FAR	False Acceptance Rate
FRR	False Rejection Rate
EER	Equal Error Rate
AVR	Ability to Verify Rate
FER	Failure to Enroll Rate
ROC	Receiver operating characteristic
OTP	One Time Password
IAM	Identity and Access Management
ISO	International Organization for Standardization
GDPR	General Data Protection Regulation
MIOT	Multi-fingers In One Template
IEC	International Electrotechnical Commission
MFA	Multi-factor authentication
ПЗ	Програмне забезпечення
ОС	Операційна система
у. о.	Умовні одиниці
ДСТУ	Державні стандарти України
НСД	Несанкціонований доступ

ВСТУП

Актуальність теми. У сучасному світі, де інформація стає найціннішим ресурсом, забезпечення її безпеки набуває вирішального значення. З розвитком технологій та цифровізації всі сфери життя, від особистого до професійного, стають все більш уразливими до кіберзагроз. Традиційні методи автентифікації, такі як паролі та пін-коди, виявляються недостатньо надійними в умовах сучасних викликів, оскільки вони можуть бути легко вкрадені або зламані. У зв'язку з цим, зростає потреба у впровадженні більш надійних та безпечних методів автентифікації.

Одним із перспективних напрямків у забезпеченні інформаційної безпеки є використання біометричних даних для автентифікації. Біометричні методи дозволяють ідентифікувати користувачів за унікальними фізичними або поведінковими характеристиками, такими як відбитки пальців, розпізнавання обличчя, райдужка ока, голос та інші. Ці методи забезпечують високий рівень захисту, оскільки біометричні дані важко підробити або викрасти.

Метою роботи є аналіз методів біометричної автентифікації, їх порівняння та розроблення рекомендацій щодо впровадження біометричної автентифікації в системи та процеси.

Об’єктом дослідження є процеси автентифікації та розпізнавання користувача, використовуючи біометричні дані для забезпечення інформаційної безпеки.

Предметом дослідження є методи автентифікації з використанням біометричних даних для забезпечення інформаційної безпеки.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Аналіз сучасних методів автентифікації за допомогою біометричних даних.
2. Проведення порівняльного аналізу різних методів біометричної автентифікації.

3. Розроблення рекомендацій щодо впровадження біометричної автентифікації в системи та процеси.

Методи дослідження. В ході проведення дослідження застосований аналіз при огляді наукових джерел та методів автентифікації; мета-аналіз і контент-аналіз наукових публікацій, аналіз журналів та логів для виявлення підозрілих активностей та інцидентів, пов’язаних з порушеннями автентифікації, міжнародні стандарти та їх порівняння.

Практичне значення одержаних результатів. Розроблені рекомендації застосування комплексної системи автентифікації за допомогою біометричних даних можуть бути використані при розробці та впровадженні систем автентифікації у різних структурах де важливий високий рівень інформаційної безпеки.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

1.1 Основні теоретичні положення, дослідження методів автентифікації суб’єктів

Взаємопов'язані процеси, які разом забезпечують контроль доступу до ресурсів і даних в інформаційних системах називають автентифікацією, ідентифікацією та авторизацією (рис. 1.1).

Рис. 1.1. Взаємопов'язані процеси контролю доступу до ресурсів

Ідентифікація – це процес визначення та надання унікального ідентифікатора для користувача або системи. Ідентифікатор може бути ім'ям користувача, номером ID, електронною адресою або іншим унікальним значенням. Основна ціль визначити, хто намагається отримати доступ до системи. Наприклад, користувач вводить своє ім'я користувача (логін).

Авторизація – це процес визначення прав та дозволів користувача або системи після успішної автентифікації. Він визначає, до яких ресурсів або даних користувач має доступ і які дії він може виконувати. Основна ціль надати або обмежити доступ до ресурсів на основі перевіреної ідентичності. Наприклад,

користувач отримує доступ до певних файлів, але не може змінювати системні налаштування.

Аутентифікація – це процес перевірки та підтвердження ідентичності користувача або системи перед наданням доступу до захищених ресурсів або інформації. Іншими словами, це метод визначення, чи є хтось або щось тим, за кого або що він/воно себе видає. Основна ціль автентифікації переконатися, що користувач є тим, за кого він себе видає. Наприклад, користувач вводить пароль або надає відбиток пальця [1, 2].

Більшість користувачів найбільш знайомі з використанням паролів, які вважаються елементами автентифікації на основі інформації, і це лише частина інформації, яка повинна бути відома користувачеві. Однак існують інші елементи автентифікації та способи їх використання для двофакторної або багатофакторної автентифікації.

Існує три фактори автентифікації, які визначаються як:

1. З паролем: це конфіденційна інформація, якою повинні володіти лише уповноважені організації. Пароль може бути голосовим словом, текстовим рядком, комбінацією символів або персональним ідентифікаційним номером (ПІН-кодом). Пароль дуже простий у використанні, але має свої недоліки, такі як складність його зберігання, крадіжка пароля та ризик злому.

2. Використання пристрою автентифікації: суб'єкт має унікальний елемент, такий як особиста печатка, ключ від замка або електронний файл із певними характеристиками. Цей метод є більш безпечним, оскільки важче отримати викрадений пристрій, і суб'єкт може швидко повідомити про його втрату або крадіжку.

3. Використання біометрії: фізичні характеристики, такі як портрет, відбитки пальців, голос і зір. Цей метод підходить для цієї теми, оскільки вам не потрібно запам'ятовувати пароль або встановлювати пристрій автентифікації. Тим не менш, біометричні системи не тільки мають високу чутливість до маркування авторизованих осіб і відхилення зловмисників з аналогічними параметрами, але з іншої сторони мають високі витрати на впровадження.

Незважаючи на недоліки, біометрія як і раніше залишається найбільш надійним і перспективним фактором автентифікації [3].

Після успішної перевірки автентичності користувача або транзакції зазвичай виконується процес авторизації. Цей процес визначає, чи може аутентифікований суб'єкт отримати доступ до певного захищеного ресурсу або системи. Навіть якщо користувач успішно пройшов автентифікацію, доступ до ресурсу може бути заборонений, якщо він не має відповідних дозволів на використання ресурсу.

Терміни "автентифікація" та "авторизація" можуть використовуватися взаємозамінно, але вони представляють різні функції. Аутентифікація-це процес автентифікації зареєстрованого користувача перед доступом до захищеного ресурсу. З іншого боку, авторизація - це процес визначення того, чи має автентифікований користувач право на доступ до певного ресурсу. Визначення та обмеження доступу до цих ресурсів для певної групи користувачів називається контролем доступу.

Процес автентифікації завжди має пріоритет над процесом авторизації. Давайте розглянемо використання автентифікації. Зазвичай користувачі проходять автентифікацію під час взаємодії з комп'ютерною системою за межами автоматично створеного гостьового облікового запису. Зазвичай користувачі вибирають ім'я користувача або ідентифікатор і вводять дійсний пароль для доступу до системи. Аутентифікація користувача дозволяє взаємодіяти між комп'ютерами, операційними системами, додатками та мережами, що дозволяє захищати певні процеси та технічні системи.

Багато компаній використовують автентифікацію користувачів, які реєструються на своїх веб-сайтах. Він може потрапити в руки кіберзлочинців без належних заходів безпеки, таких як захист даних користувачів, таких як номери дебетових карток та номери соціального страхування.

Організації також використовують аутентифікацію для управління доступом користувачів до корпоративних мереж і ресурсів, комп'ютерів, серверів, додатків і мереж.

Великі компанії та інші організації можуть використовувати єдину систему входу (SSO) для доступу до різних систем, використовуючи єдині облікові дані для входу.

Під час автентифікації, будь то через систему, локальну операційну систему або сервер автентифікації, відповідні дані, що зберігаються у файлі бази даних авторизованого користувача, якщо надані облікові дані збігаються, суб'єкт проходить автентифікацію та має право використовувати ресурс, процес завершується, і користувач може отримати до нього доступ. Тож, якщо зловмисник викраде пароль, він зможе з легкістю потрапити до системи, але при використанні біометричних даних, зловмисник отримає тільки шаблон, але не зможе по ньому пройти аутентифікацію.

Традиційно аутентифікація виконується системою або ресурсом, що надає доступ, наприклад сервером автентифікації користувача, з використанням локально реалізованої системи паролів, що містить ідентифікатор входу (ім'я користувача) і пароль або ідентифікатор і біометричні дані. Передбачається, що знання облікових даних для входу забезпечить дійсність користувача. Кожен користувач зберігає пароль, спочатку призначений або обраний ним самим (або для кожного подальшого використання іншим користувачем, наприклад системним адміністратором, користувач повинен використовувати раніше обраний пароль.

Однак протоколи онлайн-додатків, такі як HTTP та HTTPS, характеризуються відсутністю статусу. Це означає, що під час автентифікації на високому рівні кожного разу, коли кінцевий користувач отримує доступ до ресурсу за допомогою HTTPS, він перевіряється. Замість того, щоб примусити цей процес кожного разу, коли кінцевий користувач взаємодіє по мережі, захищені системи зазвичай використовують аутентифікацію на основі токенів. У цьому випадку аутентифікація виконується 1 раз на початку сеансу. Система автентифікації створює підписаний маркер автентифікації для кінцевого користувача, який додається до кожного запиту від клієнта. Для автентифікації системи та процесу, якщо ці облікові дані автоматично надсилаються цим

пристроєм, цифровий сертифікат, виданий та затверджений центром сертифікації, який діє як ідентифікатор користувача та пароль у інфраструктурі відкритого ключа machine-crt, може використовуватися для перевірки особи під час обміну інформацією. Автентифікація користувача за допомогою ідентифікатора та пароля вважається основним типом автентифікації на основі знань користувача 2 основних відомостей (ім'я користувача та пароль). Біометричний тип автентифікації також називають одноелементною автентифікацією, оскільки він базується лише на 1 елементі і це є перевагою для багатьох систем. На перший погляд, це може показатись більш небезпечним, але в розрізі біометрії це прийнятно, оскільки автентифікація на основі біометричних даних є досить точною та безпечною [4].

Фактори автентифікації визначаються як інформація або атрибути, що використовуються для визначення того, хто запитує доступ до системи. Традиційно виділялися 2 фактори: "те, що Ви знаєте, що у вас є" і "хто Ви є". Проте в останні роки були введені додаткові елементи, такі як місце розташування і час.

Елементи автентифікації, які зараз використовуються, - це різні елементи, такі як PIN-код, ім'я користувача, пароль або інформаційні елементи, що містять відому користувачеві інформацію, таку як відповіді на секретні запитання, які охоплюють дані для отримання текстових повідомлень або створення одноразових паролів.

Ключові елементи, визначені як "хто Ви є", часто базуються на біометричних методах, таких як відбитки пальців, розпізнавання обличчя та сканування сітківки ока. Фактор розташування-це питання: "де Ви". І хоча одного цього елемента недостатньо для автентифікації, його можна використовувати на додаток до інших елементів, допомагаючи усунути деякі запити, які можна точно визначити за допомогою, наприклад, GPS.

Фактор часу: "коли Ви автентифікуєтесь", цей елемент діє як додатковий механізм для запобігання спробам несанкціонованого доступу, коли авторизовані користувачі не можуть отримати доступ до ресурсів. Його також

можна використовувати в поєднанні з коефіцієнтом положення для забезпечення більш ефективного управління.

Разом факторів розташування та часу недостатньо для самоідентифікації, але вони можуть доповнювати інші фактори та створювати багатофакторні методи безпеки. Сучасні смартфони з GPS та іншими технологіями можуть допомогти з багатофакторною аутентифікацією. Це полегшує визначення місцезнаходження користувача та часу входу [5].

1.2. Огляд сучасних методів автентифікації користувачів за допомогою біометричних даних

Біометрія - це набір автоматизованих методів та інструментів, що використовуються для перевірки особистості людини на основі фізіологічних або поведінкових характеристик . Фізіологічні особливості включають відбитки пальців, форму руки, риси обличчя, райдужну оболонку і т. д (рис. 1.2). Поведінкові характеристики включають такі аспекти, як динаміка підписів, голосова ідентифікація, динаміка натискання клавіш та інші характеристики, які можуть бути придбані або покращені з часом [6].

Рис 1.2. Різні системи біометричного захисту

Біометрія функціонує як унікальна і кількісна характеристика людини для автоматичної ідентифікації або перевірки. Термін "автоматизований" означає, що біометричні системи повинні швидко і автоматично ідентифікувати або перевіряти особу в режимі реального часу.

Процес ідентифікації за допомогою біометричної системи передбачає порівняння первинного біометричного зразка з нещодавно отриманими біометричними даними.

В області біометрії важливо розрізняти поняття ідентифікації та перевірки. Що стосується ідентифікації, система може визначити, кому вона належить, порівнюючи конкретний біологічний зразок з базою даних, щоб знайти відповідність [7].

З іншого боку, перевірка - це порівняння, при якому біометричні системи перевіряють особистість людини. У цьому випадку новий біометричний зразок порівнюється з раніше зареєстрованим зразком. Порівнюючи ці 2 приклади, система підтверджує, що ця людина дійсно той, за кого себе видає. Під час процесу ідентифікації система один екземпляр порівнює з багатьма різними екземплярами, а процес автентифікації або перевірки порівнює їх "один з одним". "Система ідентифікації запитує:" Хто Ви?". В цей момент Ви надаєте свій біометричний ідентифікатор. "Система перевірки говорить: "Чи Ви дійсно говорите, Хто Ви?", порівнюючи вашу біометрію з шаблоном в базі даних.

Аутентифікація дозволяє лише автентифікованим користувачам отримувати доступ до комп'ютерних систем, мереж, баз даних, веб-сайтів та інших мережевих або сервісних програм [8, 9].

Включення декількох елементів автентифікації в звичайний процес автентифікації зазвичай підвищує рівень безпеки. Довірена автентифікація зазвичай використовує принаймні 2 різні типи факторів. Наприклад, імена користувачів та паролі можна розглядати як 2 інформації, але ця різниця важлива, оскільки їх використання в базовій автентифікації за допомогою 2 інформації не вважається формою 2-факторної автентифікації (2FA).

Двофакторна автентифікація зазвичай включає елемент інформації та біометричний або власний елемент, такий як маркер безпеки. Цим маркером безпеки може бути одноразовий код підтвердження, отриманий у текстовому повідомленні, або код підтвердження, згенерований програмою автентифікації на зареєстрованому мобільному телефоні.

Багатофакторна автентифікація разом з використанням біометричної автентифікації може бути досить надійною. Тому що, недостатньо мати тільки один з факторів безпеки. Така система показує дуже високу ефективність від недопущення нелегітимних користувачів до ресурсів системи і може бути використана як спосіб доступу не тільки до всієї системи, але й конкретних ресурсів, таких як певні директорії, тощо [10].

1.3. Огляд сучасних методик біометричної автентифікації користувачів

Метод ідентифікації осіб за відбитками пальців ґрунтується на унікальності малюнка шкіри, що складається з папілярних ліній, які знаходяться на поверхні долоні та пальців. Ці лінії створюють характерний візерунок, який вважається незмінним упродовж життя людини. У методі відрізняють два типи ознак: глобальні та локальні.

Глобальні ознаки охоплюють зовнішній вигляд відбитку, його орієнтацію, кривизну і поле напрямків, що визначає загальне розташування папілярних ліній. Ці ознаки можна спостерігати без спеціального обладнання.

Локальні ознаки включають область візерунка, де локалізовані всі глобальні ознаки. Також визначаються такі елементи, як ядро (центр), пункт "дельта" (початкова точка поділу або з'єднання борозенок папілярних ліній), тип лінії (дві найбільші лінії, які спочатку паралельні, а потім розходяться і огинають всю область одразу), і лічильник ліній (число ліній на області образу або між ядром і пунктом "дельта") (рис. 1.3).

Рис. 1.3. Аутентифікація за відбитком пальця

Метод класифікації відбитків пальців, який базується на типах папілярного візерунку, є одним із ключових підходів у сучасній криміналістиці. Кожен з цих типів має свої характеристики, які можуть бути використані для ідентифікації особи [11].

Тип "петля" відбитків може бути поділений на ліву, праву, центральну та подвійну. Ліві та праві петлі мають криволінійні лінії, що повертаються в напрямку, зворотному до початкової точки. Центральна петля має одну центральну точку, а подвійна містить дві петлі.

Тип "дельта" або "дуга" характеризується простими або гострими кутами, які можна спостерігати у відбитках пальців. Ці кути можуть бути використані для визначення конкретного типу дельти або дуги.

Тип "спіраль" має центральну або змішану структуру. Центральна спіраль характеризується обертанням ліній навколо центральної точки, тоді як змішана спіраль містить елементи обох підтипів.

Місцеві особливості, які відомі як мінуції або "точки Гальтона", є важливими для ідентифікації відбитків пальців. Ці точки представляють унікальні варіації у папілярному візерунку, такі як закінчення, роздвоєння або розриви. Вони слугують як унікальні маркери, які дозволяють відрізняти відбитки пальців між різними особами.

Зважаючи на ріст кількості електронних пристроїв, що вимагають безпечного доступу, біометричні технології стають все більш популярними як засіб автентифікації.

Одним із поширених варіантів є використання геометрії руки для ідентифікації особи. Ця методика базується на тому, що кожна людина має унікальну форму та структуру кисті руки, включаючи розміри пальців, їх вигини, ширина і товщина долоні, а також дрібні деталі, такі як зморшки на шкірі.

Для здійснення біометричної автентифікації за формою руки використовується спеціальний сканер, який може бути вбудованим у пристрої (наприклад, в смартфоні) або окремим пристроєм (наприклад, в системі безпеки корпоративного офісу). Сканер вимірює різні параметри руки, такі як довжина пальців, їх вигини, а також структуру кісток і суглобів [12, 13].

Що стосується процесу автентифікації, спочатку користувачу потрібно зареєструвати свою кисть руки у системі. Це може включати сканування кисті з різних кутів для отримання повного тривимірного образу. Після реєстрації кисті руки в системі, для подальшого доступу користувачу просто необхідно пройти процедуру сканування руки, яка порівнюється з зареєстрованим шаблоном.

Технологія автентифікації за геометрією руки має декілька переваг. По-перше, вона не вимагає фізичного контакту з пристроєм, що робить її більш гігієнічною, особливо у випадку використання в сферах охорони здоров'я чи фінансових установ. По-друге, вона може бути відносно швидкою та зручною для кінцевого користувача, оскільки процес сканування може бути автоматизованим та миттєвим. Її безпека базується на унікальних фізичних характеристиках кожної особи, що робить її важко підпорядкованим атакам імітації чи підробки.

Проте, як і у будь-якій технології, є і певні виклики та обмеження. Наприклад, зміни в структурі кісток або суглобів через травми чи хвороби можуть вплинути на ефективність сканування. Також можливість ампутації чи інших фізичних змін у кисті руки можуть ускладнити або унеможливити аутентифікацію.

Системи автентифікації, які використовують геометрію долоні, з'явилися на початку 70-х років і швидко знайшли широке застосування. Вони базуються на унікальних параметрах, які завжди присутні у людини і залишаються сталими

протягом життя, таких як контур і структура долоні, розташування зморшок, вигини пальців та інші характеристики [14].

Однак, одним з основних недоліків цієї технології є можливість насильного вилучення і використання біометричних даних. У фільмах і анімаційних стрічках часто демонструються ситуації, коли ампутується рука або відбувається викрадення очей для обману біометричних систем. Це показує, що, хоча біометричні дані неможливо передати третім особам, їх можна фізично вилучити та використати для несанкціонованого доступу (рис. 1.4).

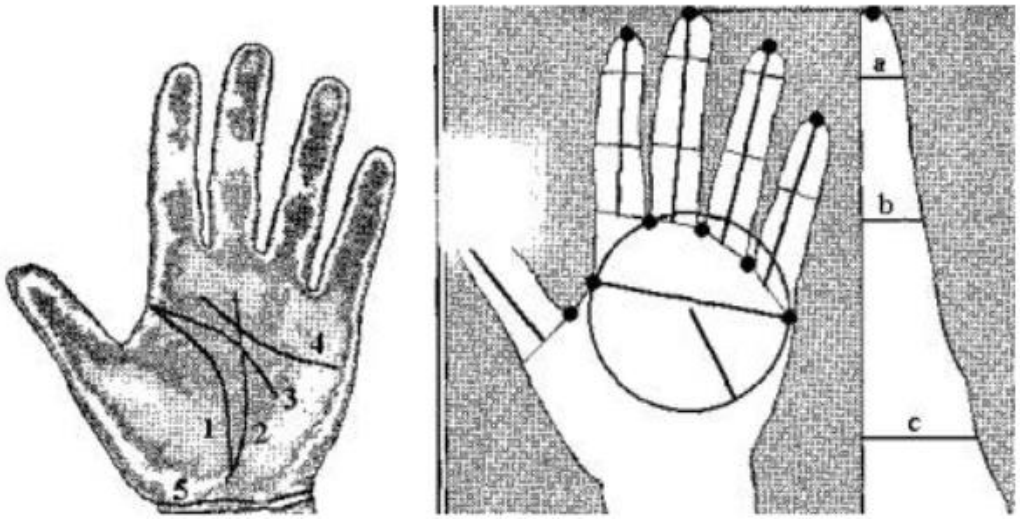

Рис. 1.4. Системи автентифікації, що використовують геометрію долоні

У цьому контексті виявляється перевага васкулярної автентифікації, яка базується на скануванні унікальних венозних мереж у долоні. Цей метод дозволяє ідентифікувати лише живу людину, оскільки венозна система перебуває в постійному русі тільки в живих організмах. Таким чином, васкулярна аутентифікація забезпечує більш високий рівень безпеки, оскільки неможливо використати аутентифікаційні дані, якщо особа не присутня [15].

Судинна аутентифікація використовує розпізнавання зображень і оптичну технологію для сканування вен долоні, тильної сторони долоні, невидимих структур пальців і інших областей. Цей метод дуже точний і стійкий до підробок, підміни та інших зловмисних дій.

Найбільш актуальним методом автентифікації в новітніх біометричних рішеннях є використання вен на долонях, що забезпечує високу точність і безпеку. Кровоносні судини створюють унікальну модель для кожної людини. Ця технологія широко використовувалася лише 5-10 років тому, але вона є однією з найновіших у галузі біометрії.

Його головна перевага полягає в тому, що ці венозні структури знаходяться всередині тіла, а не зовні. Таким чином, цей метод автентифікації є більш біологічно безпечним порівняно з іншими методами, оскільки ви не зможете вкрасти фотографії, підробити їх або використовувати інші подібні методи.

Коли долоня освітлюється ближнім інфрачервоним світлом, гемоглобін у крові підсилює це світло, відбиваючи вену у вигляді темного малюнка на тлі іншого зображення. В результаті область долоні, яка використовується для автентифікації, фотографується в ближньому інфрачервоному світлі. Візерунки у вигляді прожилок з'являються під час обробки зображень і подальшого розпізнавання. Щоб авторизувати користувача, унікальний зразок вени порівнюється з попередньо збереженим екземпляром, зашифрованим в базі даних, на смарт-карті або на іншому носії.

Існує 2 способи отримання зображення вен долоні: метод відображення і метод передачі інфрачервоного світла. Метод відображення дозволяє об'єднати всі компоненти пристрою в 1 корпус, щоб зменшити його розмір і спростити використання (вам не потрібно нікуди приклеювати руки). У методі передачі інфрачервоного світла використовується підсвічування тильної сторони долоні і камера, відфільтрована з долоні, для отримання більш детального зображення. У процесі додаток аналізує дані та створює цифровий шаблон без прямого контакту з людьми [16].

Методика ефективна, її ефективність порівнюється з розпізнаванням райдужної оболонки ока, у багатьох відношеннях вона перевершує її, а в деяких випадках поступається. Значення коефіцієнта помилкового відхилення (FRR) і коефіцієнта помилкового прийняття (FAR) для сканерів вен долоні з FRR 0,01%,

за даними розробника, FAR на рівні 0,0008%. Більш детальні графіки для різних значень не були надані жодним виробником.

Біометрична технологія, яка використовує унікальні властивості та характеристики райдужної оболонки. Райдужна оболонка - це тонка рухома діафрагма ока з отвором (зіницею) в центрі, за рогівкою і перед лінзою. Ця структура формується до народження і залишається незмінною протягом усього життя. Текстура райдужної оболонки має складний малюнок, і для забезпечення високої ефективності автентифікації можна вибрати близько 200 точок, але в кращій системі відбитків пальців використовується тільки 60-70 точок (рис. 1.5).

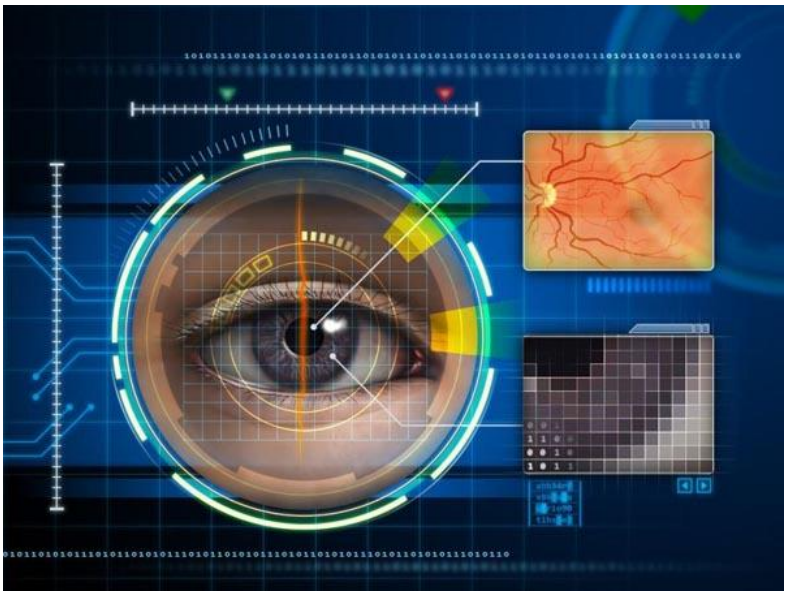

Рис. 1.5. Технологія біометричної автентифікації особистості використовує унікальні ознаки та особливості райдужної оболонки ока

Технологія розпізнавання райдужної оболонки ока призначена для запобігання втручанням, які зазвичай асоціюються зі скануванням сітківки. Для цього процесу використовується інфрачервоне або яскраве світло. Дослідження показали, що сітківка може змінюватися з часом, тоді як райдужна оболонка залишається стабільною. Важливо відзначити, що неможливо знайти абсолютно однакові 2 малюнки райдужної оболонки навіть у близнюків.

Процедура отримання окремого запису райдужної оболонки передбачає фотографування чорно-білою камерою, яка створює 30 записів в секунду. Для освітлення райдужки використовується інфрачервоне світло та невидиме світло. Зображення оцифровуються, а потім зберігаються для порівняння і можуть бути автоматизовані за допомогою голосових підказок і автофокусування. Цей метод автентифікації зазвичай чутливий до окулярів і контактних лінз [17].

Метод автентифікації за сітківкою вперше був представлений в середині 50-х років минулого століття. У той час на очному дні встановлюється унікальний візерунок вен, і навіть у близнюків ці візерунки не перетинаються. Для сканування сітківки використовується низько інтенсивне інфрачервоне випромінювання, яке спрямовується від зіниці до кровоносних судин на задній поверхні ока. З отриманого сигналу виділяються сотні особливих точок, інформація про які зберігається в шаблоні.

Одним з недоліків такої системи є психологічний фактор: не кожному хочеться бачити у своєму оці незрозумілу темну дірку, в якій щось світиться. Крім того, такі системи вимагають чіткого зображення і зазвичай схильні до неправильного розташування сітківки. З цієї причини важливо бути особливо обережним, а наявність певних захворювань, таких як катаракта, може ускладнити використання цього методу. Сканер сітківки ока забезпечує найнижчу ймовірність першого типу помилки (доступ заборонено зареєстрованим користувачам) і майже нульовий відсоток другого типу помилки, тому доступ до надсекретних об'єктів неможливий. Біометрична автентифікація на основі геометрії людини є широко використовуваним методом ідентифікації та автентифікації людини. Технічне застосування цього методу є складним і широко використовується при розробці багатьох сучасних технологій.

Використання великої кількості відеокамер у місцях масового скупчення людей, таких як вокзали, аеропорти, площі, вулиці та дороги, стало важливим фактором розвитку напрямку біометрії. Для створення 3D-моделі обличчя людини виділяються контури очей, брів, губ, носа та інших елементів обличчя.

Потім розраховується відстань між цими елементами, і на основі цього розрахунку створюється тривимірна модель. Щоб створити унікальний шаблон, який підходить конкретній людині, потрібно врахувати від 12 до 40 характерних елементів [18].

Діапазон варіацій у біометричних системах може змінюватися залежно від конкретного застосування, такого як ідентифікація, аутентифікація або віддалений пошук на великих територіях. Деякі алгоритми можуть компенсувати наявність різних аксесуарів, таких як окуляри, капелюхи, вуса чи борода.

Одним з інноваційних методів є використання термограм для біометричної автентифікації. Цей підхід базується на унікальності термограми для кожної особи і використовує камери інфрачервоного діапазону для запису теплових візерунків обличчя та інших областей. У порівнянні з іншими методами, такими як розпізнавання за геометрією обличчя, термальна біометрія розрізняє близькі за фізичними характеристиками особи, наприклад, близнюків.

Однією з головних переваг цього методу є те, що точність термограми не піддається впливу зовнішніх факторів, таких як використання масок, старіння організму чи зміни температури тіла. На відміну від інших методів, аутентифікація на основі термограми може ідентифікувати людину на відстані до десятків метрів, що робить її відмінним варіантом для використання у великих просторах або для віддаленого пошуку.

Додатково, технологія відображення шкіри, яка використовується у цьому методі, стала доступною завдяки новим сенсорам, таким як чіпи, розробленим корпорацією "Люмідінм" (Lumidinm). Ці чіпи можуть вимірювати відображення ближнього інфрачервоного світла від шкіри, що забезпечує їх ефективне використання для біометричної автентифікації. Цей метод є важливим у контексті маленького розміру чіпа та відсутності проблем з реєстрацією, які можуть виникати в інших системах.

ДНК, як біометричний параметр, є особливо цінним у сфері ідентифікації та розслідування злочинів. Він служить унікальним "цифровим підписом" для кожної особи, оскільки містить інформацію про генетичний склад клітин, що є

унікальним для кожного індивіда. Проте, слід зазначити, що однаковий генетичний код може бути у однояйцевих близнюків, що становить обмеження використання ДНК для ідентифікації в таких випадках.

В сучасному світі аналіз ДНК широко застосовується в судовій практиці для встановлення родинних зв'язків, визначення батьківства, ідентифікації осіб у злочинах, а також для проведення генетичних досліджень. Проте, порівняння ДНК-зразків може бути складним і дорогим процесом, а отже, вимагає великої уваги до деталей та стандартів.

При ідентифікації за ДНК важливо враховувати різноманітність генетичних алелей у різних локусах геному. Це означає, що для точної ідентифікації необхідно аналізувати не лише наявність певних алелей, але і їх комбінації, що може бути досить складним завданням.

Однією з ключових проблем, пов'язаних з використанням ДНК для ідентифікації, є конфіденційність інформації. Генетичний код може містити чутливі дані про особу, які можуть бути використані для незаконних цілей, таких як розкриття медичних аспектів, визначення схильності до захворювань, або навіть розкриття особистої інформації про походження або етнічне походження.

Щодо іншого біометричного параметра – форми вух – він здобуває все більше уваги в сучасних дослідженнях. Аналізуючи структуру вуха, вчені розробляють методи для автоматичної ідентифікації осіб. Це може бути корисно у судових дослідженнях, де ідентифікація осіб може відігравати ключову роль у вирішенні справ.

Таким чином, як ДНК, так і форма вуха представляють собою потужні інструменти для ідентифікації осіб, проте кожен з них має свої переваги та обмеження, які потрібно враховувати при їхньому використанні.

Інтерес до розпізнавання за формою вух зріс внаслідок проекту "Ідентифікація людини на відстані". Аналіз основних елементів вуха схожий на методику аналізу особистостей. Однак, використання лише розпізнавання за формою вуха менш ефективне порівняно з розпізнаванням за обличчям. Поєднання зображень обличчя і вуха підвищує точність ідентифікації [19].

Тривалий час відомо, що особистий запах може служити інструментом ідентифікації людини. Завдяки прогресу в хімічному аналізі з використанням напівпровідників були розроблені "електронні носи", які здатні вимірювати концентрацію різних хімічних елементів. Важливо відзначити, що ці сенсори мають свої обмеження і не мають такої ж розпізнавальної здатності як у людей. Також вони потребують калібрування і можуть погано функціонувати в умовах перенасичення запахами. Однак, нормалізувати вплив різних факторів на запах людини може бути складно.

Голос, як поведінковий біометричний параметр, залежить від різних фізичних характеристик і може бути унікальним для кожної людини (рис. 1.6). Ідентифікація особи за голосом є традиційним методом розпізнавання, який можна застосовувати для визначення співрозмовника по телефону та виявлення емоційного стану за голосовими особливостями.

Рис. 1.6. Технологія біометричної автентифікації особистості за голосом

Метод біометричної автентифікації за голосом відрізняється простотою в застосуванні, вимагаючи лише мікрофона та звукової плати, і широко використовується в бізнес-центрах. Існує різноманітність підходів до створення шаблонів за голосом, що включають різні комбінації частотних і статистичних характеристик, таких як модуляція, інтонація та висота тону.

Однак основним недоліком методу автентифікації за голосом є його низька точність. Голос піддається значним змінам під впливом емоцій та стану здоров'я людини, а також може погіршуватися через зовнішні фактори, такі як шуми чи перешкоди при передачі голосової інформації.

Незважаючи на труднощі, які виникають через зміни в голосі, існуючі системи розпізнавання за голосом використовуються в різних сферах, таких як управління доступом в приміщеннях середнього рівня безпеки [20].

Метод біометричної автентифікації за рукописним почерком ґрунтується на унікальних рухах руки людини під час підпису документів. Зазвичай для збереження підпису використовують спеціальні ручки або поверхні, які реагують на тиск. Цей метод використовує підпис особи як основний елемент для автентифікації, і шаблон створюється в залежності від рівня захисту, застосовуючи статичний або динамічний підхід до обробки даних.

Статичний метод ґрунтується на порівнянні самого підпису, використовуючи ступінь збігу двох зображень, але його недоліком є менша надійність через велику варіабельність підпису. Динамічний метод, натомість, враховує динамічні характеристики написання, такі як швидкість руху руки, сила тиску і тривалість етапів підпису, що забезпечує вищу точність.

Деякі системи використовують складніші сенсори, які записують напрямок п'яти вимірних векторів у тривимірному просторі, що дозволяє забезпечити додатковий рівень захисту від фальсифікацій.

Динамічна верифікація підпису включає ряд вимірювань, таких як евклідова відстань між траєкторією руки, параметри просторових взаємозв'язків та інші аспекти. При збігу підпису з еталоном система додає до документа параметри підпису, які включають десятки характеристик динаміки руху, такі як напрямок, швидкість і прискорення. Ці дані піддаються шифруванню, і після цього обчислюється контрольна сума, яка також шифрується, утворюючи біометричну мітку. Для налаштування системи користувач повторює процедуру підпису документа кілька разів, щоб отримати усереднені показники та довірчий інтервал.

Ідентифікація за клавіатурним почерком - це процес визначення унікального стилю друку людини на основі її взаємодії з клавіатурою. Усі мають свої власні особливості, такі як час натискання та утримання клавіш.

Існують системи, які використовують штучні нейронні мережі для розрізнення між особами за їхнім клавіатурним почерком. Вчені виявили, що відмінності між людьми стають більш помітними, коли враховують тимчасові інтервали між натисканням клавіш та тривалість утримання.

Системи ідентифікації за клавіатурним почерком можуть базуватися на введенні фіксованого слова або діяти незалежно від тексту, введеного користувачем. У деяких дослідженнях запропоновано метод ідентифікації за клавіатурним почерком на основі змінних віртуальних клавіатур, що відрізняються для кожного оператора в автоматизованих інформаційно-керуючих системах. Користувач використовує "свою" віртуальну клавіатуру протягом тривалого часу, щоб система могла аналізувати його клавіатурний почерк і визначити індивідуальні навички та характеристики введення тексту.

Висновки до розділу 1

Дослідження зосереджено на теоретичних аспектах та методах автентифікації суб’єктів на основі біометричної інформації. Оглянуто сучасні методики біометричної автентифікації користувачів. Вивчені методи збору, обробки та зберігання біометричних даних.

Виявлено, що біометрична аутентифікація ґрунтується на унікальних фізіологічних або поведінкових характеристиках особи, таких як відбитки пальців, обличчя, голос та інші, що можна використовувати для ідентифікації. Кожна з цих методик має свої переваги та недоліки, і їх вибір залежить від конкретного застосування та вимог до точності та безпеки.

Проаналізовано сучасні методи автентифікації користувачів на основі біометричних даних, такі як відбитки пальців, розпізнавання обличчя, голосова аутентифікація тощо. Встановлено, що кожен з цих методів має свої переваги та

обмеження, і вибір методу залежить від конкретних вимог до безпеки та точності.

Розділ 2 ДОСЛІДЖЕННЯ ПРОБЛЕМ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ТА ОБҐРУНТУВАННЯ МОЖЛИВИХ РІШЕНЬ

2.1 Огляд підходів до біометричної автентифікації користувачів

Всі системи біометричної автентифікації виконують дві ключові функції:

1. Реєстрація:

- функція включає збір декількох вимірювань з біометричного пристрою;
- отримані вимірювання конвертуються у цифрове представлення біометричної характеристики, наприклад, у вигляді шаблону або моделі;
- цифрове представлення унікально відповідає конкретній зареєстрованій особі.

2. Розпізнавання:

- під час розпізнавання зчитувальний пристрій отримує одне або кілька вимірювань біометричної характеристики;
- отримані вимірювання перетворюються у цифрову форму, що може бути використана для подальшої обробки.

Потім ця цифрова форма порівнюється з двома різними методами:

1) верифікація, або порівняння "один до одного", полягає у порівнянні біометричного шаблону з єдиним шаблоном, вибраним за попереднім номером або кодом. Результатом є числова оцінка ймовірності того, що порівнювані шаблони відповідають одній особі;

2) ідентифікація, або порівняння "один до багатьох", полягає у порівнянні біометричного шаблону з усіма зареєстрованими шаблонами без попереднього вибору. Результатом є список найбільш схожих шаблонів, і за допомогою математичних критеріїв приймається рішення про ідентичність шаблонів [21].

Всі біометричні системи працюють за подібною схемою. Спочатку вони фіксують біометричний зразок під час процесу запису. Це може включати кілька замірів для отримання найточнішого представлення характеристики. Зібрана інформація обробляється та перетворюється в математичний код.

Крім того, система може вимагати виконання додаткових дій для пов'язання зразка з конкретною особою. Наприклад, персональний ідентифікаційний номер (user ID) може бути прикріплений до зразка або використовуватися смарт-карта, яка містить зразок. В такому випадку створюється новий біометричний зразок та порівнюється з вже наявним.

Ідентифікація за допомогою будь-якої біометричної системи складається з чотирьох основних кроків:

1) запис - біометричний зразок фіксується та зберігається для подальшого використання;

2) виділення - унікальна інформація виділяється з отриманого зразка для створення біометричного шаблону або еталону;

3) порівняння - записаний зразок порівнюється з еталоном, який може бути взятий з бази даних;

4) визначення збігу/розбіжності - система вирішує, чи збігаються біометричні зразки, і приймає відповідне рішення щодо ідентифікації особи.

Важливо зазначити, що, на відміну від ідентифікації за допомогою паролів або ключів, біометричні системи базуються на ймовірностях, оскільки існує завжди мала можливість того, що дві особи можуть мати схожі біологічні характеристики.

Біометрична ідентифікація використовує такі ключові терміни:

- коефіцієнт помилкової відмови в доступі (FRR - False Rejection Rate): Ймовірність того, що система не розпізнає суб'єкта, і доступ забороняється правильному користувачеві;
- коефіцієнт помилкового допуску (FAR - False Acceptance Rate) - ймовірність того, що одна особа буде визнана іншою, що може призвести до надання доступу неавторизованому користувачеві;

- рівень рівних помилок (EER - Equal Error Rate) - коефіцієнти, при яких обидві помилки (FRR = FAR) є однаковими;
- крива ROC (Receiver operating characteristic curve) - графік, що оцінює компроміс між FAR та FRR та визначає, наскільки близько зразок має бути до шаблону для визначення його як збігу [22].

На сьогоднішній день існує розмаїття методів біометричної автентифікації, які можна поділити на дві основні категорії: статичні та динамічні.

Статичні методи ґрунтуються на фізіологічних характеристиках людини, які є сталими протягом усього життя, від народження до смерті. Ці характеристики є унікальними для кожної особи і неможливо втратити, вкрасти або скопіювати.

Серед статичних методів можна виділити:

- відбитки пальців;
- форма/геометрія долоні;
- розташування вен на тильній стороні долоні;
- райдужна оболонка ока;
- сітківка ока;
- форма/геометрія обличчя (2D / 3D);
- ДНК суб’єкта;
- форма вух.

Динамічні методи автентифікації базуються на унікальних поведінкових рисах людини, які виявляються через характерні підсвідомі рухи, що виникають під час виконання звичних дій. Ці методи включають в себе:

- голос;
- рукописний почерк;
- клавіатурний почерк;
- хода;
- рух губ.

Ці методи використовуються для впізнавання особи на основі її унікальних підсвідомих рухів, що є важливою складовою системи біометричної автентифікації [23].

2.2 Проблеми біометричної автентифікації користувачів

Біометрія – це наука, що займається вимірюванням і статистичним аналізом фізичних та поведінкових характеристик людей. Вона використовується для ідентифікації та автентифікації осіб, забезпечуючи високий рівень безпеки та точності.

Біометрія ґрунтується на вимірюванні та аналізі унікальних фізичних і поведінкових характеристик людини для ідентифікації та автентифікації. Основна ідея полягає в тому, що певні характеристики кожної людини є неповторними і можуть бути використані для точного розпізнавання [24].

Фізичні характеристики біометрії (рис. 2.1) - це атрибути, які є відносно незмінними і унікальними для кожної людини:

- відбитки пальців - унікальні візерунки гребінців та долин на пальцях. Відбитки пальців використовуються вже більше століття в криміналістиці та сучасних системах безпеки;
- розпізнавання обличчя - використовує геометричні характеристики обличчя, такі як відстань між очима, форма носа та щелепи;
- сітківка ока - візерунки, що утворюються кровоносними судинами на сітківці, або кольорові візерунки на ірисі, є унікальними для кожної людини;
- форма руки - використання довжини, ширини та форми руки або пальців;
- структура вен - розпізнавання унікального розташування вен на руці чи пальці.

Рис. 2.1 Фізіологічні характеристики біометрії

Поведінкові характеристики (рис. 2.2) - це динамічні риси, які можуть змінюватися з часом, але все одно мають унікальні індивідуальні патерни:

- голос - аналіз тембру, висоти, частоти та інших характеристик голосу;
- підпис - динаміка написання підпису, включаючи швидкість, тиск та траєкторію;
- манера ходьби - спосіб, яким людина ходить, включаючи ритм, довжину кроку та інші параметри;
- динаміка введення тексту - швидкість та ритм введення тексту на клавіатурі [25-27].

Рис. 2.2 Поведінкові характеристики біометрії

Принципи роботи біометричних систем:

1) збір біометричних даних - спеціальні сенсори або пристрої збирають біометричні дані. Наприклад, сканери відбитків пальців, камери для розпізнавання обличчя або мікрофони для аналізу голосу;

2) передача даних та попередня обробка - зібрані дані передаються до системи для обробки та порівняння. Також, на цьому етапі дані обробляються для виділення унікальних характеристик. Це може включати фільтрацію шуму, нормалізацію та інші методи;

3) обробка даних - система обробляє отримані біометричні дані, перетворюючи їх на числові значення або шаблони для подальшого збереження;

4) зберігання - витягнуті характеристики зберігаються в базі даних для подальшого порівняння. Зазвичай вони зберігаються у вигляді математичних моделей або шаблонів;

5) порівняння з шаблонами - під час спроби входу виконується процес ідентифікації - нові зібрані дані порівнюються з збереженими шаблонами для визначення збігу;

6) визначення відповідності - на цьому етапі виконується процес автентифікації коли система визначає, чи відповідають представлені біометричні дані збереженим шаблонам;

7) прийняття рішення - на основі результатів порівняння система приймає рішення про доступ користувача до системи чи відмову у доступі. Це процес авторизації;

8) виконання дій - якщо користувач відповідає збереженим шаблонам, йому надається доступ до системи. Якщо ні, доступ може бути відхилений;

9) аудит та журналювання - всі дії користувачів та результати автентифікації реєструються для подальшого аналізу та аудиту [28].

З огляду на всі фактори описані вище, можна зрозуміти, що система з використанням біометричних даних для автентифікації користувачів є досить надійною та безпечною. При такому підході до побудови системи автентифікації

мінімізуються проблемні фактори, які б могли виникнути при побудові класичної системи, наприклад, на основі паролів. Але все ж таки не можна сказати, що ця система є ідеальною.

Проблеми біометричної автентифікації користувачів пов'язані з кількома ключовими аспектами, включаючи безпеку, конфіденційність, технічні обмеження та юридичні питання [29].

Безпека:

- вразливість до зловживань - однією з головних проблем є можливість зловмисників отримати та використати біометричні дані для шахрайства. Наприклад, високоякісні зображення відбитків пальців або обличчя можуть бути використані для створення підроблених біометричних зразків;
- компрометація біометричних даних - на відміну від паролів, біометричні дані не можна змінити. Якщо ці дані будуть скомпрометовані, їх не можна просто "перезавантажити" або замінити, як це можливо з паролями.

Конфіденційність:

- збирання та зберігання даних - використання біометричних даних вимагає збирання та зберігання особистої інформації, що може бути використано для відстеження або профілювання користувачів. Це створює ризики для конфіденційності, особливо якщо дані зберігаються централізовано;
- довіра користувачів - багато користувачів можуть бути занепокоєні через можливість зловживань їхніми біометричними даними, що може знизити довіру до систем, які використовують біометричну автентифікацію.

Технічні обмеження:

- точність та надійність - біометричні системи можуть мати проблеми з точністю, особливо в умовах поганого освітлення або якщо користувач має фізичні зміни, такі як поранення пальця або зміни в зовнішності. Також можуть виникати помилкові спрацьовування або відмови в доступі;
- сумісність та масштабованість - впровадження біометричних систем може вимагати значних технічних ресурсів і бути складним для інтеграції з

існуючими системами безпеки. Крім того, масштабованість таких рішень для великих організацій може бути викликом.

Юридичні питання:

- правові норми та регулювання - використання біометричних даних регулюється різними законодавствами, що можуть вимагати дотримання певних стандартів захисту даних та конфіденційності. Недотримання цих вимог може призвести до юридичних наслідків та штрафів;
- права користувачів - існують питання щодо прав користувачів на доступ до своїх біометричних даних, їх виправлення та видалення. Організації, які використовують біометричну автентифікацію, повинні забезпечити відповідні механізми для управління цими правами.

Ці проблеми потребують ретельного вирішення, щоб забезпечити ефективність, безпеку та прийняття біометричної автентифікації користувачами. Важливим є також забезпечення балансу між зручністю для користувачів та захистом їхніх прав та даних.

2.3 Порівняння та рекомендації щодо методів біометричної автентифікації користувачів

Сучасні методи та методики біометричної автентифікації включають різноманітні технології, які використовують фізичні або поведінкові характеристики людини для підтвердження її особи. Кожен з методів має свої особливості, переваги та області застосування [30].

Одним із найпоширеніших методів є використання відбитків пальців. Ця технологія передбачає сканування відбитків пальців за допомогою спеціальних сенсорів, які аналізують унікальні візерунки гребенів та долинок на поверхні пальців. Відбитки пальців мають високу точність і швидкість автентифікації, що робить цей метод популярним у багатьох сферах, включаючи смартфони та системи контролю доступу.

Методика 1:

- використання сенсорів для сканування відбитків пальців;
- аналіз унікальних візерунків гребнів та долинок на поверхні пальців.

Переваги методики:

- висока точність і швидкість автентифікації;
- можливість використання в різних умовах освітлення.

Розпізнавання обличчя також є зручним і ефективним методом біометричної автентифікації. За допомогою камер знімаються зображення обличчя, а потім аналізуються структурні характеристики, такі як відстань між очима, форма носа та контури щелепи. Цей метод є зручним для користувачів і є досить поширеним в сучасному світі, для прикладу використовується для входу в банківські додатки.

Методика 2:

- використання камер для знімання зображення обличчя;
- аналіз структурних характеристик обличчя, таких як відстань між очима, форма носа, контури щелепи, тощо.

Переваги методики:

- зручність і безконтактне використання;
- широке розповсюдження і прийняття в різних додатках.

Ще одним високотехнологічним методом є розпізнавання райдужки ока. Для цього використовуються спеціалізовані камери, які сканують райдужну оболонку ока і аналізують її унікальні візерунки. Розпізнавання райдужки забезпечує високу точність і надійність автентифікації, а також стійкість до змін у зовнішньому вигляді, таких як носіння окулярів чи контактних лінз.

Методика 3:

- використання спеціалізованих камер для сканування райдужної оболонки ока;
- аналіз унікальних візерунків райдужки.

Переваги методики:

- висока точність і надійність;

- стійкість до змін у зовнішньому вигляді.

Розпізнавання голосу базується на аналізі акустичних характеристик голосу, таких як тон, тембр і інтонація. Цей метод є легким у використанні та інтеграції в телефонні та комп'ютерні системи, що робить його зручним для користувачів і ефективним для автентифікації без фізичного контакту.

Методика 4:

- аналіз акустичних характеристик голосу, таких як тон, тембр, інтонація;
- використання мікрофонів для запису голосу.

Переваги методики:

- легкість у використанні та інтеграції в телефонні та комп'ютерні системи;
- можливість автентифікації без фізичного контакту.

Сучасні системи безпеки також використовують розпізнавання за геометрією долоні та вен. Цей метод передбачає використання інфрачервоного світла для сканування візерунків вен під шкірою долоні та аналіз унікальної геометрії долоні і вен. Він забезпечує високу точність і безпеку, оскільки вени не можна підробити або скопіювати.

Методика 5:

- використання інфрачервоного світла для сканування візерунків вен під шкірою долоні;
- аналіз унікальної геометрії долоні та вен.

Переваги методики:

- висока точність і безпека;
- неможливість підробки або копіювання.

Розпізнавання за динамікою натискання клавіш є іншим цікавим методом біометричної автентифікації. Він передбачає аналіз часу та ритму натискання клавіш під час введення пароля або тексту. Цей метод є непомітним для користувача і може використовуватися на звичайних клавіатурах без додаткового обладнання.

Методика 6:

- аналіз часу та ритму натискання клавіш під час введення пароля або тексту;
- використання програмних засобів для збору та аналізу даних.

Переваги методики:

- непомітність для користувача;
- можливість використання на звичайних клавіатурах без додаткового обладнання.

Поведінкові характеристики, такі як спосіб ходьби, рух миші або натискання клавіш, також можуть використовуватися для автентифікації. Цей метод базується на аналізі поведінкових моделей за допомогою датчиків руху та програмного забезпечення. Він є зручним для користувачів і може бути інтегрований у різні системи та пристрої.

Методика 7:

- аналіз поведінкових моделей, таких як спосіб ходьби, рух миші, натискання клавіш;
- використання датчиків руху та програмного забезпечення для збору та аналізу даних.

Переваги методики:

- непомітність і зручність для користувача;
- можливість інтеграції в різні системи і пристрої [31].

Порівняння різних методів біометричної автентифікації наведені в Таблиці 1 [32].

Таблиця 1

Порівняння різних методів біометричної автентифікації за різними характеристиками.

Методи отримання біометричних параметрів	Ймовірність відмови у доступі, %	Ймовірність помилкової ідентифікації(без використання муляжу), %	Ймовірність помилкової ідентифікації (з використання муляжу), %	Вартість технічної реалізації, у.о.
Відбитки пальців	1 - 4	0,0001	0,5 - 2	50 - 500
Геометрія долоні	0,2 - 4	0,2 - 1	1 - 10	600 - 2000
Обличчя людини	1 - 5	-	10 - 40	1000
Райдужна оболонка ока	0,2 - 2	0,0001	-	10000
Голос людини	2 - 10	0,5 - 5	25 - 90	50 - 200
Рукописний почерк	0,5 - 5	0,5 - 5	0,5 - 5	~ 200
Клавіатурний почерк	3 - 9	3 - 9	-	~ 200

Загалом, сучасні методи біометричної автентифікації забезпечують високу точність, надійність і зручність для користувачів. Вибір конкретного методу залежить від вимог до безпеки, зручності та специфіки застосування. Комбінування різних біометричних методів (багатофакторна автентифікація) дозволяє підвищити рівень захисту і знизити ймовірність несанкціонованого доступу.

На основі таблиці порівняння різних методів біометричної автентифікації, можна зробити такі рекомендації щодо їх застосування на практиці:

Для систем з високими вимогами до безпеки:

- відбитки пальців: цей метод є одним з найнадійніших та доступних. Його можна використовувати для автентифікації користувачів комп'ютерів, смартфонів, банкоматів та інших пристроїв;
- райдужна оболонка ока: цей метод ще більш надійний, ніж відбитки пальців, але він також дорожчий і складніший у впровадженні. Його можна використовувати для автентифікації користувачів високочутливих систем, таких як системи контролю доступу до державних установ або банківських сховищ.

Для систем з середніми вимогами до безпеки:

- геометрична будова руки: цей метод є досить надійним і доступним, але він не такий надійний, як відбитки пальців або райдужна оболонка ока. Його можна використовувати для автентифікації користувачів банкоматів, платіжних терміналів та інших пристроїв, де не потрібна найвища ступінь безпеки;
- геометрія обличчя: цей метод стає все більш популярним завдяки розвитку технологій розпізнавання обличь. Він є досить зручним для користувачів, але не такий надійний, як інші методи. Його можна використовувати для автентифікації користувачів смартфонів, комп'ютерів та інших пристроїв, де важлива зручність використання.

Для систем з низькими вимогами до безпеки:

- рукописний почерк: цей метод є досить простим і доступним, але він не дуже надійний. Його можна використовувати для автентифікації користувачів систем, де не потрібна висока ступінь безпеки;
- клавіатурний почерк: цей метод також є досить простими і доступним, але він не дуже надійний. Його можна використовувати для автентифікації користувачів комп'ютерів, де не потрібна висока ступінь безпеки;
- розпізнавання голосу: цей метод є найменш надійним з усіх перерахованих, але він може бути корисним для додаткової автентифікації користувачів. Його можна використовувати для автентифікації користувачів систем, де важлива зручність використання [33].

Також, важливо відмітити рекомендації для використання цих методів в складі цілої системи автентифікації і контролю доступу:

1) використання багатофакторної автентифікації (MFA). Поєднання біометричної автентифікації з іншими методами, такими як паролі, токени або SMS-коди, може значно підвищити рівень безпеки. Це забезпечує додатковий захист у разі компрометації біометричних даних;

2) шифрування біометричних даних. Біометричні дані повинні бути шифровані як при зберіганні, так і при передачі. Це допоможе захистити їх від несанкціонованого доступу та зловживання;

3) використання локального зберігання. Зберігання біометричних даних на локальному пристрої користувача (наприклад, у захищеній області смартфона) замість централізованих серверів може знизити ризик масової компрометації даних;

4) регулярне оновлення алгоритмів розпізнавання. Алгоритми розпізнавання біометричних даних повинні регулярно оновлюватися та вдосконалюватися для забезпечення високої точності та зменшення ймовірності помилкових спрацьовувань;

5) оцінка та управління ризиками. Проведення регулярних аудитів безпеки та оцінки ризиків для виявлення потенційних вразливостей та розробки відповідних заходів для їх усунення;

6) конфіденційність та прозорість. Організації повинні інформувати користувачів про те, як їхні біометричні дані збираються, зберігаються та використовуються. Необхідно забезпечити прозорість у відношенні політики конфіденційності та збору даних;

7) дотримання правових норм та стандартів. Використання біометричних даних повинно відповідати вимогам законодавства та міжнародним стандартам захисту даних, таким як GDPR (General Data Protection Regulation) або ISO/IEC 27001;

8) навчання та обізнаність користувачів. Користувачів слід навчати безпечному використанню біометричної автентифікації та інформувати про потенційні ризики та заходи безпеки;

9) використання передових методів біометричної автентифікації. Впровадження новітніх технологій, таких як розпізнавання обличчя з використанням 3D-камер або аналізу вен, може забезпечити вищий рівень безпеки порівняно з традиційними методами, такими як сканування відбитків пальців;

10) моніторинг та реагування на інциденти [34]. Встановлення систем моніторингу для виявлення підозрілої активності та негайне реагування на інциденти безпеки допоможе мінімізувати наслідки компрометації біометричних даних.

Виконання цих рекомендацій сприятиме створенню більш безпечної та надійної системи біометричної автентифікації, яка відповідатиме вимогам сучасних загроз та забезпечить захист конфіденційності користувачів.

Висновки до розділу 2

Під час аналізу варіантів забезпечення автентифікації на основі біометричної інформації було розглянуто різноманітні підходи та методи, що включають в себе використання різних типів біометричних даних (таких як відбитки пальців, розпізнавання обличчя, голосу тощо), комбінацію різних методів автентифікації (наприклад, багатофакторна аутентифікація), а також вдосконалення технологій біометричної ідентифікації.

На основі аналізу були запропоновані різні стратегії та підходи для вирішення виявлених проблем, такі як вдосконалення алгоритмів обробки даних, розвиток нових технологій біометричної ідентифікації, а також посилення заходів захисту приватності користувачів, таких як шифрування та анонімізація біометричних даних.

Ретельно розглянуто проблеми, можливості та перспективи використання біометричних даних для автентифікації суб’єктів, та запропоновано шляхи

подальшого розвитку та вдосконалення цих технологій з метою забезпечення більшої ефективності, надійності та безпеки.

Розділ 3 РОЗРОБКА ТА ВТІЛЕННЯ ВАРІАНТУ СИСТЕМИ АВТЕНТИФІКАЦІЇ ОСІБ З ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ ДАНИХ

3.1 Установлення ключових вимог до системи автентифікації біометричними даними

Біометричні системи відрізняються за декількома основними характеристиками [35]:

1) пропускна спроможність - ця характеристика визначає час, необхідний для обробки даних одного користувача. Вона може варіюватися залежно від завдань системи, таких як аутентифікація чи ідентифікація. Наприклад, процес ідентифікації може займати більше часу, оскільки потребує порівняння даних з цілою базою;

2) ціна - ця характеристика включає вартість обладнання, розробки та підтримки програмного забезпечення, і може значно впливати на загальні витрати на впровадження біометричної системи;

3) надійність ідентифікації - цей аспект визначається співвідношенням між хибнопозитивними та хибнонегативними результатами. Для ефективної роботи системи важливо досягти балансу між цими двома типами помилок;

4) простота та зручність використання - ця характеристика відображає, наскільки легко користувач може встановити та використовувати систему. Це може включати такі аспекти, як інтуїтивність інтерфейсу та потребу в мінімальному навчанні;

5) ступінь психологічного комфорту - показує, наскільки користувачі сприймають систему. Важливо, щоб система не викликала негативних емоцій або сумнівів серед користувачів;

6) вразливість системи - ця характеристика визначає, наскільки легко можна обійти систему або підробити біометричні дані. Вона може бути особливо

важливою для систем, які використовуються для важливих цілей, таких як фінансові транзакції або в'їзд на об'єкти з підвищеною безпекою;

7) продуктивність - цей аспект залежить від кількох факторів, включаючи точність, вартість та зручність використання системи. Він важливий для забезпечення ефективності та ефективної роботи системи;

8) інтеграція - можливість інтеграції декількох біометричних систем може поліпшити їхні характеристики та функціональність;

9) конфіденційність - ця характеристика важлива для забезпечення захисту приватності користувачів та уникнення можливості використання їхніх біометричних даних для неправомірних цілей [36].

Характеристики ефективності біометричної системи включають наступні ключові показники:

1) коефіцієнт хибного доступу (FAR - False Acceptance Rate). Цей показник визначає ймовірність того, що система прийме особу за іншу, виражену у відсотках. Його також називають "помилка 2-го роду";

2) коефіцієнт хибної відмови в доступі (FRR - False Rejection Rate). Цей показник вказує на ймовірність того, що система не розпізнає особу, виражену у відсотках. Його також називають "помилка 1-го роду";

3) коефіцієнт рівної вірогідності помилок (ERR - Equal Error Rate). Цей показник відображається, коли обидва коефіцієнти хибного доступу і хибної відмови в доступі є однаковими;

4) коефіцієнт спроможності до верифікації (AVR - Ability to Verify Rate). Цей показник визначає ефективність системи у верифікації ідентичності;

5) коефіцієнт невдалої реєстрації (FER - Failure to Enroll Rate). Цей показник показує частоту невдалих спроб реєстрації в системі [37].

Індикатор FAR вказує на ймовірність того, що біометрична система прийме іншого користувача або шахрая. Індикатор FRR відображає ймовірність збою біометричної системи для тих, хто зареєстрований в системі на законних підставах і має доступ до системи. Індикатор несправності (ERR) показує стан

системи, при якому FAR і FRR однакові, що робить його ідеальним або оптимальним налаштуванням для будь-якого типу біометричної системи.

Чорна крива відображає FRR, а сіра лінія відображає FAR. У центрі знаходиться пунктирна лінія, яка відображає результат перевірки. Цей результат теоретично є оптимальним налаштуванням для біометричної системи. Область зліва від помилки вказує, що FRR більше, тобто вірогідність хибної відмови більша. Тому що, за менш короткий проміжок часу сканер може не встигнути захопити потрібні для аналізу біометричні дані. Область праворуч від помилки вказує, що FAR більше, ніж FRR, це означає що при збільшенні проміжку часу сканер може захопити більше точок і теоретично деякі комбінації цих точок можуть співпасти з уже існуючим шаблоном. Середня лінія з перетин двох кривих FAR і FRR, тобто в цій точці результат обробки біометричних даних буде найбільш правильним (рис. 3.1).

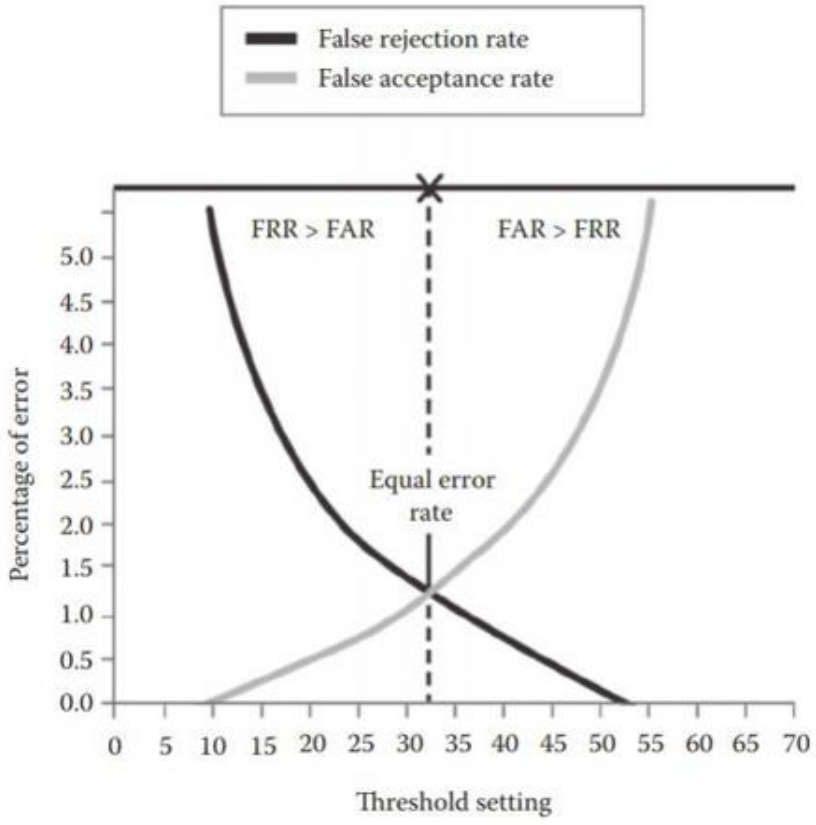

Рис. 3.1. Зона з найбільш позитивним результатом автентифікації

Очевидно, що ідеальна ситуація для біометричної системи - це знаходження в самому центрі, коли коефіцієнт хибного доступу (FAR) дорівнює коефіцієнту хибної відмови в доступі (FRR). Проте на практиці досягнення цього ідеалу майже неможливе. Навіть у випадку, коли біометрична система має просту структуру (наприклад, єдиний автономний біометричний пристрій), наближення до рівня помилок ERR є вельми складним завданням.

У більшості випадків оптимальним є стан, де FRR перевищує FAR. Це означає, що кількість законних користувачів, яким система відмовляє у доступі, перевищує кількість незаконних користувачів, яким надається доступ. Це практично означає, що в системі може бути більше помилок перевірки, ніж дозволених випадків несправедливого відмовлення у доступі.

Коефіцієнт спроможності до верифікації (AVR) визначає загальний відсоток осіб у конкретній популяції, які можуть бути коректно зареєстровані у біометричній системі. Цей показник не залежить від типу популяції - це може бути загальна кількість працівників певного бізнесу або громадян конкретної країни. Головне - це загальна кількість людей, які можуть бути правильно включені до біометричної системи.

Математично, AVR можна розглядати як комбінацію FER та FRR, виражену формулою:

$$AVR = (1 - FER) * (1 - FRR) \quad (1)$$

де AVR - коефіцієнт спроможності до верифікації, %;

FER - коефіцієнт невдалої реєстрації, %;

FRR - коефіцієнт хибної відмови в доступі, %.

Показник FER статистично описує відсоток популяції, який не може бути правильно зареєстрований у біометричній системі. Ця метрика є оберненою до AVR. Існує кілька причин, чому деякі особи не можуть бути включені до

біометричної системи, такі як фізичні захворювання (наприклад, артрит), зміни в кольорі шкіри, сліпота, а також відсутність певних фізичних та біологічних особливостей [38].

3.2 Впровадження системи біометричної автентифікації за допомогою відбитків пальців

Програмне забезпечення призначене для організації та управління процесом збору біометричних даних, зокрема відбитків пальців людини. Основні функції цього програмного продукту включають [39]:

1) контроль за правильністю введення зразків. Програмне забезпечення забезпечує можливість контролювати правильність збору та введення біометричних даних, зокрема відбитків пальців. Це включає перевірку на наявність артефактів або неправильних даних, а також дотримання необхідних стандартів та протоколів;

2) завантаження раніше створеної бази даних. Програмне забезпечення дозволяє завантажувати раніше створені бази даних збережених біометричних даних. Це дозволяє використовувати вже існуючі дані для подальшого аналізу, порівняння або оновлення [40].

Система автентифікації осіб з використанням біометричних даних може включати кілька компонентів і етапів для забезпечення безпеки та зручності користувачів. Для повноцінного функціонування системи автентифікації до комп'ютера був підключений сканер відбитків пальців “Futronic FS80” та встановлено програмне забезпечення “Futronik Logon Finger Manager” (рис. 3.2).

Нижче наведена схема системи автентифікації за допомогою сканера відбитків пальців та відповідного програмного забезпечення:

Схема 3.1 Система автентифікації користувача

Система автентифікації з використанням біометричних даних складається з наступних компонентів:

1) біометричний датчик:
   - сканер відбитків пальців.
2) програмне забезпечення:
   - біометричний модуль обробки даних - програмне забезпечення для обробки і порівняння біометричних даних з збереженими зразками.
   - система управління доступом - програмне забезпечення для контролю доступу на основі результатів біометричної автентифікації.
   - база даних біометричних даних - захищена база даних, де зберігаються біометричні зразки користувачів.
3) Графічні інтерфейси:
   - панель керування системою і управління доступом користувачів.
   - додаток, який дозволяє користувачам зручно проходити автентифікацію.
4) Засоби захисту:
   - шифрування - захист переданих та збережених біометричних даних за допомогою криптографічних методів.
   - системи виявлення зловживань - інструмент для виявлення підозрілих спроб доступу.

Процес роботи системи автентифікації користувача складається з наступних кроків:

1) реєстрація користувачів. При першій реєстрації користувачі надають свої біометричні дані (відбиток пальців). Зібрані біометричні зразки шифруються і зберігаються в захищеній базі даних;
2) сканування відбитка пальця. Користувач пред'являє свій біометричний зразок (сканує відбиток пальця) для доступу до системи. Сканер Futronis FS80 використовує оптичну технологію для зняття зображення відбитка пальця. Зображення складається з тисяч точок, кожна з яких відповідає гребню або долині на відбитку пальця;
3) перетворення зображення на код. Програмне забезпечення Futronik Logon Finger Manager перетворює зображення відбитка пальця на цифровий код. Цей код є математичним представленням унікальних характеристик відбитка пальця;
4) порівняння коду з базою даних. Код відбитка пальця порівнюється з кодами, що зберігаються в базі даних. База даних містить коди відбитків пальців усіх користувачів, які мають доступ до системи;
5) аутентифікація. Якщо код відбитка пальця збігається з кодом, що зберігається в базі даних, користувач вважається аутентифікованим. Це означає, що користувач підтвердив свою особу і йому буде надано доступ до системи.
6) відмова в доступі. Якщо код відбитка пальця не збігається з кодом, що зберігається в базі даних, користувачеві відмовляється в доступі. Це може бути пов'язано з тим, що користувач не зареєстрований в системі або що він ввів неправильний відбиток пальця;
7) моніторинг і аудит. Всі спроби автентифікації (успішні та невдалі) записуються в журнали для подальшого аналізу. В подальшому можна переглядати ці журнали автентифікації для виявлення можливих порушень або загроз.

Також, можуть бути використані додаткові можливості цієї системи:

1) Мультифакторна автентифікація (MFA). Крім біометричних даних, система може використовувати додаткові фактори, такі як одноразові паролі (OTP), апаратні токени або смарт-карти для підвищення рівня безпеки.
2) Інтеграція з іншими система. Система автентифікації може бути інтегрована з іншими корпоративними системами, такими як системи управління ідентичностями (IAM), для централізованого управління доступом.
3) Мобільний доступ. Використання мобільних пристроїв як додаткових або основних засобів автентифікації, що дозволяє здійснювати автентифікацію за допомогою відбитків пальців безпосередньо з мобільного телефону.

Нижче детально описано процес роботи програмного забезпечення. На рисунку 3.2 зображено процес інсталювання програми.

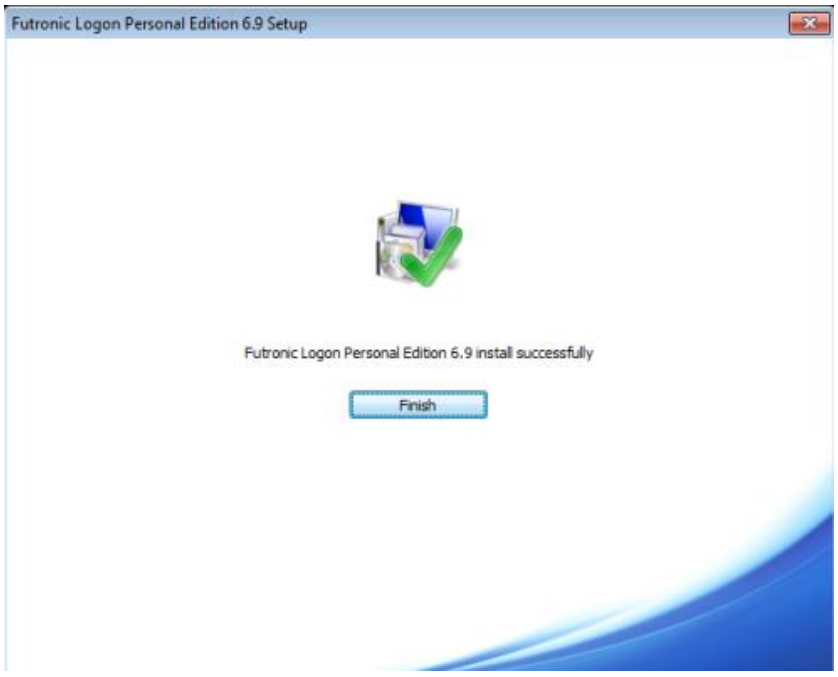

Рис. 3.2. Завершення інсталювання програми Futronik Logon

Також були встановлені відповідні драйвери, які забезпечують сумісність між сканером та комп'ютером, щоб забезпечити правильну роботу програми зі збору біометричних даних (рис. 3.3).

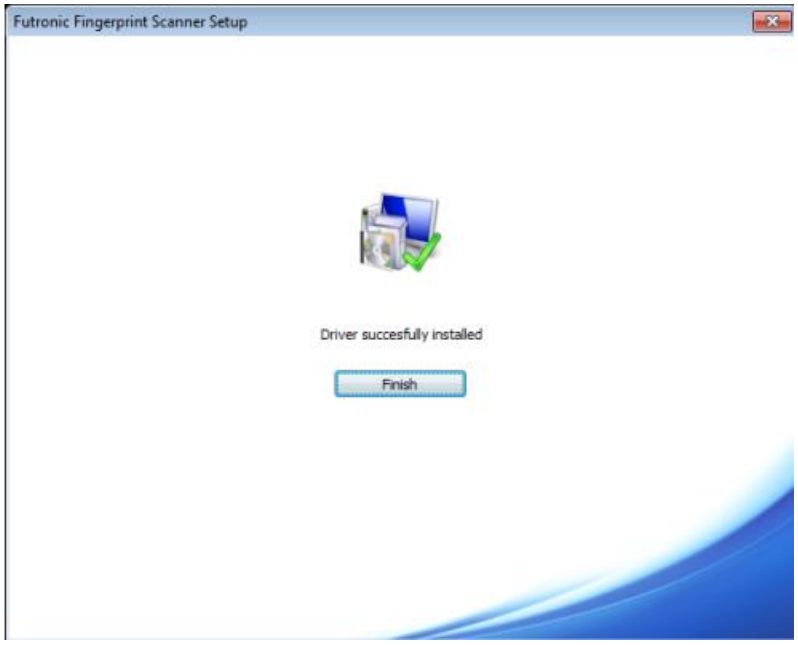

Рис. 3.3. Завершення інсталювання драйверів для сумісності зі сканером

У представленому рисунку 3.4 головному вікні програмного забезпечення для створення баз відбитків можна виділити дві основні частини.

Верхня частина вікна виділена під інструменти і призначена для керування програмою. Тут можна створити нового користувача, відредагувати уже існуючого, змінити вигляд програми та змінити налаштування самої програми.

Нижня частина вікна слугує вікном для перегляду всієї основної інформації. Тут відбувається основна робота зі сканером і користувачами: безпосереднє створення, редагування користувачів, процес сканування відбитків пальців і перевірка збережених образів відбитків в базі. Тут можна переглядати, вибирати та керувати збереженими відбитками пальців.

Це головне вікно дозволяє ефективно управляти процесом створення та управління базами даних відбитків пальців, надаючи зручний інтерфейс для користувача (рис. 3.4).

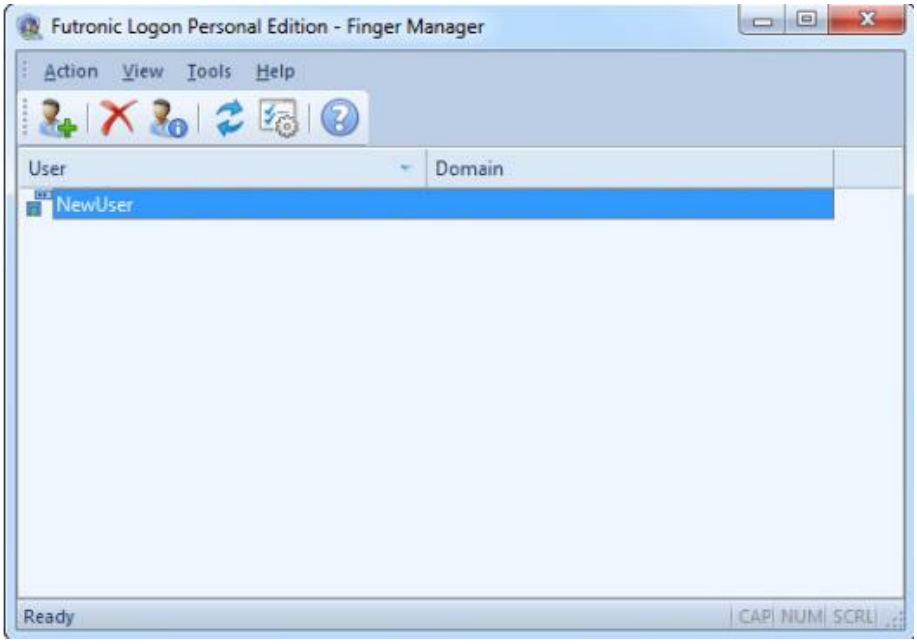

Рис. 3.4. Головне вікно програмного забезпечення для створення баз відбитків

Це програмне забезпечення надає користувачеві можливість створення нової бази біометричних даних або внесення змін в існуючу базу. Процес формування бази включає кілька етапів.

Спочатку користувач додає обліковий запис нового користувача до системи. Це може включати введення особистих даних таких як ім'я користувача та пароль. Далі користувач може захопити зображення відбитка пальця за допомогою підключеного сканера. Цей процес може вимагати декількох спроб для отримання якісного зображення.

Отримані дані зберігаються у вигляді файлів бази даних. Ці файли зазвичай зберігаються в робочій папці програми, що забезпечує зручний доступ до них для майбутнього використання.

Для того щоб створити нового користувача потрібно натиснути кнопку “Action”, а потім “Add User” (рис. 3.5). Після цього відкриється вікно, в якому потрібно дотримуватись запропонованих кроків та інструкцій.

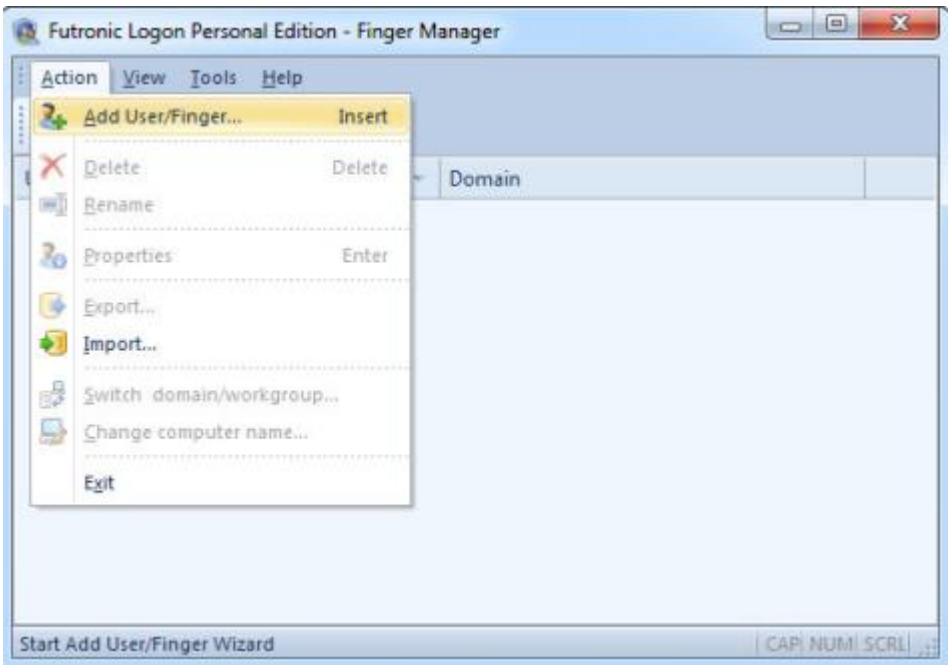

Рис. 3.5. Вікно створення нового користувача

Для ідентифікації і безпечного збереження даних потрібно ввести ім'я користувача (User name) та пароль (Password) (рис. 3.6).

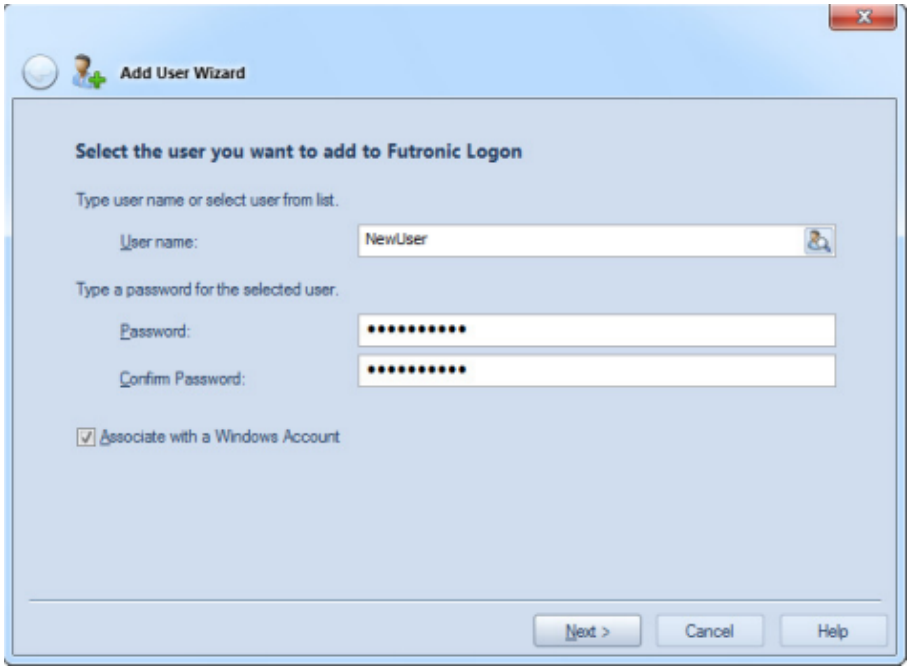

Рис. 3.6. Ввід облікових даних користувача

Після цього відкривається вікно вибору методів автентифікації (рис. 3.7).

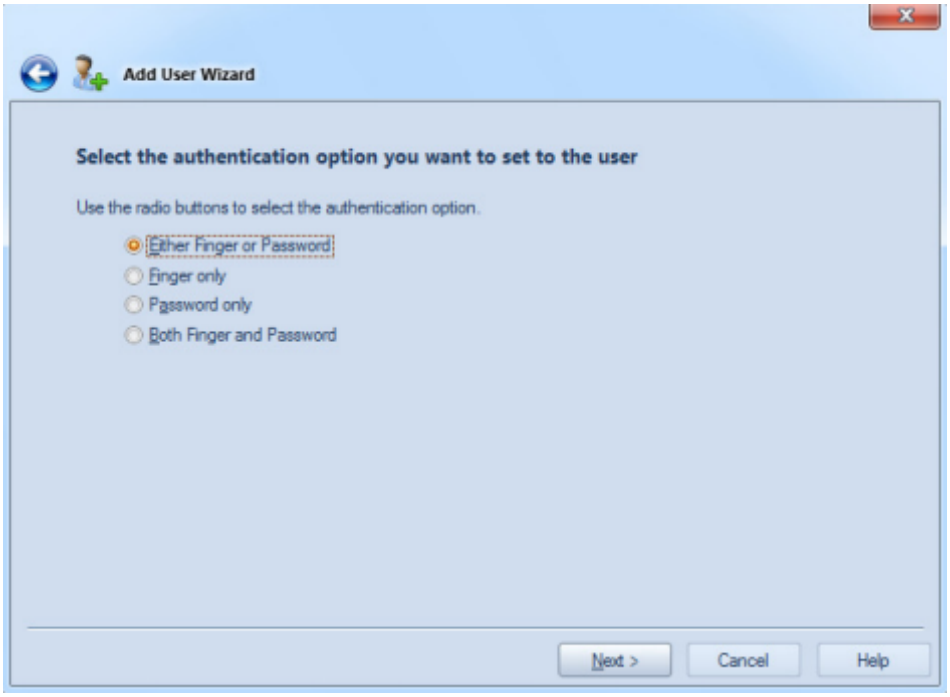

Рис. 3.7. Вибір методу автентифікації

У цьому вікні є кілька варіантів вибору:

- або відбиток пальця або пароль;
- тільки відбиток пальця;
- тільки пароль;
- разом і відбиток пальця і пароль.

На наступному етапі потрібно вибрати який палець використовувати для автентифікації (рис. 3.8).

Рис. 3.8. Вибір пальця для зняття відбитка

Пальці будуть ідентифіковані як RF1..RF5 і LF1..LF5, де RF або LF означає палець правої або лівої руки. 1,2,3,4 і 5 позначають номер пальця, починаючи з великого.

На наступному етапі можна побачити повідомлення "Place your finger on the scanner", користувач повинен розмістити палець на сканері та натиснути його з невеликим зусиллям. Тепер сканер починає робити зразки вашого пальця для отримання цифрового шаблону. Важливо дотримуватися вказівок на екрані. Для уникнення значної деформації відбитку пальця під час переміщення рекомендується відривати його від сканера та знову притискати послідовно.

Зроблені зображення відбитку повинні знаходитися всередині рамки, переважно по центру. Зсування або перекочування може суттєво спричинити деформацію рисунку папілярних ліній і вплинути на якість формування бази (рис. 3.9).

У випадку, якщо знімок відбитку не відбувається належним чином, користувач може:

- натискати палець сильніше за вказівкою;
- переміщати палець вправо або вліво;
- повертати палець вертикально.

Рис. 3.9. Процес сканування відбитка пальця

Після того як сканування пальця завершиться потрібно натиснути кнопку “Finish”, для збереження всієї інформації.

Для одного користувача можна додати до 10 відбитків (всіх) пальців, які потім можна використовувати для автентифікації. Щоб додати більше відбитків пальців для того самого користувача, потрібно повторити процедуру “Add User/Finger”, але вибрати інший палець у діалоговому вікні вибору пальця.

Натиснувши на ім'я користувача на головному екрані, можна перейти до редагування цього користувача (рис. 3.10).

На вкладці “User Properties” можна змінити пароль, а також змінити способи автентифікації.

Рис. 3.10. Вкладка “User Properties”

Перейшовши на вкладку “”Fingers”, можна побачити всі збережені відбитки для цього користувача. Також, за потреби можна перевірити або видалити конкретний відбиток та одразу замінити його на новий.

Для того щоб зробити глобальні налаштування системи потрібно на головному екрані натиснути спочатку “Tools”, а потім “Settings”. У відкритому вікні основними налаштуваннями є глобальні якісні показники знімків відбитків пальців (рис. 3.11).

Нижче наведений основний список наявних налаштувань:

- якість розпізнавання (Recognition Quality) - всього є 5 рівнів. “Високий” є найбезпечнішим (низький FAR і високий FRR), а “Низький” є найменш безпечним(високий FAR і низький FRR).
- мінімальна кількість деталей (Minimum number of minutiae) - рівень мінімальної кількості деталей для зареєстрованого шаблону.
- увімкнути візуалізацію для захоплення зображення (Enable Visualization for image capture) - потрібно увімкнути цей параметр, якщо потрібно переглядати відбиток пальця користувача додаючи або перевіряючи його.
- визначення підробки відбитка - сканер визначає чи палець дійсно справжній.
- опція MIOT (Multi-fingers In One Template) - потрібно увімкнути цю опцію, для того, щоб програма перевіряла, чи притиснув користувач той самий палець до сканера під час реєстрації.

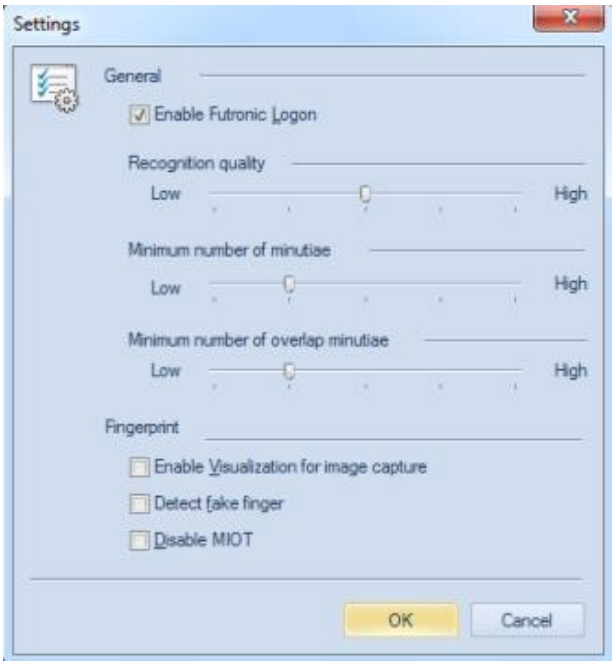

Рис. 3.11. Вкладка “Settings”

Також, в системі присутній функціонал завантаження та вивантаження бази відбитків пальців. Імпорт та експорт бази даних користувачів/відбитків пальців дозволяє швидко відновити, перевстановити або перенести на іншу систему без повторної реєстрації користувача/відбитку пальця. Також рекомендується адміністратору системи використовувати функцію експорту для регулярного резервного копіювання бази даних. Для запуску процедури "Import" або "Export" потрібно вибрати відповідну опцію в меню "Action" (рис. 3.12).

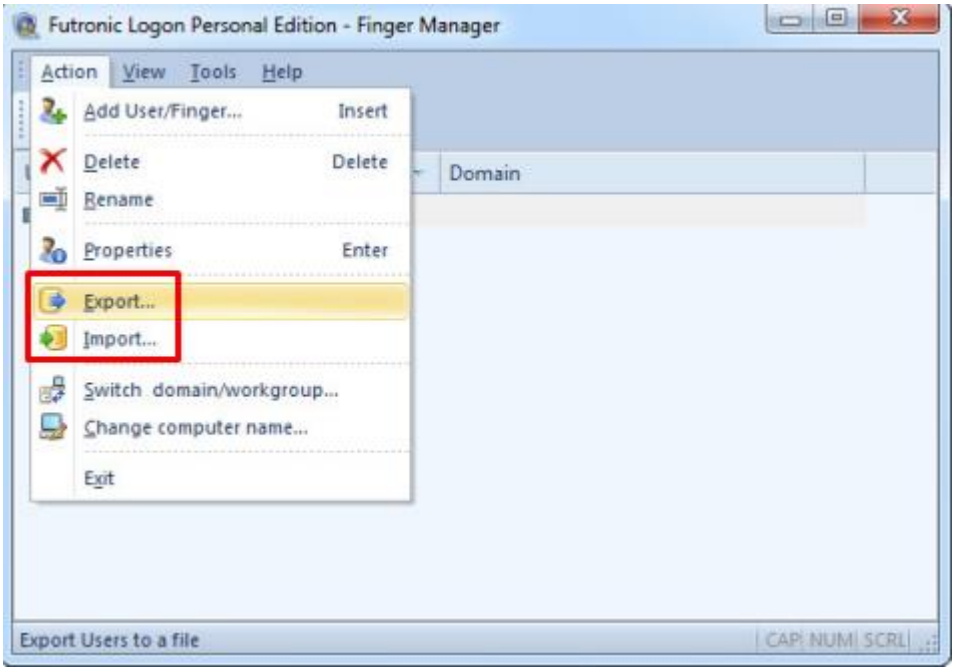

Рис. 3.12. Вкладки "Import" та"Export"

Для того, щоб вивантажити базу даних користувачів спочатку потрібно вибрати файл для зберігання. Далі потрібно вибрати користувачів, яких треба експортувати (за замовчення всі). Після цього натиснути кнопку “Next” і база збережеться у вибраний файл (рис. 3.13).

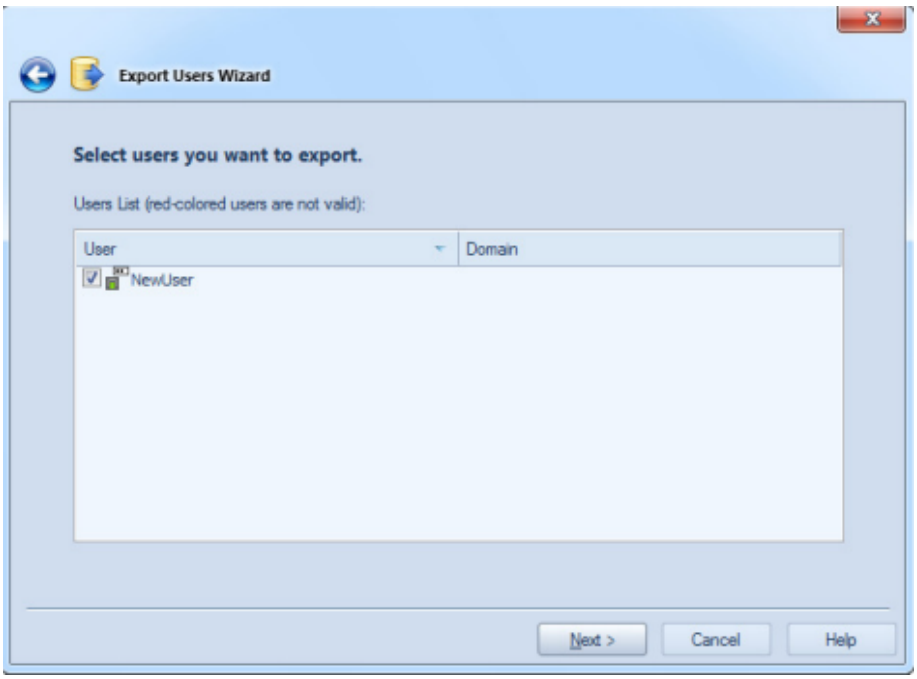

Рис. 3.13. Процес вивантаження бази даних користувачів

Імпорт бази даних дуже схожий, але обернений процес на експорт. По-перше потрібно вибрати файл де зберігається база. По-друге, потрібно вибрати список тих користувачів, які мають бути імпортовані в систему. Всі користувачі/відбитки пальців будуть імпортовані за замовчуванням (рис. 3.14). Користувачі, позначені червоним кольором, не є дійсними для системи і не можуть бути імпортовані [41] .

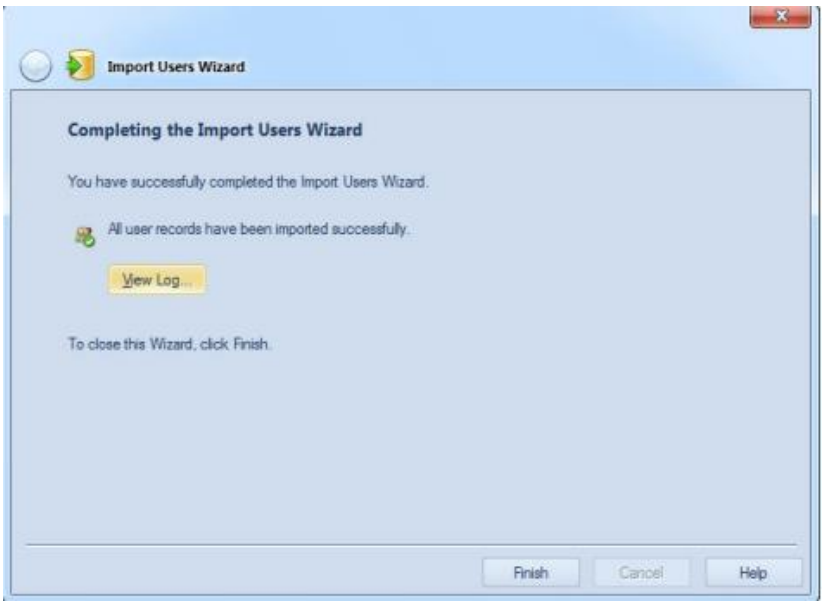

Рис. 3.14. Успішний результат імпорту бази користувачів

Описана система ідеально підходить для реалізації автентифікації для перевірки особистості та доступу до ресурсів або приміщень у невеликих організаціях, де важливо мати достатньо гарний рівень безпеки і контролю доступу. Тому що, система проста у використанні і для її адміністрування не потрібно великих вмінь, також вартість впровадження такої система невелика, основні витрати складають придбання сканера відбитків пальців, а офіційне програмне забезпечення можна завантажити на сайті виробника сканера. В той же час, система не є достатньо автоматизованою і велика кількість користувачів може вплинути на швидкодію програми. Впровадження такої системи автентифікації допоможе значно підвищити рівень безпеки в організації, забезпечивши надійний контроль доступу до важливих ресурсів і зменшивши ризик несанкціонованого доступу.

Висновки до розділу 3

Розглянуто різноманітні аспекти, пов'язані з вимогами до системи автентифікації, включаючи безпеку, надійність, ефективність та зручність використання. Були вивчені потреби користувачів та вимоги до системи з метою забезпечення оптимальної функціональності.

Під час визначення основних принципів функціонування системи було встановлено, що вона повинна ефективно впроваджувати процес автентифікації на основі унікальних характеристик користувачів, забезпечуючи високий рівень безпеки та зручності використання.

У результаті розроблено комплексну систему автентифікації на основі біометричних даних, яка враховує високу точність і швидкість в роботі, а також забезпечує захист приватності користувачів. Були створені програмні модулі та інструменти для збору, обробки та аналізу біометричних даних.

ВИСНОВКИ

Дослідження зосереджено на теоретичних аспектах та методах автентифікації суб’єктів на основі біометричної інформації. Оглянуто сучасні методики біометричної автентифікації користувачів, включаючи методи порівняння ДНК, папілярних ліній, методи голосової автентифікації та інші. Вивчені методи збору, обробки та зберігання біометричних даних.

Проаналізовано сучасні методи автентифікації користувачів на основі біометричних даних. Встановлено, що кожен метод має свої переваги та обмеження, і вибір методу залежить від конкретних вимог до безпеки та точності.

Виявлено, що біометрична аутентифікація ґрунтується на унікальних фізіологічних або поведінкових характеристиках особи, таких як відбитки пальців, обличчя, голос та інші, що можна використовувати для ідентифікації.

Під час аналізу варіантів забезпечення автентифікації на основі біометричної інформації розглянуто різноманітні підходи та методи, що включають в себе використання різних типів біометричних даних (таких як відбитки пальців, розпізнавання обличчя, голосу тощо), комбінацію різних методів автентифікації (наприклад, багатофакторна аутентифікація), а також вдосконалення технологій біометричної ідентифікації.

На основі аналізу були запропоновані різні рекомендації по вибору методу біометричної автентфікації та підходи для вирішення виявлених проблем, такі як вдосконалення алгоритмів обробки даних, розвиток нових технологій біометричної ідентифікації, а також посилення заходів захисту приватності користувачів, таких як шифрування та анонімізація біометричних даних.

Ретельно розглянуто проблеми, можливості та перспективи використання біометричних даних для автентифікації суб’єктів, та запропонував шляхи подальшого розвитку та вдосконалення цих технологій з метою забезпечення більшої ефективності, надійності та безпеки.

Розглянуто різноманітні аспекти, пов'язані з вимогами до системи біометричної автентифікації, включаючи безпеку, надійність, ефективність та зручність використання. Були вивчені потреби користувачів та вимоги до системи з метою забезпечення оптимальної функціональності.

У результаті розроблено комплексну систему автентифікації на основі біометричних даних, яка враховує високу точність і швидкість в роботі, а також забезпечує захист приватності користувачів. Був описаний програмний модуль та інструменти для збору, обробки та аналізу біометричних даних.

Під час визначення основних принципів функціонування системи було встановлено, що вона повинна ефективно впроваджувати процес автентифікації на основі унікальних характеристик користувачів, забезпечуючи високий рівень безпеки та зручності використання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Anil J., J. Anil, B. Ruud, P. Sharath Biometrics - Personal Identification in Networked Society. New-York: Springer, 2006. P. 410.

2. N. Boulgouris, Konstantinos N., E. Micheli-Tzanakou. Biometrics: Theory, Methods, and Applications, Canada, 2009. 719 p. URL: https://books.google.com/books?id=fefutm-Dhy0C&printsec=frontcover&dq=BIOMETRIC+SYSTEMS&hl=ru&newbks=1&newbks_redir=1&sa=X&ved=2ahUKEwixy8Kzq5H_AhX8hP0HHcKeAIUQ6AF6BAgIEAI (дата звернення 05.04.2024).

3. Polunina D., Zolotukhina O., Nehodenko O., Yarosh I. Methods of Biometric Authentication for Personal Identification. 2nd International Congress of Electrical and Computer Engineering. March 2024. P. 327-339

4. М.В. Короленко, Н. А. Потапова Ідентифікація та автентифікація користувачів на основі біометричних даних, Донецький національний університет імені Василя Стуса, 2023. URL: https://jait.donnu.edu.ua/article/view/14074 (дата звернення 07.04.2024).

5. Definition of 'Authentication' URL: https://economictimes.indiatimes.com/definition/authentication (дата звернення 07.04.2024).

6. Gudkov, V. Mathematical Models of Fingerprint Image On the Basis of Lines Description, Proc. of The 19th International Conference on Computer, 2010. URL: https://www.researchgate.net/publication/228497858_Mathematical_Models_of_Fingerprint_Image_On_the_Basis_of_Lines_Description (дата звернення 10.04.2024).

7. Electronic Authentication Guideline // NIST Special Publication 800 - 63 April 2006 URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf (дата звернення 11.04.2024).

8. K, Krishna Prasad and Aithal, P. S. A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP. International Journal of

Advanced Trends in Engineering and Technology, 2018, p. 1-11. URL: https://ssrn.com/abstract=3097480 (дата звернення 13.04.2024).

9. A. Tiwari, R. Agarwal, S. Goyal Biometric Authentication for Mobile Banking Security, May 17, 2014. URL: http://dx.doi.org/10.2139/ssrn.2438213 (дата звернення 16.04.2024).

10. K, Krishna Prasad ABCD Analysis of Fingerprint Biometric Attendance Maintenance System, International Journal of Applied Engineering and Management Letters, 2018, p. 53-70, URL: https://ssrn.com/abstract=3279373 (дата звернення 17.04.2024).

11. Farik M., Nilesh L., Prasad S. A Review of Authentication Methods, International Journal of Scientific & Technology Research, Nov 2016.

12. Aithal, P. S. Biometric Authenticated Security Solution to Online Financial Transactions, International Journal of Management, IT and Engineering, July 2015, p. 455-464, URL: https://ssrn.com/abstract=2779027 (дата звернення 18.04.2024).

13. Продан Т.І., Івасьєв С.В. Сучасні методи біометричної ідентифікації. Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп’ютерно – інтегровані технології» (АКІТ -2022), Тернопіль, 2022. 62-65 с.

14. Х. В. Луценко., К. В. Нікулін ГОЛОСОВА ІДЕНТИФІКАЦІЯ ДИКТОРА ЯК ОДИН ІЗ СУЧАСНИХ БІОМЕТРИЧНИХ МЕТОДІВ ІДЕНТИФІКАЦІЇ ОСОБИ, Харківського НДІСЕ, 2020, URL: https://doi.org/10.32353/ 1.2019.018 343.982 (дата звернення 19.04.2024).

15. Ometov A., Bezzateev S., Mäkitalo N., Mikkonen T. Multi-Factor Authentication: A Survey. Tampere University, Finland, Jan 2018. P. 12.

16. Joseph N. Pato, Lynette I. Millett Biometric Recognition: Challenges and Opportunities, National Research Council, 2010, URL: https://doi.org/10.17226/12720 (дата звернення 20.04.2024).

17. Кузик В.М., Продан Т.І., Івасьєв С.В., Слєпцова О.Я. Біометрична система автентифікації з використанням голосових даних. Збірник матеріалів

науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2020), Тернопіль, 2020. С.56-59.

18. An emerging biometric API industry standard. URL: https://doi.org/10.1109/2.820046 (дата звернення 20.04.2024).

19. Кауненко С.І., Колесніков К.В. Методи ідентифікації людини в інформаційних системах, Інтелектуальні системи прийняття рішень та проблем штучного інтелекту, Матеріали міжнародної наукової, Херсон-Євпаторія ХНТУ, 2012, С. 164-167.

20. Precise Biometrics. URL: https://precisebiometrics.com/ (дата звернення 21.04.2024).

21. Шкіра Ю.Р. , Гевко Н.І., Гавриків Н.Г., Осадчук О.Я. Алгоритми та засоби автоматичної детекції обличчя в відео потоці. Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2020), Тернопіль, 2020. С.19.

22. Олена Висоцька Методи біометричної автентифікації користувачів інформаційних систем за їх клавіатурним та рукописним почерком, Національний авіаційний університет, 2019, URL: http://er.nau.edu.ua/handle/NAU/40426 (дата звернення 25.04.2024).

23. Juul N. C. Recommendation on the Use of Biometric Technology, Book: Security and Privacy in Biometrics, Jan 2013, p.415-433.

24. Brunelli R., Poggio T. Face recognition through geometrical features Computer Vision. Springer Berlin/Heidelberg, 1992.

25. Salahaldeen D. Voice Biometric Identity Authentication Model for IoT Devices. International Journal of Security, Privacy and Trust Management, URL: https://ssrn.com/abstract=3667519 (дата звернення 28.04.2024).

26. Ahonen T., Hadid A., Pietikäinen M. Face recognition with local binary patterns. Computer vision-eccv, 2004.

27. Стасєв Ю. В., Гончаренко К. Г., Мороз В. І. Аналіз методу багатофакторної автентифікації користувачів інформаційних систем на основі

райдужної оболонки ока. Системи обробки інформації. 2023, С. 63-69. URL: https://doi.org/10.30748/soi.2023.174.09 (дата звернення 29.04.2024).

28. Amazon Launches New Payment System Using Palm Recognition, 2020. URL: https://www.aboutamazon.com/news/retail/amazon-one-app (дата звернення 01.05.2024).

29. Berezsky O. Biomedical image search and retrieval algorithms / O. Berezsky, G. Melnyk, Yu Batko, 2008. T. 7, Vol 1. P. 108–113.

30. FindFace URL: https://findface.pro/en/cases/fraud-prevention/ (дата звернення 03.05.2024).

31. Shynkarenko, I., Zakharov V., Zakharova O. CONCEPTUAL ASPECTS OF THE USE OF BIOMETRIC TECHNOLOGIES IN THE FIELD OF COUNTERACTION TO CRIMINAL OFFENSES IN THE AIRLINE INDUSTRY. Archives of Criminology and Forensic Sciences, 2020, p. 102-113. URL: https://doi.org/10.32353/acfs.3.2021.11 (дата звернення 05.05.2024).

32. Бідюк П. , Бондарчук В. Сучасні методи біометричної ідентифікації, 2009. URL: https://ela.kpi.ua/server/api/core/bitstreams/7f1251ba-7156-4730-8a08-3ae82ddbc1f3/content (дата звернення 07.05.2024).

33. Bezruk V., Skoryk V., Kobtseva V. Comparison of methods of biometric authentication on the total of quality indicators, International science conference High-Technologies in info communications, 2019. URL: https://visn-icct.uu.edu.ua/index.php/icct/article/download/25/6 (дата звернення 10.05.2024).

34. Мороз А. О. Біометричні технології ідентифікації людини. Огляд системи. Математичні машини і системи, 2011. URL: http://www.immsp.kiev.ua/publications/articles/2011/2011_1/01_2011_Moroz.pdf (дата звернення 11.05.2024).

35. Скорик Ю., Безрук В. Вибір переважного методу біометричної автентифікації. International Science Journal of Engineering & Agriculture, 2023, p. 28-34. URL: https://doi.org/10.46299/j.isjea.20230204.04 (дата звернення 13.05.2024).

36. Д. Драгоєв Методи автентифікації та керування доступом до веб-ресурсу згідно до GDPR, Scientific Practice: Modern and Classical Research Methods, 2022. URL: http://dx.doi.org/10.36074/logos-16.09.2022.22 (дата звернення 15.05.2024).

37. Cyber Security Survey: Major Australian Business // Australian Government, Australian Cyber Security Centre, 2015, p. 12-17.

38. Policy for a Common Identification Standard for Federal Employees and Contractors., Homeland Security Presidential Directive, August 27, 2004. URL: https://www.dhs.gov/homeland-security-presidential-directive-12 (дата звернення 17.05.2024).

39. ISO / IEC 2382-37, Information technology - Vocabulary - Part 37: Biometrics, 2017. URL: https://webstore.iec.ch/preview/info_isoiec2382-37%7Bed2.0%7Den.pdf (дата звернення 18.05.2024).

40. Остапець Д., Дзюба В., Коваль Т. Комплекс для вивчення принципів автентифікації за відбитками пальців в системах захисту інформації, System Technologies, March 2021. URL: https://www.researchgate.net/publication/350799376_KOMPLEKS_DLA_VIVCENNA_PRINCIPIV_AUTENTIFIKACII_ZA_VIDBITKAMI_PALCIV_V_SISTEMAH_ZAHISTU_INFORMACII (дата звернення 19.05.2024).

41. Futronic Logon Personal Edition, User’s Guide, 2020. URL: https://www.futronic-tech.com/futronic/attachment/upload/futronic/download/FinLogonPE_User_Guide_V7.4.pdf (дата звернення 20.05.2024).