МІНІСТЕРСТВО ОСВІТИ І НАУКИ

Західноукраїнський національний університет

Факультет комп'ютерно-інформаційних технологій

Кафедра комп'ютерної інженерії

ДАЛЕКИЙ Артем Русланович

Алгоритми генерації унікального персонального ключа на основі біометричних параметрів людини/ Algorithms for generating a unique personal key based on a person's biometric parameters

Спеціальність 123 – Комп'ютерна інженерія

Освітньо-професійна програма – Комп'ютерна інженерія

Кваліфікаційна робота

Виконав студент групи Кім-21

А.Р. Далекий

_____

Науковий керівник

к.т.н. Ю.М. Батько

_____

Кваліфікаційну роботу допущено

до захисту

"___" _____20___ р

Завідувач кафедри

_____Л.О.Дубчак

ТЕРНОПІЛЬ - 2023

РЕЗЮМЕ

Кваліфікаційна робота на тему «Алгоритми генерації унікального персонального ключа на основі біометричних параметрів людини » зі спеціальності 123 «Комп’ютерна інженерія» освітньої програми «Комп'ютерна інженерія» написана обсягом в 95 сторінок і містить 17 ілюстрацій, 17 таблиць, 10 додатків та 50 використаних джерел.

Метою даної кваліфікаційної роботи є розробка та вивчення ефективних алгоритмів генерації унікального персонального ключа на основі біометричних параметрів людини для підвищення рівня безпеки систем автентифікації.

Наукова новизна. Виявлення та аналіз ключових факторів, що впливають на ефективність та безпеку систем генерації біометричних ключів. Особливу увагу приділено новітнім розробкам у галузі машинного навчання та штучного інтелекту, які відкривають нові можливості для підвищення точності та надійності біометричних систем.

Результати дослідження: проведено дослідження та класифікацію персональних даних, досліджено біометричні персональні дані, проаналізовано програмно-апаратні системи генерації ключів, зроблено аналіз алгоритмів генерації персональних ключів, розроблено алгоритм генерації ключа на основі біометричних параметрах людини, проведено реалізацію та тестування програмно-апаратної системи генерації персоналізованих ключів.

Ключові слова: ПЕРСОНАЛЬНІ ДАНІ, ЗАХИСТ ДАНИХ, БІОМЕТРИЧНИЙ КЛЮЧ, ПРОГРАМНО-АПАРАТНІ СИСТЕМИ, АЛГОРИТМ ГЕНЕРАЦІЇ

RESUME

The qualification work on the topic "Algorithms for generating a unique personal key based on human biometric parameters" from specialty 123 "Computer Engineering" of the educational program "Computer Engineering" is written in the volume of 95 pages and contains 17 illustrations, 17 tables, 10 appendices and 50 used sources.

The purpose of this qualification work is to develop and study effective algorithms for generating a unique personal key based on a person's biometric parameters to increase the level of security of authentication systems.

Scientific novelty. Identification and analysis of key factors affecting the efficiency and security of biometric key generation systems. Particular attention is paid to the latest developments in the field of machine learning and artificial intelligence, which open up new opportunities for increasing the accuracy and reliability of biometric systems.

Research results: research and classification of personal data was carried out. biometric personal data was investigated, hardware and software systems for key generation were analyzed, algorithms for generating personal keys were analyzed, a kev generation algorithm based on human biometric parameters was developed, the software and hardware system for generating personalized keys was implemented and tested kevs

Keywords: PERSONAL DATA, DATA PROTECTION, BIOMETRIC KEY, SOFTWARE AND HARDWARE SYSTEMS, GENERATION ALGORITHM.

ЗМІСТ

ВСТУП

У сучасному світі, де технології швидко розвиваються і де цифрові дані стають невід'ємною частиною нашого життя, питання захисту персональних даних набуває особливої актуальності. Особисті дані стають цільовими для зловмисників, які використовують їх для фінансового шахрайства, крадіжки ідентичності, а також для розповсюдження шпигунських програм. В той же час, організації та установи використовують персональні дані для надання персоналізованих послуг, але також мають забезпечувати їхню конфіденційність та цілісність. Автентифікація є одним з основних методів захисту інформації, яка перевіряє особу користувача, перш ніж надавати доступ до цінної інформації або систем. Традиційні методи автентифікації, зокрема паролі, часто піддаються ризику через їхню вразливість до витоку, крадіжки та зламу. Біометрична автентифікація, яка використовує унікальні біологічні характеристики особи, такі як відбитки пальців, сітківка ока або голосові дані, пропонує високий рівень безпеки, враховуючи їхню унікальність і стійкість до підробки.

Але навіть біометричні дані можуть бути скомпрометовані. Якщо зловмисники отримають доступ до бази біометричних даних, вони можуть використовувати ці дані для несанкціонованого доступу до персональних та корпоративних систем. Саме тому важливо не просто збирати біометричні дані, але й забезпечувати їх надійне шифрування та захист. У цьому контексті актуальним є розробка систем, які можуть генерувати унікальні персональні ключі на основі біометричних параметрів людини, які будуть використовуватися для шифрування та захисту персональних даних. Цей підхід не тільки поліпшить безпеку біометричних систем автентифікації, але й забезпечить зручність для кінцевих користувачів, оскільки персональний ключ буде генеруватися автоматично без потреби пам'ятати складні паролі або використовувати фізичні ключові носії.

Актуальність теми. У сучасному світі, де цифровізація і автоматизація проникають в усі сфери життя людини, забезпечення безпеки персональної інформації стає ключовим питанням. Автентифікація та ідентифікація користувачів стали невід'ємними частинами багатьох систем, від банківських операцій до особистих гаджетів. Традиційні методи автентифікації, такі як паролі, PIN-коди та магнітні картки, постійно стають мішенями для хакерів. Біометрична автентифікація, яка базується на унікальних фізіологічних або поведінкових характеристиках особи, визначається як одна з найбільш перспективних технологій для забезпечення безпеки. Проте, поряд з перевагами, такий підхід привносить і нові виклики. На відміну від паролів, біометричні дані не можуть бути легко змінені у випадку компрометації, що робить їх захист вкрай важливим. З урахуванням вищезазначеного, розробка ефективних алгоритмів генерації унікального персонального ключа на основі біометричних параметрів людини стає актуальною та невідкладною задачею. Вивчення та розробка таких алгоритмів може сприяти створенню надійних систем захисту, які забезпечать конфіденційність, цілісність та доступність персональних даних користувачів. Тому дослідження в області генерації унікальних персональних ключів на основі біометричних параметрів є не тільки актуальним, а й вкрай важливим для розвитку сфери інформаційної безпеки в умовах сучасного цифрового світу.

Мета і завдання дослідження. Розробка та вивчення ефективних алгоритмів генерації унікального персонального ключа на основі біометричних параметрів людини з метою підвищення рівня безпеки систем автентифікації.

Реалізація цих завдань дозволить створити надійний і ефективний метод генерації біометричних ключів, який може бути впроваджений в різноманітних сферах застосування, від фінансових операцій до особистих електронних пристроїв.

Об'єкт дослідження. Процеси генерації унікальних персональних ключів з використанням біометричних параметрів людини, включаючи алгоритми, методи та технології, що застосовуються для цієї мети в сучасних системах ідентифікації та автентифікації.

Предмет дослідження. Алгоритми генерації унікального персонального ключа на основі біометричних параметрів (відбиток пальця, сітківка ока, голос), їхні основні характеристики, принципи роботи, а також методи їх інтеграції в сучасні системи автентифікації та захисту персональних даних.

Для досягнення цієї мети необхідно розв’язати наступні задачі:

1. Провести дослідження та класифікацію персональних даних
2. Дослідити біометричні персональні дані
3. Проаналізувати програмно-апаратні системи генерації ключів
4. Аналіз алгоритмів генерації персональних ключів
5. Розробити алгоритм генерації ключа на основі біометричних параметрах людини
6. Провести реалізації та тестування програмно-апаратної системи генерації персоналізованих ключів

Методи дослідження. В процесі виконання даної роботи було використано ряд методів дослідження, кожен з яких спрямований на вирішення конкретних завдань та досягнення поставленої мети:

1. Методи теоретичного аналізу та синтезу:
2. Методи експериментального дослідження:
3. Методи математичного моделювання та статистики:

Наукова новизна одержаних результатів полягає у виявленні та аналізі ключових факторів, що впливають на ефективність та безпеку систем генерації біометричних ключів. Особливу увагу приділено новітнім розробкам у галузі машинного навчання та штучного інтелекту, які відкривають нові можливості для підвищення точності та надійності біометричних систем. Крім того, в статті висвітлено важливі аспекти захисту приватності та етичні питання, пов'язані з обробкою біометричних даних.

Практичне значення отриманих результатів полягає у їх можливому застосуванні для покращення та оптимізації існуючих біометричних систем. Особливо цінними є висновки, що стосуються забезпечення безпеки та захисту даних в рамках цих систем, які можуть бути використані для розробки більш

надійних та безпечних методів аутентифікації та захисту інформації. Також результати дослідження можуть сприяти розвитку правових та етичних норм, що регулюють використання біометричних технологій, що є важливим для забезпечення довіри та прийняття цих технологій у суспільстві.

Публікації та апробація випускної кваліфікаційної роботи. Отримані результати апробовані в межах VIII науково-практичної конференції молодих вчених і студентів «Інтелектуальні комп'ютерні системи та мережі» Західноукраїнського національного університету та опубліковано дві тези доповідей за темою роботи [3,4].

Кваліфікаційна робота складається із трьох розділів, висновків, списку використаної літератури та додатків.

У першому розділі систематизовано та описано алгоритми систем захисту та персональних даних.

У другому розділі розроблено методи та алгоритми генерації персональних ключів.

У третьому розділі розроблено та реалізовано алгоритми системи генерації персонального біометричного ключа. Проведено тестування по функціонуванню розроблених алгоритмів.

1 СИСТЕМИ ЗАХИСТУ ТА ПЕРЕДАЧІ ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Персональні дані та системи їх захисту

Персональні дані - це будь-яка інформація, що стосується ідентифікованої або ідентифікованої фізичної особи. Це можуть бути такі дані, як ім'я, адреса, номер телефону, електронна пошта, ідентифікаційний номер, медичні записи тощо.

Захист персональних даних - це сукупність заходів, які призначені для забезпечення конфіденційності, цілісності та доступності персональних даних. Для цього використовуються технічні, організаційні та юридичні заходи.

Основні принципи захисту персональних даних включають:

- Право на інформацію - особа має право знати, які персональні дані збираються про неї, для яких цілей вони збираються і як довго вони зберігаються.
- Принцип обмеження цілей - персональні дані можуть збиратися тільки для певних законних цілей і не можуть використовуватися для інших цілей без згоди власника даних.
- Принцип необхідності та обґрунтованості - збір персональних даних має бути обмеженим тільки тими даними, які необхідні для виконання визначених цілей. Збір даних має бути обґрунтованим.
- Принцип точності - персональні дані мають бути точними та актуальними.
- Принцип обмеження зберігання - персональні дані мають зберігатися тільки протягом необхідного часу для виконання визначених цілей.
- Принцип цілісності та конфіденційності - персональні дані мають бути захищені від несанкціонованого доступу, втрати, зміни чи пошкодження.

Технічні заходи для захисту персональних даних включають шифрування, використання паролів та ідентифікаторів, захист мережі, захист пристроїв від вірусів та інших шкідливих програм. Організаційні заходи включають побудову відповідальної структури для захисту персональних даних, навчання персоналу з питань захисту даних, розробку політик та процедур збору, зберігання та обробки персональних даних. Юридичні заходи включають визначення прав та обов'язків

сторін, що займаються обробкою персональних даних, законодавчу базу для захисту даних, а також встановлення механізмів контролю за дотриманням вимог щодо захисту персональних даних [33].

Для правильного розуміння сутності питань захисту персональних даних необхідно визначити, які саме дані потребують особливого підходу та захисту. Зокрема, потрібно відрізняти загальні дані від даних, які вважаються конфіденційними або чутливими:

1. Основні (загальні) дані:
   - ПІБ (прізвище, ім'я, по батькові);
   - дата народження;
   - місце народження;
   - стать;
   - громадянство.
2. Контактні дані:
   - адреса проживання;
   - телефонний номер;
   - електронна пошта;
   - інші контактні дані.
3. Біометричні дані:
   - відбитки пальців;
   - сітківка ока;
   - голосові характеристики;
   - інші унікальні фізіологічні або поведінкові характеристики.
4. Чутливі дані:
   - расова або етнічна приналежність;
   - політичні погляди;
   - релігійні або світоглядні переконання;
   - членство в професійних спілках;
   - дані про здоров'я;

- дані про сексуальне життя або сексуальну орієнтацію;
- генетичні та біохімічні дані.

5. Економічні та фінансові дані:
   - номер банківського рахунку;
   - кредитна історія;
   - доходи та витрати;
   - власність та інші активи.
6. Дані про освіту та професійну діяльність:
   - освітні установи;
   - спеціальність;
   - місце роботи;
   - посада;
   - кваліфікація.
7. Дані про інтернет-діяльність:
   - IP-адреса;
   - місцезнаходження;
   - історія перегляду;
   - дані про використані додатки та послуги;
   - соціальні мережі.

Захист персональних даних є важливою проблемою у світі, де все більше інформації збирається та зберігається в електронному форматі [10]. Це має велике значення для індивідуальних прав та свобод, а також для бізнесу, який збирає та використовує персональні дані. Він повинен бути у фокусі уваги кожної компанії, яка збирає та обробляє ці дані. Порушення захисту може призвести до серйозних наслідків, таких як крадіжка особистої інформації, зловживання та використання цієї інформації для шахрайства, або незаконного доступу до банківських рахунків та інших особистих даних. Для захисту персональних даних, компанії повинні дотримуватися всіх вимог та стандартів, що стосуються збору, зберігання та

обробки цих даних. Крім того, необхідно використовувати відповідні технічні та організаційні заходи, щоб запобігти несанкціонованому доступу до цих даних [11].

З підвищенням обсягів даних, які обробляються щоденно, і зростанням значущості даних для сучасного суспільства, актуальність захисту персональних даних набуває все більшого значення. Процеси збору, зберігання та обробки даних потребують впровадження ефективних методів захисту для запобігання несанкціонованому доступу, втраті або витоку інформації [12].

У криптографії використовують симетричне та асиметричне шифрування. Симетричне шифрування використовує один і той же ключ для шифрування та дешифрування. Приклади: AES, DES, 3DES. Асиметричне шифрування використовує два різних ключа: приватний (закритий) та публічний (відкритий). Приклади: RSA, ECC.

У цифрових підписах використовуються для підтвердження автентичності даних і гарантування, що вони не були змінені після підпису.

Для мережевих засобів захисту використовують міжмережеві екрани, системи виявлення інтрузій та системи запобігання інтрузій. Міжмережеві екрани (firewalls) контролюють вхідний і вихідний мережевий трафік. Системи виявлення інтрузій (IDS) і системи запобігання інтрузіям (IPS) аналізують мережевий трафік на наявність аномалій або відомих сигнатур атак.

Для біометричного захисту використовують унікальні фізіологічні або поведінкові характеристики особи для ідентифікації. Приклади: відбитки пальців, сітківка ока, розпізнавання голосу.

Використання двох або більше методів аутентифікації для підтвердження особи користувача. Встановлення правил для визначення, хто може мати доступ до конкретних даних і як ці дані можна використовувати. Постійний збір та аналіз даних про доступ до систем та їх використання для виявлення аномалій та можливих порушень.

Сучасні методи захисту поєднуються, створюючи багаторівневі системи безпеки, які забезпечують надійний захист даних в різних ситуаціях. Завдяки

постійному розвитку технологій, нові методи і засоби захисту з'являються регулярно, допомагаючи адаптуватися до нових загроз і викликів [13].

Для ефективного захисту персональних даних, компанії можуть використовувати різні технології та методи, такі як шифрування даних, мультифакторна аутентифікація, контроль доступу, моніторинг та аналіз поведінки користувачів та інші. Крім того, компанії повинні мати відповідні політики та процедури щодо захисту персональних даних та регулярно оновлювати свої заходи безпеки, щоб бути в курсі нових загроз та вразливостей.

Крім захисту персональних даних, компанії також повинні відповідати за порушення безпеки даних та надавати компенсацію користувачам, які постраждали в результаті таких порушень. У деяких країнах існують спеціальні органи, які відповідають за регулювання та нагляд за захистом персональних даних, такі як Державна служба з охорони персональних даних в Україні та Комісія з охорони даних в Європейському Союзі.

Зі зростанням обсягів та важливості персональних даних у сучасному світі стає дедалі актуальнішою проблема їх безпеки. Під час збору, зберігання та обробки таких даних виникає багато потенційних ризиків та загроз.

Доступ до баз даних може призвести до витоку великих обсягів персональної інформації, який може бути використаний зловмисниками для шахрайства, крадіжок тощо. Техніка шахрайства, спрямована на отримання конфіденційних даних від користувача (логіни, паролі, номери кредитних карток) через маскування під надійні джерела. Різноманітне програмне забезпечення, яке може викрасти, змінити або знищити персональні дані на зараженому пристрої. Атаки "людина посередині" (Man-in-the-middle). Коли зловмисник перехоплює і можливо змінює комунікацію між двома сторонами без їх відома. Не завжди загроза приходить ззовні; іноді співробітники, або інші особи, які мають легальний доступ до системи, можуть зловживати своїми повноваженнями. Це може включати в себе крадіжку або втрату носіїв інформації, таких як жорсткі диски, ноутбуки, флешки тощо. Без регулярного аудиту та контролю системи можна пропустити потенційні порушення безпеки.

Розуміння цих ризиків та загроз є важливим для розробки ефективних стратегій та методів захисту персональних даних. Тому компанії та організації повинні приділяти особливу увагу захисту інформації та навчанню своїх співробітників основам інформаційної безпеки.

Важливо зазначити, що захист персональних даних стає все більш складною проблемою зі зростанням кількості даних та їх розподілом по різних системах та платформах. Тому, розвиток технологій та регулювання в цій сфері є надзвичайно важливими завданнями для забезпечення безпеки та конфіденційності персональних даних [14].

У світлі постійно зростаючого обсягу обробки персональних даних та високої важливості їхнього захисту було розроблено ряд стандартів та протоколів. Ці документи стали основою для впровадження надійних методів захисту інформації в багатьох організаціях та компаніях [15].

- ISO/IEC 27001: Це міжнародний стандарт управління безпекою інформації. Він визначає вимоги до системи управління безпекою інформації та включає в себе аспекти ризиків безпеки.
- GDPR (General Data Protection Regulation): Європейський регулятивний акт, який стосується обробки персональних даних. Це, можливо, найбільш відомий закон про захист даних у світі, який визначає вимоги до зберігання та обробки інформації про громадян ЄС.
- PCI DSS (Payment Card Industry Data Security Standard): безпеки даних для галузі платіжних карток. Він визначає вимоги для всіх організацій, які обробляють, передають або зберігають інформацію платіжних карток.
- HIPAA (Health Insurance Portability and Accountability Act): Американський закон, який регулює обробку медичної інформації. Цей акт встановлює вимоги до захисту медичних записів і іншої інформації про здоров'я.
- OpenID і OAuth: Протоколи аутентифікації та авторизації, які дозволяють користувачам взаємодіяти з ресурсами без необхідності передачі пароля або інших конфіденційних даних.

- TLS (Transport Layer Security): Протокол безпеки, який забезпечує захищене з'єднання між клієнтом і сервером через Інтернет.

Огляд стандартів та протоколів захисту персональних даних свідчить про глобальне усвідомлення важливості збереження та обробки інформації в безпечному середовищі. Кожен з розглянутих стандартів або протоколів має своє специфічне застосування, від фінансової сфери до медичних послуг, що демонструє універсальність підходів до захисту інформації.

Працюючи в сфері IT, особливо в напрямку обробки та зберігання персональних даних, важливо забезпечити дотримання відповідних стандартів і протоколів. Це не тільки підвищує довіру клієнтів та користувачів, але й забезпечує юридичний захист для організацій у випадку порушень або витоків даних.

Обробка персональних даних має здійснюватися законно, справедливо та прозоро для суб'єкта персональних даних. Всі дії, пов'язані з обробкою даних, повинні відповідати чинному законодавству. Персональні дані мають збиратися з конкретними, явно визначеними та законними метами і не можуть оброблятися способом, який є несумісним з цими метами. Збір персональних даних повинен бути обмежений тим, що дійсно необхідно для досягнення зазначених мет. Персональні дані мають бути точними та актуальними. Неточна інформація має бути видалена або виправлена без затримки. Персональні дані мають зберігатися в формі, яка дозволяє ідентифікувати суб'єкта даних не довше, ніж це необхідно для досягнення мети обробки персональних даних, що має здійснюватися таким чином, щоб забезпечувати належний захист даних від несанкціонованого або незаконного оброблення, втрати, знищення чи пошкодження. Відповідальність за дотримання принципів обробки персональних даних лежить на дата-контролері, який повинен забезпечувати і демонструвати дотримання цих принципів.

Враховуючи вищезазначені принципи, організації та установи повинні розробляти та впроваджувати відповідні політики і процедури з обробки персональних даних, що відповідають міжнародним стандартам та національному законодавству.

В сучасному світі технології обробки та зберігання персональних даних відіграють ключову роль. Новітні методи обробки даних не лише дозволяють ефективно керувати великими об'ємами інформації, але і гарантують її безпеку [16].

Хмарні рішення, такі як Google Cloud, AWS, Microsoft Azure та інші, дозволяють зберігати, обробляти та аналізувати персональні дані в масштабах, недосяжних для традиційних серверних рішень. Хмарні платформи пропонують ряд інструментів для захисту даних, включаючи шифрування, автоматичне резервне копіювання та багатофакторну аутентифікацію. Технологія блокчейн може бути використана для створення безпечних і прозорих систем зберігання даних, де кожна транзакція записується та зберігається без можливості зміни чи видалення. СУБД, такі як PostgreSQL, MongoDB, MariaDB, дозволяють гнучко та ефективно управляти великими об'ємами даних, пропонуючи при цьому розширений набір інструментів для їх захисту. Технології шифрування, такі як SSL/TLS для захищеного з'єднання, алгоритми AES чи RSA для шифрування даних, гарантують конфіденційність інформації під час передачі та зберігання. Алгоритми машинного навчання можуть бути використані для виявлення аномалій або підозрілих дій у базах даних, що сприяє попередженню можливих витоків. Сучасні технології захисту даних також включають в себе фізичний захист серверів і дата-центрів від несанкціонованого доступу, стихійних лих та інших загроз.

Враховуючи швидкий розвиток технологій і зростання об'ємів зберігання даних, важливо постійно моніторити та адаптуватися до нових методів та інструментів захисту, щоб гарантувати безпеку персональних даних на високому рівні.

1.2 Біометричні характеристики людини

Біометрія є науковою дисципліною, що займається вивченням унікальних фізіологічних та поведінкових характеристик особистості з метою її ідентифікації. Від грецького "біо" (життя) і "метрія" (вимірювання), біометрія є ключовою складовою сучасних систем безпеки, доступу та аутентифікації.

У сучасному світі, де технології постійно розвиваються, і важливість безпеки персональних даних стає все більш актуальною, біометрія відіграє ключову роль. Вона допомагає не тільки забезпечити конфіденційність даних, але і зменшити ризик шахрайства, незаконного доступу та ідентифікації.

Біометрія є важливою областю наукових досліджень та практичних застосувань, яка допомагає забезпечити безпеку, конфіденційність та ідентифікацію осіб у сучасному світі. Вона відіграє ключову роль у забезпеченні прав людини, зокрема права на приватність, і вимагає постійного вивчення та вдосконалення [17].

1. Відбиток пальця як біометрична характеристика.

Відбиток пальця є однією з найбільш розпізнаваних та широко використовуваних біометричних характеристик. Кожна людина має унікальний відбиток пальця, що формується ще до народження і залишається незмінним протягом життя.

Основними елементами відбитка пальця є папілярні лінії, дільники та озерця.

Папілярні лінії – це вигнуті лінії на поверхні пальця, які формують різноманітні малюнки. Дільники (відокремлення) – місця, де папілярні лінії розходяться або сходяться. Озерця – центральні точки малюнка відбитка пальця.

Для отримання цифрового зображення відбитка пальця використовуються спеціальні сканери. Ці сканери можуть бути оптичними, ультразвуковими або ємнісними. Після отримання зображення воно піддається обробці за допомогою алгоритмів, які виділяють ключові особливості відбитка для подальшої ідентифікації.

Відбитки пальців використовуються в різних сферах для ідентифікації особи, включаючи системи контролю доступу, ідентифікація осіб при перетині кордону, банківські операції. Розблокування смартфонів, планшетів та інших пристроїв. Автентифікація користувача при користуванні онлайн-послугами.

Переваги використання відбитка пальця:

- Висока точність: відбитки пальців є унікальними для кожної особи.
- Низька ймовірність помилки: сучасні системи можуть розпізнавати відбитки з великою точністю.

Недоліки використання відбитка пальця:

- Можливість підробки: є техніки, які дозволяють створити копії відбитків.
- Обмеження за станом шкіри: ушкодження або зміни на поверхні пальця можуть ускладнити розпізнавання.

Головні переваги цього методу включають велику швидкість розпізнавання, досить високу точність і відносну простоту інтеграції. Але є й недоліки: відбитки пальців можуть змінюватися впродовж життя, і їх можливо підробити за певних умов [18].

2. Сітківка ока як біометрична характеристика.

Сітківка ока представляє собою тонкий шар нервової тканини на задній частині очного яблука, який відповідає за сприйняття світла та перетворення його на нервові імпульси. Основні характеристики сітківки включають унікальний малюнок кровообігу та невеликі аномалії, такі як мікроаневризми.

Сканування сітківки виконується за допомогою спеціалізованого обладнання, яке використовує інфрачервоне випромінювання для створення детального зображення сітківки. Після отримання зображення воно аналізується з метою виявлення унікальних характеристик сітківки. Використання сітківки для біометричної ідентифікації є однією з найбільш точних методик.

Сітківка часто використовується в системах контролю доступу в стратегічно важливих об'єктах. В медичних системах як ідентифікація пацієнтів. У банківській сфері для клієнтів при виконанні високоризикових операцій.

Переваги використання сітківки ока:

- Висока точність: сітківка є унікальною для кожної особи і має низьку ймовірність помилки.
- Важко підробити: сітківка є вкрай складною для підробки чи копіювання.

Недоліки використання сітківки ока:

- Обладнання: потреба в спеціалізованому обладнанні для сканування сітківки.
- Незручно для користувача: процес може бути менш комфортним порівняно з іншими біометричними методами.

Сітківка ока вважається однією з найбільш точних біометричних технологій. Її унікальний малюнок кровообігу в сітківці важко підробити, і він залишається майже незмінним протягом усього життя особи. Однак, основними недоліками є потреба в спеціалізованому обладнанні для сканування та можливий дискомфорт для користувача під час процесу.

3. Голос як біометричний параметр

Голосова ідентифікація вже давно використовується в різних галузях, від систем безпеки до комерційних служб підтримки клієнтів. Голос — це унікальна характеристика особи, яка визначається анатомічною структурою гортані та іншими частинами дихальної системи, а також способом артикуляції і інтонуванням. Основні характеристики голосової біометрії наведені на рисунку 1.1.

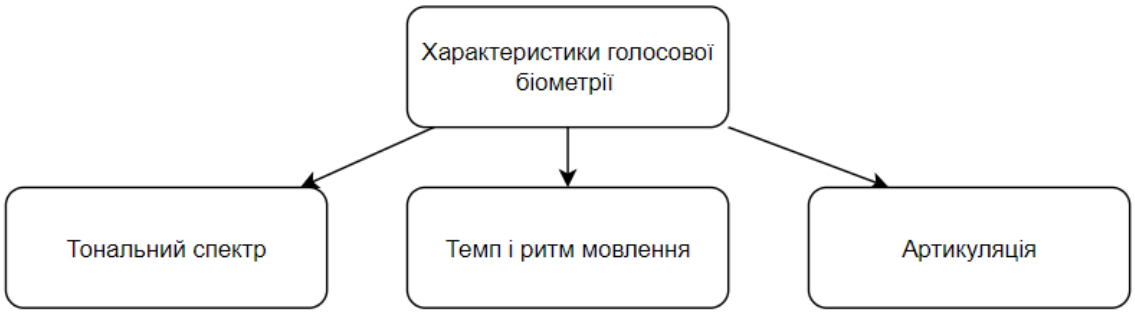

Рисунок 1.1 – Характеристики голосової біометрії

Переваги голосової біометрії:

- Зручність: Не потрібно спеціального обладнання, крім мікрофона.
- Дистанційне використання: Можливість проведення ідентифікації на відстані через телефон або Інтернет.

Недоліки:

- Змінність: Голос може змінюватися через захворювання, старіння або інші фактори.
- Підробка: Існують технології, які можуть імітувати голос людини.

Голосова біометрія активно використовується в банківській сфері, службах підтримки, системах безпеки й інших віддалених сервісах, де потрібна швидка і

зручна ідентифікація користувача. Голос як біометричний параметр має свої переваги та недоліки. Він може бути особливо корисним в комбінації з іншими біометричними параметрами для підвищення надійності системи ідентифікації.

4. Використання комбінованих біометричних параметрів для підвищення надійності. Ідентифікація особи на основі одного біометричного параметра може не завжди гарантувати абсолютну точність. Отже, дедалі більше систем безпеки починають використовувати комбіновані біометричні параметри для підвищення точності та надійності. Основні принципи комбінованої біометрії наведені на рисунку 1.2.

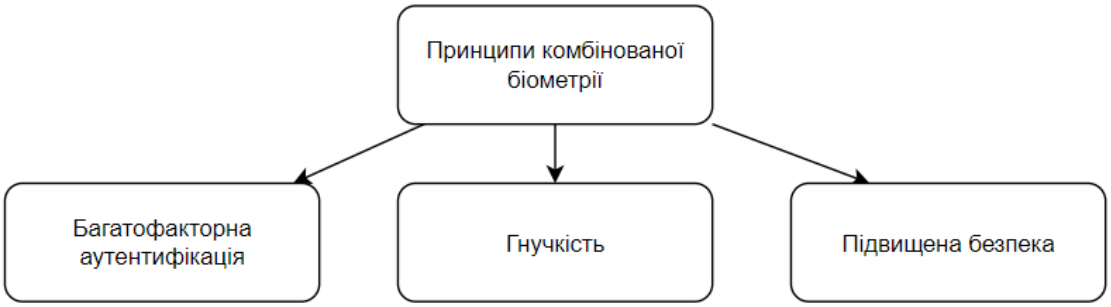

Рисунок 1.2 – основні принципи комбінованої біометрії

Основними перевагами комбінованої біометрії є підвищена безпека. Складніше обійти систему, яка вимагає кілька різних параметрів для входу. Точність. Співставлення декількох параметрів забезпечує менший ризик помилкового впізнавання. Гнучкість. Можливість вибору та комбінації різних параметрів відповідно до потреб.

Використання комбінованих біометричних параметрів стає нормою у сучасних системах безпеки, особливо в критичних додатках, таких як банківська сфера, аеропорти або державні установи. Комбінована біометрія пропонує рішення для недоліків, пов'язаних з використанням одного лише біометричного параметра. Вона забезпечує вищу надійність та безпеку, що робить її важливим інструментом у сучасних системах ідентифікації.

Комбінована біометрія є прогресивним і перспективним напрямком в сфері аутентифікації особистості, який відкриває нові горизонти в сфері інформаційної безпеки [19]. Її ключова особливість полягає в тому, що вона поєднує декілька різних біометричних параметрів, що значно знижує ризик помилкової ідентифікації або шахрайства. Однак, як і будь-яка технологія, комбінована біометрія має свої виклики та обмеження. Інтеграція різних біометричних систем може стати складною задачею, яка вимагає висококваліфікованих спеціалістів та відповідного обладнання. Це також збільшує вартість реалізації та впровадження таких систем. Крім того, зберігання та обробка більшого обсягу біометричних даних вимагає підвищення рівня безпеки, щоб уникнути порушень конфіденційності. Проте, незважаючи на ці виклики, комбінована біометрія має широкий спектр застосувань у різних галузях, від банківської сфери до медицини. Вона відіграє ключову роль у формуванні майбутнього цифрової безпеки, де надійна аутентифікація користувача стає все більш критичною. Для подальшого розвитку та удосконалення комбінованої біометрії важливо зосереджуватися на наступних напрямках: вдосконалення існуючих біометричних технологій, інтеграція з сучасними технологіями, такими як штучний інтелект, та розробка нових методів захисту та шифрування біометричних даних.

В узагальненому вигляді можна сказати, що комбінована біометрія – це майбутнє інформаційної безпеки, яке вже сьогодні активно формується завдяки дослідженням та інноваціям у цій області [20].

1.3 Програмні системи генерації персональних біометричних ключів

З початком ери інформаційних технологій, необхідність у захищеному зберіганні та передачі даних стала критично важливою. Програмні системи генерації ключів стали одним з основних інструментів, що забезпечують конфіденційність, цілісність та доступність даних у цифровому світі. Програмні системи генерації ключів – це комп'ютерні програми або системи, які використовуються для створення, зберігання та управління криптографічними ключами. Ці ключі можуть використовуватися для шифрування та дешифрування

інформації, а також для підписування цифрових документів, аутентифікації користувачів та інших завдань, пов'язаних із захистом інформації.

Системи можна класифікувати за рядом критеріїв:

- За способом генерації: детерміновані та випадкові.
- За областю застосування: загального призначення, спеціалізовані (наприклад, біометричні системи).
- За рівнем захисту: високий, середній, низький.

З історичної точки зору, потреба у створенні надійних методів шифрування виникла задовго до виникнення сучасних комп'ютерів. Древні цивілізації, такі як єгиптяни та римляни, використовували різноманітні методи кодування для передачі секретних повідомлень. Проте, з розвитком комп'ютерних технологій та глобальних мереж, виникла потреба у стандартизованих системах, що можуть працювати на великих масштабах та забезпечити високий рівень захисту. В Україні, як і в багатьох інших країнах, активний розвиток програмних систем генерації ключів розпочався у 90-х роках XX століття, паралельно із загальним ростом інформаційних технологій. Відтоді, індустрія безпеки інформації та програмні рішення для генерації ключів продовжують свій розвиток, адаптуючись до змінюваних умов та викликів сучасного світу.

При розробці програмних систем генерації ключів дотримуються певних принципів та методологій, щоб забезпечити ефективність, безпеку та надійність роботи систем [21]. Одним з найважливіших принципів є криптографічна стійкість. Це властивість системи опиратися проти спроб атаки, намагаючись зламати ключ чи систему шифрування. Стійкість залежить від довжини ключа, алгоритму шифрування та способу генерації ключа. Секретність забезпечує, що ключі генеруються, зберігаються та передаються у захищеному вигляді. Це допомагає запобігти несанкціонованому доступу до ключів та можливій компрометації системи. Важливим принципом при генерації випадкових ключів є ентропія - міра непередбачуваності ключа. Висока ентропія забезпечує, що ключ буде важко передбачити або вгадати. Для забезпечення надійності роботи системи та підвищення її безпеки часто використовують принцип розділення функцій. Це

означає, що різні частини процесу генерації ключа відокремлені та виконуються різними компонентами чи суб'єктами.

При розробці систем генерації ключів можуть використовуватися різні методології, зокрема:

- Водопадна модель: послідовний підхід до розробки, де кожен етап виконується послідовно до початку наступного.
- Гнучкі методології (Agile): підхід, що зосереджений на ітераційному розвитку та залученні клієнта у процес розробки.
- TDD (Test-Driven Development): методологія, де спочатку пишуться тести, а потім код, який повинен пройти ці тести.

Застосування цих принципів та методологій дозволяє створювати надійні та захищені програмні системи генерації ключів.

При розробці програмних систем генерації біометричних ключів важливо вибрати оптимальний набір технологій та інструментів, що відповідають специфіці дослідження, та водночас забезпечують надійність і безпеку кінцевих продуктів [22]. Основні мови програмування для розробки систем генерації біометричних ключів наведено на рисунку 1.3.

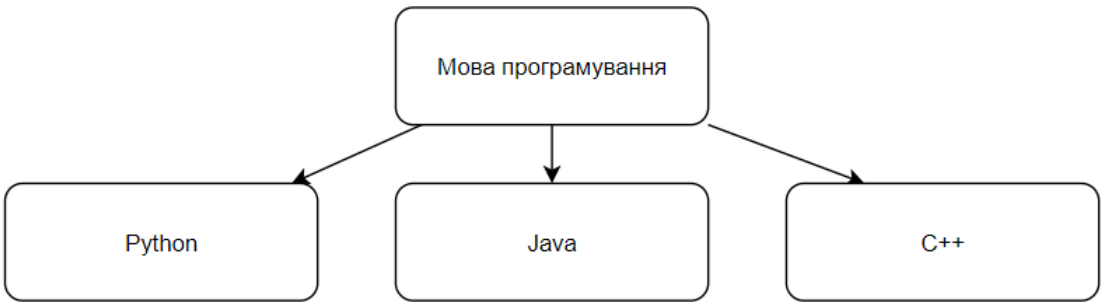

Рисунок 1.3 – Мови програмування для розробки систем генерації біометричних ключів

Завдяки бібліотекам як TensorFlow та OpenCV, Python є популярним вибором для розробки біометричних систем. Java також активно використовується в цій галузі завдяки своїй портативності та здатності до високої продуктивності. C++

часто застосовується для розробки реалізацій, які потребують високої швидкості обробки, завдяки своїй високій продуктивності та доступу до низькорівневих операцій. Бібліотеки та фреймворки, які найчастіше використовуються у розробці, наведені на рисунку 1.4.

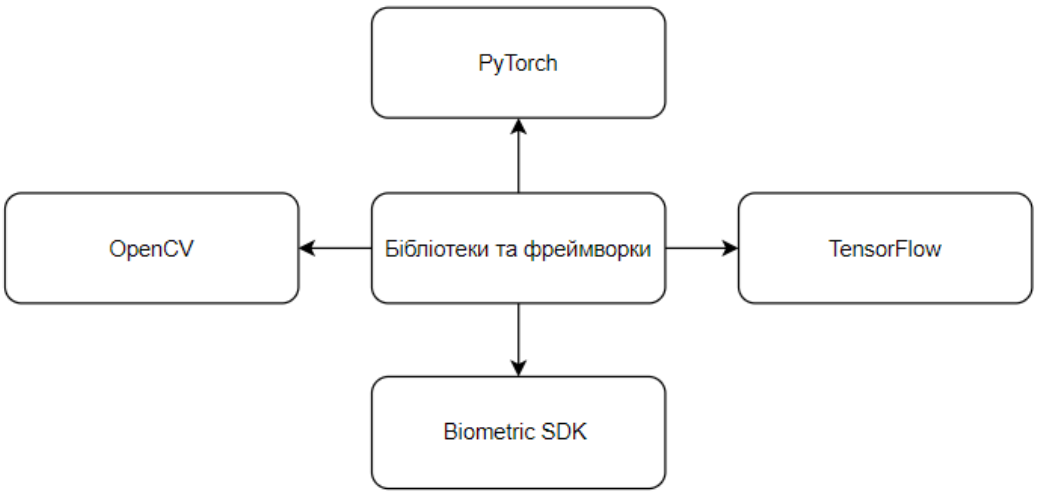

Рисунок 1.4 – Бібліотеки та фреймворки

OpenCV популярна бібліотека обробки зображень та комп'ютерного зору, яка надає інструменти для аналізу біометричних даних. TensorFlow та PyTorch – фреймворки глибокого навчання, які можуть використовуватися для розробки нейронних мереж для аналізу біометричних даних. Biometric SDK –спеціалізовані набори розробника, що надають функціональність для розробки систем на основі конкретних біометричних параметрів.

Використовується два види баз даних. SQL бази даних (MySQL, PostgreSQL) використовуються для зберігання біометричних профілів та інших даних користувача. NoSQL бази даних (MongoDB, Cassandra) можуть використовуватися для зберігання великих об'ємів біометричних даних завдяки їх горизонтальній масштабованості.

Основними технологіями безпеки є: SSL/TLS: для захищеної передачі даних між клієнтом та сервером, хешування (наприклад, SHA-256): для безпечного зберігання

даних та верифікації їх цілісності, криптографічні бібліотеки (OpenSSL, libsodium): для реалізації функцій шифрування та аутентифікації в програмних системах.

Враховуючи специфіку біометричних систем генерації ключів, при їх розробці важливо зосередитися на технологіях, які надають не тільки високу продуктивність, але й високий рівень безпеки

При розробці програмних систем генерації біометричних ключів існують численні виклики та ризики, які потрібно враховувати, щоб забезпечити ефективність, безпеку та надійність результуючого продукту. Біометричні параметри, такі як відбитки пальців, сітківка ока або голос, можуть змінюватися з часом або під впливом різних факторів (наприклад, травми). Це може ускладнити визначення особи або генерацію ключа [23]. Необхідність в спеціалізованому обладнанні для отримання високоякісних біометричних даних може призвести до великих витрат. Хоча біометричні дані є унікальними, вони також можуть бути вкрадені, підроблені або змінені, що створює ризики безпеки. Збір та зберігання біометричних даних викликає питання щодо конфіденційності особистої інформації. Технічні обмеження. При розробці програмних систем необхідно враховувати обмеження відповідного апаратного забезпечення, а також можливі проблеми із сумісністю різних компонентів системи. Потрібно враховувати законодавчі регуляції щодо використання біометричних даних, що можуть відрізнятися в різних країнах. При неправильному введенні біометричних даних або при їх пошкодженні можуть виникати проблеми із доступом до ресурсів або інформації. Збір та використання біометричних даних може викликати етичні питання, особливо у контексті інформованої згоди користувача.

Розробка програмних систем генерації біометричних ключів є складною та багатогранною задачею, яка вимагає глибокого розуміння технічних, правових та етичних аспектів. Щоб забезпечити надійність і безпеку таких систем, розробники повинні враховувати всі можливі ризики та виклики.

Для успішної інтеграції біометричних систем в існуючі IT-інфраструктури, особливо важливо використовувати стандартні протоколи та інтерфейси. Це забезпечує сумісність, масштабованість та здатність до модифікацій [24].

- BioAPI. Це відкритий стандарт, який надає загальний інтерфейс для різних біометричних технологій. BioAPI визначає, як програмні модулі біометрики мають взаємодіяти з різними системами та додатками.
- BAC (Biometric Application Programming Interface). Це інтерфейс, який забезпечує взаємодію між прикладними програмами та біометричними пристроями, такими як сканери відбитків пальців.
- WS-Biometric Devices. Це стандарт веб-служби для доступу до біометричних пристроїв через мережу.
- Common Biometric Exchange File Format (CBEFF). Стандарт, що визначає формати даних для обміну біометричною інформацією між різними системами.
- ISO/IEC 19794. Серія міжнародних стандартів, які визначають формати біометричних даних для різних видів біометрії, таких як відбитки пальців, обличчя та голос.
- ISO/IEC 24745. Стандарт, який визначає заходи безпеки для захисту біометричних даних від несанкціонованого доступу та підробки.

Завжди важливо переконатися, що обрані стандарти сумісні з поточною IT-інфраструктурою та вимогами організації. Технології швидко розвиваються, тому стандарти можуть вимагати оновлення. Організації мають слідкувати за новими версіями стандартів і адаптуватися до них. Дотримання стандартів може забезпечити базовий рівень безпеки, але завжди потрібно розглядати додаткові заходи захисту, щоб відповідати конкретним потребам організації.

Використання стандартних протоколів та інтерфейсів є критично важливим для успішної інтеграції біометричних систем в різні IT-інфраструктури. Це не тільки спрощує процес інтеграції, але і гарантує безпеку, сумісність та здатність до масштабування [25].

Біометричні дані – це унікальні фізіологічні або поведінкові характеристики особи, які можуть бути використані для ідентифікації або верифікації її особистості. Важливість коректного зберігання та обробки таких даних не може бути переоцінена, оскільки вони часто мають велику цінність та чутливість.

Правильне зберігання та обробка біометричних даних вимагає комплексного підходу, що враховує технічні, організаційні та законодавчі аспекти. Тільки забезпечуючи високий рівень безпеки та конфіденційності на кожному етапі життєвого циклу даних, можна гарантувати їх надійне та безпечне використання.

Важливою характеристикою сучасних програмних систем, які використовують біометричні ключі, є їх адаптивність та гнучкість. Це відноситься до здатності системи пристосовуватися до змінних умов використання, нових технологій та змінних вимог користувачів.

Сучасні системи здатні працювати з різними типами біометричних даних, від відбитків пальців до голосової активності. Гнучка система може підтримувати нові формати без необхідності глобального редагування коду.

Оскільки потреби організацій можуть змінюватися, програмні системи повинні бути скальованими, щоб відповідати зростаючим або зменшуваним потребам.

Здатність інтегруватися з іншими IT-системами та платформами є ключовим аспектом гнучкості. Це може включати в себе інтеграцію з системами управління бази даних, хмарними сервісами або іншими програмами безпеки.

Адаптивні системи повинні вміти вірно реагувати на різні помилки або непередбачувані обставини, які можуть виникнути під час роботи з біометричними даними. Це може включати неправильний ввід даних, пошкоджені файли або намагання злому.

Щоб залишатися актуальними та ефективними, системи мають регулярно оновлюватися. Гнучка система забезпечує простоту додавання нових функцій, вдосконалення безпеки та інших важливих оновлень.

Адаптивність та гнучкість є ключовими атрибутами сучасних програмних систем, які працюють з біометричними ключами. Такі системи повинні бути здатні пристосовуватися до змінних умов, нових технологій та потреб користувачів, щоб забезпечити надійний та ефективний захист даних.

Однією з основних проблем при використанні біометричних даних для генерації ключів є забезпечення їх безпеки та конфіденційності. Втрата або

компрометація біометричних даних може призвести до незворотних наслідків, адже відмінно від паролів чи карток доступу, біометричні характеристики людини змінити неможливо.

1.4 Висновки до розділу та постановка задач кваліфікаційної роботи

Після глибокого аналізу систем захисту та передачі персональних даних, а також вивчення аспектів біометричних характеристик людини та програмних систем генерації персональних біометричних ключів, можна сформулювати наступні висновки:

- Персональні дані в сучасному світі стають ключовим ресурсом, що вимагає високого рівня захисту, особливо в контексті зростаючої кількості кібератак та порушень даних.
- Біометричні характеристики набувають популярності як надійний засіб аутентифікації, але при цьому несуть ризики, пов'язані з порушенням приватності.
- Програмні системи для генерації персональних біометричних ключів покращують безпеку даних, але водночас мають ліміти та можливі вектори атак.

На основі цих висновків, ціль даної магістерської роботи полягає в розробці надійного алгоритму для генерації унікального персонального ключа на основі біометричних параметрів людини.

Для досягнення цієї мети було поставлено наступні завдання:

1. Аналіз існуючих методів генерації персональних ключів.
2. Дослідження найбільш релевантних біометричних параметрів для генерації ключів.
3. Розробка алгоритму генерації ключа на основі вибраних параметрів.
4. Тестування та оптимізація розробленого алгоритму.
5. Аналіз етичних та соціальних аспектів впровадження таких систем.

З урахуванням зроблених висновків та поставлених завдань, наступний етап роботи буде спрямований на вивчення методів та алгоритмів генерації персональних ключів.

2 МЕТОДИ ТА АЛГОРИТМИ ГЕНЕРАЦІЇ ПЕРСОНАЛЬНИХ КЛЮЧІВ

2.1 Алгоритми генерації цифрових ключів

Визначення та класифікація криптографічних ключів

Криптографічний ключ – це інформаційна послідовність, яка використовується в криптографічних алгоритмах для шифрування або дешифрування даних. Залежно від функціональності та методу використання, ключі поділяють на декілька типів:

- Симетричні ключі: Використовуються один і той же ключ для шифрування та дешифрування. Приклади алгоритмів: DES, AES.
- Асиметричні ключі: Використовуються різні ключі для шифрування та дешифрування - публічний ключ для шифрування та приватний ключ для дешифрування. Приклади алгоритмів: RSA, ECC.

Основні принципи роботи симетричних та асиметричних ключів:

- Симетричне шифрування вважається досить надійним, якщо ключ зберігається в таємниці. Основна вада - обидві сторони повідомлення повинні мати доступ до ключа, що ставить під загрозу безпеку передачі ключа.
- Асиметричне шифрування вирішує проблему безпечної передачі ключа. Публічний ключ можна передавати відкрито, але тільки власник відповідного приватного ключа може розшифрувати повідомлення. Це шифрування, зазвичай, вимагає більше часу на обробку через велику математичну складність.

Застосування специфічного ключа залежить від вимог до безпеки та доступних ресурсів. Симетричні ключі швидше обробляють дані, тоді як асиметричні ключі надають вищий рівень безпеки при передачі даних. Симетричне шифрування є вкрай ефективним у випадках, коли великі обсяги даних потребують швидкої обробки без значного збільшення витрат на ресурси. Асиметричне шифрування, використовуючи пару ключів, є ідеальним для умов, де важливі безпека та ідентифікація. Порівняння симетричного та асиметричного шифрування наведено у таблиці 2.1.

Таблиця 2.1 – Порівняння симетричного та асиметричного шифрування

Критерій	Симетричне Шифрування	Асиметричне Шифрування
Тип ключів	Один ключ для шифрування та дешифрування.	Два ключі: приватний та публічний.
Швидкість обробки	Зазвичай швидше, менш обчислювально інтенсивне.	Повільніше через більшу обчислювальну складність.
Застосування	Часто використовується для шифрування даних у масштабі.	Переважно для шифрування невеликих обсягів даних, часто використовується для шифрування ключів симетричного шифрування або для цифрового підпису.
Управління ключами	Управління ключами може бути складним, оскільки потребує безпечного обміну ключем між сторонами.	Легше управління ключами, оскільки публічний ключ може бути відкритим, а приватний ключ залишається в користувача.
Рівень безпеки	Високий, але залежить від безпечного обміну ключами.	Вважається більш безпечним, особливо при великих довжинах ключів, але залежить від збереження приватного ключа.
Приклади алгоритмів	AES, DES, 3DES, Blowfish.	RSA, ECC, ElGamal, DSA.
Складність реалізації	Відносно простіше для реалізації.	Більш складне у реалізації, особливо при роботі з ключами.
Використання	Ідеально підходить для шифрування великих обсягів даних, таких як бази даних або файлові системи.	Часто використовується для обміну ключами, цифрових підписів та аутентифікації.

Приклад застосування ключів:

- Симетричний ключ: Два користувача, хочуть обмінюватися зашифрованими повідомленнями. Вони домовляються про секретний ключ (наприклад, "12345") і використовують його для шифрування та дешифрування своїх повідомлень. Якщо хтось інший спробує перехопити їхнє повідомлення, він не зможе його розшифрувати без правильного ключа. Приклад створення наведено на рисунку 2.1.

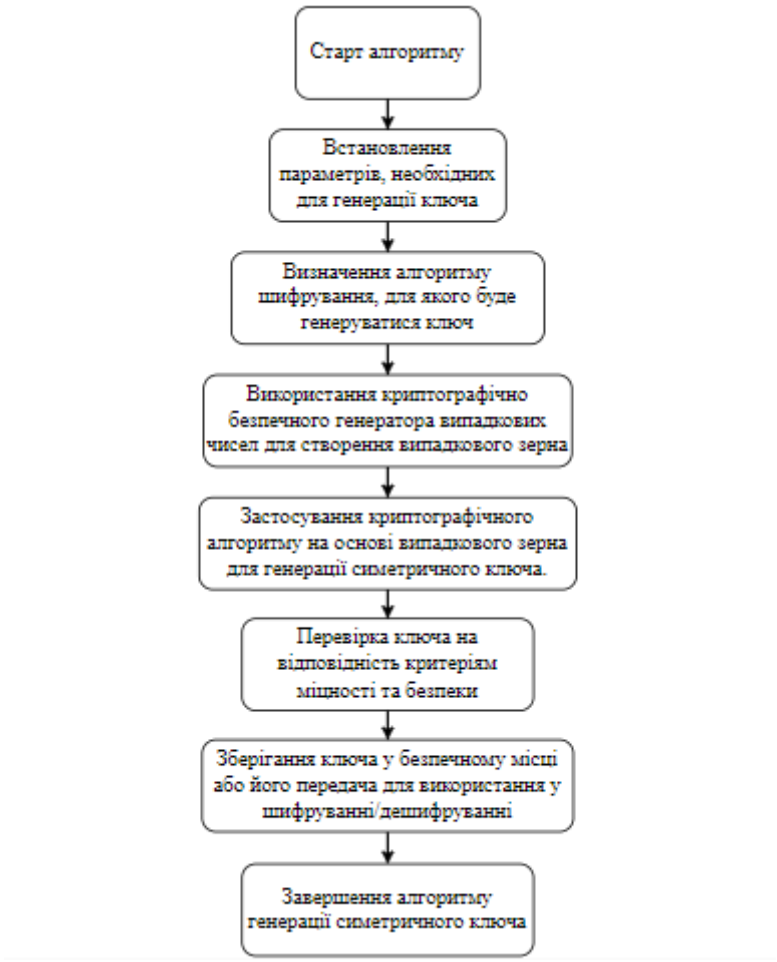

Рисунок 2.1 – схема створення симетричного ключа

- Асиметричний ключ: Агент «А» генерує пару ключів: публічний та приватний. Вона надсилає свій публічний ключ Агенту «Б» і зберігає приватний ключ в таємниці. Агент «Б» шифрує повідомлення для Агента «А», використовуючи її публічний ключ, і надсилає їй. Тільки Агент «А», маючи

приватний ключ, може розшифрувати повідомлення. Приклад створення наведено на рисунку 2.2.

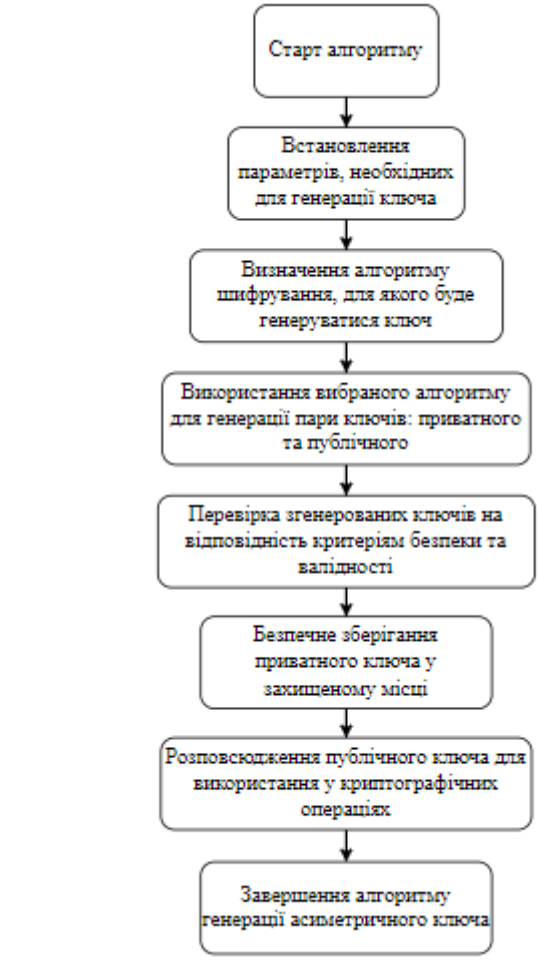

Рисунок 2.2 – схема створення асиметричного ключа

- Якщо вони використовують симетричний ключ для обміну повідомленнями і цей ключ стає відомий третій особі, всі їхні комунікації можуть бути розшифровані. Тому важливо регулярно змінювати ключі та забезпечувати їх безпечне зберігання.

Банківські установи часто використовують асиметричне шифрування для обміну даними з клієнтами в онлайн-банкінгу. Коли користувач хоче увійти в свій аккаунт, банк шифрує запит допомогою публічного ключа користувача. Тільки користувач, маючи відповідний приватний ключ, може розшифрувати запит та надати відповідь. Сучасні системи криптографічного захисту інформації базуються на двох основних класах алгоритмів шифрування: симетричні (або закритого

ключа) та асиметричні (або відкритого ключа). Ці алгоритми використовують різні підходи до генерації, зберігання та обміну ключами. У симетричних системах один ключ використовується як для шифрування, так і для дешифрування інформації. З цієї причини ключ повинен бути збережений в секреті від несанкціонованих користувачів [26].

Приклади: DES (Data Encryption Standard), AES (Advanced Encryption Standard), RC4.

Використання у генерації ключів: Такі ключі часто генеруються випадковим чином та потребують механізмів зберігання та обміну в безпечний спосіб. У асиметричних системах використовуються два ключі: приватний (закритий) та публічний (відкритий). Публічний ключ може бути відкрито доступним, але приватний ключ повинен залишатися в секреті. Основні алгоритми генерації ключів:

Генерація надійних криптографічних ключів є важливою складовою безпечної системи шифрування. Якість ключа, а саме його випадковість та непередбачуваність, грає рішучу роль у захисті інформації від несанкціонованого доступу. В даному розділі будуть розглянуті найбільш популярні алгоритми генерації ключів.

Псевдовипадкові генератори чисел використовують математичні алгоритми для генерації послідовностей чисел, які схожі на випадкові. Linear Congruential Generators (LCG), Mersenne Twister зазвичай використовуються у комбінації з іншими методами для покращення випадковості ключа.

Алгоритми на основі ентропії збирають випадковість (або ентропію) з зовнішніх джерел, таких як рухи миші користувача, інтервали між натисканням клавіш та ін./dev/random в Unix-подібних системах. Забезпечують високу випадковість ключа, особливо при комбінованому використанні з ПВГЧ. Фізичні генератори випадкових чисел – це фізичні процеси для генерації випадковості, такі як радіоактивний розпад. Засновані на квантових явищах генератори. Зазвичай використовуються у високобезпечних системах, де необхідна максимальна випадковість. Генератори на основі криптографічних алгоритмів використовують

криптографічні примітиви, такі як функції хешування та блочні шифри, для генерації випадкових послідовностей. Fortuna, CryptGenRandom в Windows забезпечують високий рівень безпеки ключа та широко використовуються у сучасних криптографічних застосунках. Основна мета цих алгоритмів – забезпечити створення ключів, які було б важко передбачити або відтворити. З урахуванням цієї мети важливо регулярно перевіряти та оновлювати методи генерації ключів, щоб вони відповідали сучасним стандартам безпеки.

Псевдовипадкові генератори чисел (ПВГЧ) відіграють важливу роль у криптографії. Хоча такі генератори не створюють справжньо-випадкові числа, вони генерують послідовності, які важко передбачити або відрізнити від випадкових.

При генерації секретного ключа для шифрування важливо, щоб цей ключ був випадковим і непередбачуваним. Це забезпечує, що атакуючий не може здогадатися або відтворити ключ. У багатьох режимах блочного шифрування використовується випадковий ініціалізаційний вектор для кожного шифрування, що забезпечує унікальність кожного зашифрованого повідомлення. При встановленні безпечного з'єднання, наприклад, при використанні SSL або TLS, використовуються випадкові числа для обміну ключами та аутентифікації. Більшість ПВГЧ починають з вихідного параметра (або "зерна") і використовують його для генерації послідовності чисел. Цей вихідний параметр повинен бути випадковим. Хоча ПВГЧ генерують числа, які виглядають випадково, вони є повністю передбачуваними, якщо ви знаєте вихідний параметр. Тобто, якщо ви знаєте вихідний параметр, ви можете відтворити всю послідовність.

Деякі криптографічні ПВГЧ використовують криптографічні функції хешування для генерації псевдовипадкових послідовностей. Багато криптографічних бібліотек та стандартів включають ПВГЧ спеціально для криптографічних застосувань. Наприклад, в Python є бібліотека secrets, яка надає функції для генерації безпечних випадкових чисел і рядків. Алгоритм генерації наведений на рисунку 2.3.

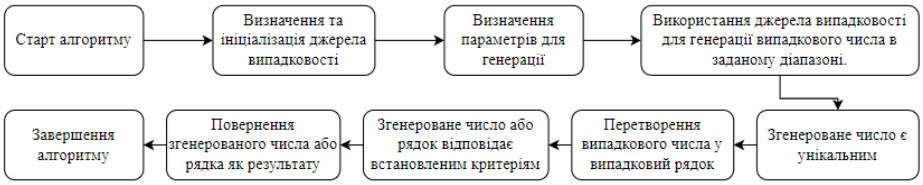

Рисунок 2.3 – Алгоритм генерації безпечних випадкових чисел і рядків

Псевдовипадкові генератори чисел є критично важливими для багатьох аспектів криптографії, від генерації ключів до створення унікальних ініціалізаційних векторів. Правильний вибір і використання ПВГЧ може значно підвищити безпеку криптографічної системи.

Ключова управлінська інфраструктура (PKI) – це комплекс технологій, служб та політик, які використовуються для управління цифровими сертифікатами та ключами в сучасних інформаційних системах. PKI дозволяє підтвердити автентичність цифрового представника чи об'єкта, гарантує конфіденційність, цілісність даних та підтвердження їхньої достовірності.

PKI автоматизує процес генерації пари ключів: приватного та публічного. Правильно налаштована PKI забезпечує, що ключі генеруються в безпечному оточенні, недоступному для зовнішніх атак.

Роль PKI у зберіганні ключів: приватні ключі, як правило, зберігаються в захищених модулях або спеціалізованих апаратних засобах, таких як криптографічні токени. Дистрибуція публічних ключів: PKI дозволяє безпечно дистрибютувати публічні ключі між користувачами та системами. Це здійснюється за допомогою цифрових сертифікатів, які підтверджують аутентичність публічного ключа. Відновлення та анулювання ключів: У разі втрати приватного ключа або компрометації ключа PKI дозволяє швидко анулювати діючий сертифікат та відновити ключі [27]. Огляд основних компонентів інфраструктури відкритих ключів наведено у таблиці 2.2

Таблиця 2.2 – Опис компонентів PKI

Компонент	Опис
Сертифікаційний Центр (CA)	Установа, що видає та підтверджує цифрові сертифікати. Відповідає за випуск, управління, анулювання та поновлення сертифікатів.
Реєстр (RA)	Помічник CA, який перевіряє запити на сертифікати перед їх обробкою CA.
База Даних Сертифікатів	Зберігає всі видані та анульовані сертифікати.
Список Відкликаних Сертифікатів (CRL)	Список сертифікатів, які були анульовані до закінчення строку їх дії.
Кінцевий Користувач	Особа або система, яка використовує сертифікати для забезпечення безпечного обміну інформацією.
Ключовий Сервер	Забезпечує безпечне зберігання приватних ключів та управління ними.
Шлюз Безпеки	Забезпечує безпечний обмін даними між різними мережами або системами.
ПЗ для Клієнтів	Програмне забезпечення, що встановлюється на стороні користувача для використання функцій PKI.

У сучасному світі PKI є фундаментом для безпечного електронного обміну інформацією, забезпечуючи конфіденційність, автентифікацію та невід'ємність повідомлень.

Безпека генерації цифрових ключів відіграє критичну роль у криптографічних системах. Якщо ключ генерується, зберігається або передається ненадійно, це може призвести до компрометації усієї системи безпеки.

Генеровані ключі повинні бути дійсно випадковими, щоб забезпечити їхню непередбачуваність. Використання слабких або передбачуваних джерел випадковості може призвести до ключів, які легко відновлюються. Ентропія є мірою випадковості. При генерації ключів важливо мати достатню кількість ентропії, щоб зробити ключ непередбачуваним. Після генерації ключ повинен бути

збережений у безпечному місці. Використання апаратних засобів безпеки, таких як HSM (апаратні модулі безпеки) або криптографічні токени, може допомогти у цьому. Процес генерації ключа повинен бути захищений від будь-яких зовнішніх спроб втручання або вивчення. Важливо передбачити, як довго ключ буде використовуватися, і коли його слід замінити. Це запобігає можливості атаки "на використання ключа протягом тривалого часу". Регулярний аудит та моніторинг генерації ключа допомагає виявляти будь-які аномалії або потенційні проблеми.

Виклики безпеки при генерації ключів. Апаратні проблеми можуть зменшити випадковість генерованих ключів. Якщо генератор ключів ініціалізується слабким або передбачуваним значенням, ключі можуть стати передбачуваними. Сторонні атаки можуть спробувати вплинути на процес генерації ключа, спрямовуючи його на виробництво слабших ключів.

Безпечна генерація ключів є фундаментом для створення надійних криптографічних систем. Вона вимагає уважності до деталей, використання надійних методів та алгоритмів, а також постійного моніторингу та аудиту.

Алгоритми генерації цифрових ключів використовуються в ряді практичних застосувань, що забезпечують безпеку та приватність даних. Типові практичні приклади наведені у таблиці 2.3.

Таблиця 2.3 – Приклади практичного застосування.

Назва	Опис
SSL/TLS сертифікати	Коли ви відвідуєте веб-сайт, що використовує HTTPS, це гарантує, що ваші дані передаються безпечно. Це здійснюється завдяки алгоритмам генерації ключів, які створюють пару ключів: публічний і приватний.
VPN (віртуальні приватні мережі)	VPN дозволяє користувачам безпечно підключатися до приватних мереж через публічний інтернет. Це здійснюється за допомогою алгоритмів генерації ключів, які створюють унікальні сесійні ключі для кожної сесії.

Продовження таблиці 2.3

Електронний підпис	Цифрові ключі використовуються для створення і перевірки електронних підписів, які підтверджують автентичність та цілісність документа або повідомлення.
Двофакторна автентифікація	Додатковий рівень безпеки при вході в систему може вимагати від користувача введення одноразового пароля, що генерується за допомогою спеціального ключа.
Зашифровані зберігання даних	Дискове зашифровування, таке як BitLocker або FileVault, використовує ключі для шифрування і розшифровування даних на вашому комп'ютері.
Безпечні месенджери	Месенджери, такі як Signal або WhatsApp, використовують ключі для шифрування повідомлень, так що лише відправник та отримувач можуть їх прочитати.
Блокчейн і криптовалюта	Транзакції і гаманці в блокчейн-системах, таких як Bitcoin, використовують ключі для підтвердження власності та проведення безпечних транзакцій.

Алгоритми генерації цифрових ключів відіграють критичну роль у забезпеченні безпеки і конфіденційності даних. Враховуючи швидкість розвитку технологій та зростаючу потребу в захищеній інформації, можна стверджувати, що алгоритми генерації ключів будуть продовжувати грати важливу роль у майбутніх дослідженнях та розробках в галузі інформаційної безпеки [28].

Алгоритми генерації цифрових ключів є вітальним інструментом у сучасному цифровому світі, де інформаційна безпека виступає як один з найбільш пріоритетних напрямків. Ці алгоритми відіграють критичну роль у забезпеченні конфіденційності, цілісності та доступності даних. З дослідження алгоритмів генерації цифрових ключів стає очевидним, що вони можуть бути використані у різноманітних сценаріях: від стандартних методів аутентифікації користувачів до

складних систем шифрування для захисту передачі даних на великі відстані. Основна цінність таких алгоритмів полягає у їхній спроможності створювати унікальні, непередбачувані ключі, які важко зламати чи відтворити. Це забезпечує високий рівень безпеки та довіри до систем, які використовують ці ключі для захисту інформації. Проте, поряд із численними перевагами, існують і питання, пов'язані з управлінням ключами, їх зберіганням та обміном. Управлінські інфраструктури ключів, такі як PKI, служать відповіддю на ці виклики, пропонуючи стандартизовані рішення для ефективного управління життєвим циклом ключів. Враховуючи стрімке зростання цифрових технологій та все більше загроз для інформаційної безпеки, важливість алгоритмів генерації цифрових ключів лише зростатиме. Тому їх дослідження, вдосконалення та адаптація під конкретні задачі є актуальним та важливим завданням для спільноти спеціалістів з інформаційної безпеки.

2.2 Алгоритми генерації біометричних ключів

Біометричні системи з кожним роком набувають все більшої популярності в сучасних системах аутентифікації. Вони пропонують набагато більш надійну та інтуїтивно-зрозумілу методологію порівняно з традиційними паролями та магнітними картками. Основа біометричної аутентифікації – це унікальні фізичні чи поведінкові характеристики особи. Біометрія є науковим напрямком, який зосереджений на вивченні унікальних фізичних або поведінкових характеристик особи з метою її ідентифікації або верифікації. Дана галузь знаходить застосування у численних системах безпеки, доступу та автентифікації [29]. Основні принципи біометрії наведені у таблиці 2.4. З огляду на ці принципи можна сказати, що біометричні системи намагаються максимізувати коректність ідентифікації особи, при цьому мінімізуючи ризик помилок.

Таблиця 2.4 – Основні принципи біометрії

Основний принцип	Опис
Унікальність	Біометричні дані повинні бути унікальними для кожної особи, щоб забезпечити точну ідентифікацію.
Стабільність	Біометричні характеристики повинні залишатися стабільними протягом тривалого часу.
Захист від підробки	Система біометрії повинна бути захищена від шахрайства та підробки, наприклад, використання фальшивих відбитків пальців.
Зручність використання	Система повинна бути зручною для кінцевих користувачів.
Швидкість обробки	Обробка біометричних даних має бути достатньо швидкою для забезпечення ефективного доступу.
Масштабованість	Система біометрії повинна бути здатною до масштабування, щоб обслуговувати різні обсяги користувачів.
Безпека даних	Біометричні дані повинні бути захищені від несанкціонованого доступу та витоку інформації.
Відмова від помилкового доступу	Система повинна мінімізувати ймовірність неправильної ідентифікації чи помилкового доступу.
Згода на обробку даних	Використання біометричних даних повинно відбуватися зі згоди особи, до якої ці дані належать.

Використання біометрії як джерела для генерації ключів дозволяє створити ряд унікальних ключових систем, які базуються на фізичних або поведінкових характеристиках особи. Відмінність таких систем полягає в тому, які саме біометричні дані використовуються та яким чином вони обробляються для отримання ключа [30].

Вирізняють декілька типів біометричних ключів:

- Відбитки пальців: це найпоширеніший тип біометричного ідентифікаційного ключа. Основна характеристика, яка використовується, – це мінуси та лінії на поверхні пальця. Такі ключі часто використовуються в мобільних пристроях для блокування/розблокування.
- Сітківка та радужка ока: сітківка ока має унікальний шаблон кровоносних судин, в той час як радужка має унікальний текстурний шаблон. Обидва ці типи можуть бути використані для створення високоунікальних ключів.
- Голос: голосові ключі базуються на унікальних характеристиках голосу особи. Ці характеристики включають тон, тембр, швидкість мовлення та ін.
- Лице: характеристики обличчя, такі як відстань між очима, форма носа, розташування родимок можуть бути використані для створення біометричних ключів.
- Динаміка ходьби: деякі системи можуть використовувати унікальні характеристики способу, яким людина ходить, для генерації ключа.
- Серцевий ритм: електрокардіограми (ЕКГ) або пульс можуть бути використані для генерації біометричних ключів на основі унікальних серцевих характеристик особи.

Порівняння різних типів біометричних ключів, вказуючи їх основні переваги та недоліки наведено у таблиці 2.5.

Таблиця 2.5 – Порівняння типів біометричних ключів

Тип біометричного ключа	Переваги	Недоліки
Відбитки пальців	Широко розповсюджені, висока точність, простота використання.	Можливість підробки, вразливість до бруду та пошкоджень на пальцях.

Продовження таблиці 2.5

Сітківка та радужка ока	Висока точність, складно підробити, стабільність з часом.	Потребує спеціального обладнання, може бути некомфортним для деяких користувачів.
Голос	Зручність використання, можливість віддаленого доступу.	Вразливий до шуму, змін голосу (наприклад, через застуду), можливість підробки.
Лице	Безконтактний метод, широко доступний (через смартфони та камери).	Вразливий до змін зовнішності (заростання бороди, макіяж), освітлення, виразів обличчя.
Динаміка ходьби	Менш інвазивний, може бути зібраний на відстані.	Низька точність порівняно з іншими методами, вплив зовнішніх факторів (взуття, підлога).
Серцевий ритм	Унікальний для кожної особи, може бути зібраний без відома особи.	Потребує спеціального обладнання для моніторингу, вплив фізичного стану та емоцій на ритм серця.

Вибір конкретного типу біометричного ключа залежить від конкретних потреб безпеки, зручності використання, доступності обладнання, а також вимог до приватності і точності.

При виборі конкретного типу біометричного ключа важливо враховувати зручність використання, ступінь безпеки та надійність. Хоча деякі типи ключів, такі як відбитки пальців або радужка ока, можуть надавати вищий рівень безпеки, інші, такі як голос або динаміка ходьби, можуть бути менш надійними через зовнішні фактори, такі як шум або зміна стану здоров'я особи [31].

Процес генерації біометричних ключів полягає в перетворенні біометричних даних, отриманих від особи, в унікальний цифровий код, який може бути використаний для аутентифікації або шифрування.

Збір біометричних даних. Це перший крок, де відбувається взяття зразка біометричних даних від користувача за допомогою сенсора (наприклад, сканера відбитків пальців, камери тощо).

Попередня обробка. Цей етап включає в себе видалення шумів, нормалізацію, вирівнювання та інші техніки обробки, щоб підготувати даний біометричний зразок до подальшого аналізу.

Виділення ознак. За допомогою специфічних алгоритмів з біометричних даних виділяються ключові ознаки. Наприклад, для відбитків пальців це можуть бути мінуси або лінії.

Кодування. Ознаки перетворюються у цифровий формат, який може бути використаний як ключ. Цей процес може включати в себе хешування, квантування або інші методи кодування.

Зберігання та використання ключа. Отриманий біометричний ключ може бути збережений на пристрої або в централізованій базі даних. Цей ключ потім може бути використаний для різних застосувань, таких як аутентифікація, шифрування або електронний підпис.

Порівняння ключів. При спробі доступу система знову збере біометричний зразок, перетворить його у ключ і порівняє з раніше збереженим ключем.

Важливим моментом у процесі генерації біометричних ключів є забезпечення конфіденційності та цілісності даних. Будь-яке втручання або зміни в біометричних даних можуть зробити ключ непридатним для використання, тому від відбору зразка до його зберігання і використання необхідно забезпечити високий рівень безпеки.

Створення біометричного ключа на основі біометричних даних є складним завданням, що вимагає спеціалізованих бібліотек та інструментів. ключові етапи процесу створення біометричного ключа на основі відбитків пальців наведені у таблиці 2.6

Таблиця 2.6 – Ключові етапи процесу створення біометричного ключа

Етап	Опис
Зчитування зображення	Використання сканера або іншого сенсорного пристрою для зчитування зображення відбитка пальця.
Виявлення мінутій	Застосування спеціалізованих алгоритмів для виявлення мінутій (характерних точок), таких як закінчення та розгалуження ліній на відбитку пальця.
Генерація ключа	Створення унікального біометричного ключа на основі виявлених мінутій. Цей ключ використовуватиметься для ідентифікації або верифікації особи.

2.3 Алгоритми генерації унікального цифрового ключа на біометричних параметрах людини

Теорія роботи алгоритмів генерації унікального цифрового ключа на основі біометричних параметрів людини обумовлена необхідністю забезпечення високого рівня безпеки при ідентифікації особи. Біометричні параметри включають унікальні фізіологічні та поведінкові характеристики людини, такі як відбитки пальців, сканування сітківки ока, риси обличчя тощо. Дані збираються за допомогою спеціалізованих сенсорів, що перетворюють фізичні властивості в цифрові дані. Збір біометричних даних залежить від специфіки обраної біометричної характеристики та апаратної підтримки. Наприклад, для відбитків пальців можуть знадобитися спеціалізовані сканери, тоді як для розпізнавання обличчя можуть використовуватися стандартні камери. Попередня обробка біометричних даних є дуже важливою, оскільки вона допомагає підготувати дані для подальшого аналізу і визначення унікальних особливостей особи. Цей процес може включати фільтрацію шумів, вирівнювання контрасту, нормалізацію, сегментацію тощо. Етапи підготовки збору біометричних параметрів наведені у таблиці 2.7.

Таблиця 2.7 – Етапи підготовки збору біометричних параметрів

Етап	Опис
Вибір біометричного параметра	Визначення типу біометричних даних, які будуть використані (наприклад, відбитки пальців, сітківка ока).
Підготовка обладнання	Налаштування та калібрування обладнання для збору біометричних даних (наприклад, сканер відбитків пальців).
Інструктаж користувача	Інформування користувача про процес збору даних та необхідні дії з їхнього боку.
Збір даних	Власне процес збору біометричних даних за допомогою відповідного обладнання.
Первинна обробка	Попередня обробка зібраних даних, яка може включати фільтрацію шумів, корекцію зображення тощо.
Перевірка якості даних	Оцінка якості зібраних біометричних даних для визначення їх придатності до подальшого аналізу.
Зберігання або передача даних	Збереження зібраних даних для подальшої обробки або передача їх в систему обробки.

Попередня обробка біометричних даних є дуже важливою, оскільки вона допомагає підготувати дані для подальшого аналізу і визначення унікальних особливостей особи. Цей процес може включати фільтрацію шумів, вирівнювання контрасту, нормалізацію, сегментацію тощо.

Завантаження зображення: завантажуємо зображення обличчя у відтінках сірого для простішої обробки.

Нормалізація: метод equalizeHist використовується для нормалізації гістограми зображення. Це поліпшує контраст зображення, роблячи його яскравішим і дозволяючи виділити основні особливості обличчя.

Видалення шумів: метод fastNlMeansDenoising використовується для видалення шумів з зображення. Шум може бути в результаті поганого освітлення

або низької якості камери. Видалення шуму допомагає покращити якість зображення та підвищити точність визначення біометричних особливостей. Зберігання обробленого зображення: зберігаємо після обробки зображення.

Генерація біометричного шаблону — це складний процес, який зазвичай включає в себе виявлення унікальних особливостей біометричного зразка (наприклад, відбиток пальця, зображення сітківки ока чи лицеві точки) і створення з них даних, які можна порівняти. Алгоритм який створює біометричний шаблон на основі відбитку пальця.

Оскільки текстурні особливості легше виявити на зображенні відтінків сірого, перетворюємо кольорове зображення. Метод для екстракції текстурних особливостей, який порівнює кожен піксель із його сусідами і кодує цю інформацію у двійковому вигляді. Використовуємо гістограму LBP значень для створення шаблону, який ефективно відображає текстурні особливості відбитку пальця [32]. Нормалізуємо гістограму, щоб уніфікувати представлення шаблону, роблячи його менш чутливим до змін в освітленні чи контрасті.

Верифікація та автентифікація на основі біометричних даних – це процес, в якому спочатку визначається відповідність поданого біометричного шаблону зареєстрованому шаблону, а потім на основі цієї відповідності вирішується, чи надати доступ користувачу до системи. Перевірка шаблону: Функція verify_biometric_key отримує збережений ключ, сіль і шаблон, який представлений для верифікації. Генерація хешу для верифікації: Створюється хеш з наданого біометричного шаблону і збереженої солі за тим же алгоритмом, що було використано для створення збереженого ключа. Якщо хеш наданого шаблону з сіллю відповідає збереженому ключу, користувач верифікований. Процес верифікації є дуже чутливим до змін у біометричних даних, тому на практиці зазвичай використовуються складніші методи зіставлення, які можуть обробляти невеликі варіації в біометричних шаблонах. Зазвичай це реалізується за допомогою спеціалізованого біометричного зіставлювального ПЗ або апаратного забезпечення.

Крім того, для зберігання і обробки біометричних даних важливо використовувати заходи безпеки, щоб захистити конфіденційність і цілісність даних.

Оновлення системи біометричної верифікації та автентифікації може включати оновлення біометричного шаблону користувача, параметрів системи або безпекових політик. Оскільки оновлення біометричного шаблону може відбуватися за різними причинами, як-от зміна біометричних характеристик або покращення точності. Функція оновлення: update_biometric_template використовується для оновлення біометричного шаблону користувача. Вона приймає ідентифікатор користувача та нові біометричні дані. Для нового біометричного шаблону генерується нова сіль, щоб забезпечити безпеку хешування. Створюється новий хешований ключ на основі нового біометричного шаблону та солі [33]. Інформація оновлюється в базі даних за допомогою функції «update_biometric_template_in_db». Схема оновлення біометричного шаблону користувача відображена на рисунку 2.4.

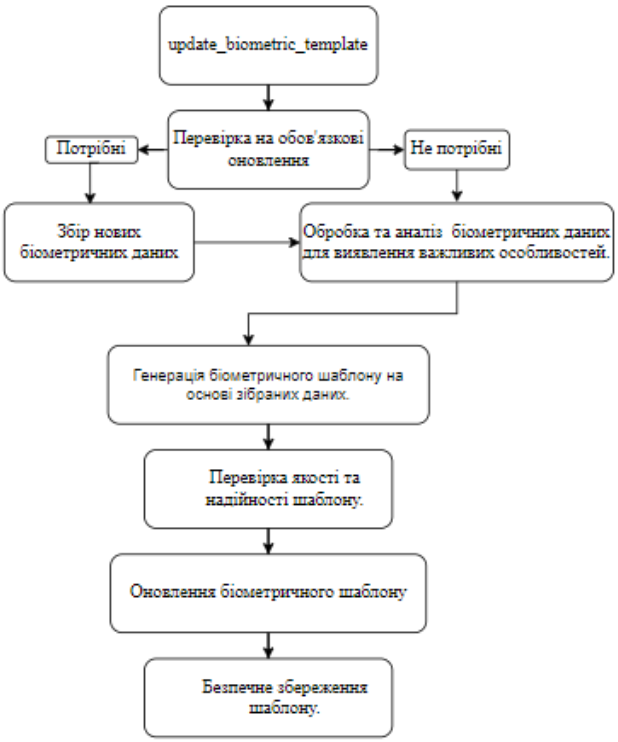

Рисунок 2.4 – Оновлення біометричного шаблону користувача

Алгоритми генерації унікальних цифрових ключів, що базуються на біометричних параметрах, відіграють важливу роль у сучасних системах аутентифікації. Інтеграція біометричних технологій з криптографічними методами дозволяє створювати надійні, неповторні та безпечні ключі, які важко підробити або відтворити. Використання хеш-функцій, функцій розсіювання, аналізу мінуцій відбитків пальців, іридології, розпізнавання обличь, а також потенціалу ДНК для генерації ключів, є ключовими стратегіями у цій області. Кожен із цих методів має свої унікальні переваги, які вибираються в залежності від вимог безпеки, прийнятності для користувачів та доступних ресурсів. Незважаючи на технологічний прогрес, існують певні виклики, зокрема точність збору даних, обробка шумів, захист від підробки та забезпечення приватності користувачів. Розвиток алгоритмів генерації ключів з біометричних даних повинен враховувати ці виклики, а також неухильно слідувати принципам криптографічної стійкості та етичної обробки особистих даних.

3 ПРОГРАМУВАННЯ СИСТЕМИ ГЕНЕРАЦІЇ ПЕРСОНАЛЬНОГО БІОМЕТРИЧНОГО КЛЮЧА

3.1 Структура програмної системи генерації біометричного ключа

Структура програмної системи генерації біометричного ключа описує організацію та взаємодію між різними модулями та компонентами системи, які спільно виконують завдання створення унікального біометричного ключа.

Інтерфейс користувача (UserInterface) взаємодіє з модулем збору біометричних даних (BiometricDataCollector), ініціюючи процес збору даних. Користувач через інтерфейс відправляє команду на збір даних, і модуль активує відповідне обладнання. Після збору біометричних даних, BiometricDataCollector передає ці дані в модуль попередньої обробки (PreprocessingModule). Тут відбувається фільтрація шуму, нормалізація та інші процедури обробки для підготовки даних. Оброблені дані передаються з PreprocessingModule в модуль екстракції особливостей (FeatureExtractor). Цей модуль аналізує дані для виділення ключових характеристик, які будуть використані для генерації ключа. Отримані особливості передаються в модуль генерації ключа (KeyGenerator). Цей модуль використовує спеціалізовані алгоритми для перетворення особливостей у унікальний біометричний ключ. Після створення біометричного ключа, KeyGenerator передає його для зберігання в модулі збереження ключів (KeyStorage). Це забезпечує безпечне зберігання ключа. Модуль аутентифікації (AuthenticationModule) взаємодіє з KeyStorage для перевірки біометричного ключа під час спроб доступу до системи. AuthenticationModule запитує ключ з KeyStorage і порівнює його з наданими біометричними даними для аутентифікації користувача. База даних (Database) використовується для зберігання біометричних даних, шаблонів та інформації про ключі. Вона може взаємодіяти з різними модулями для надання або зберігання необхідної інформації. Кожен з цих компонентів відіграє важливу роль у загальній роботі системи. Схема взаємодії модулів системи генерації біометричного ключа відображена на рисунку 3.1.

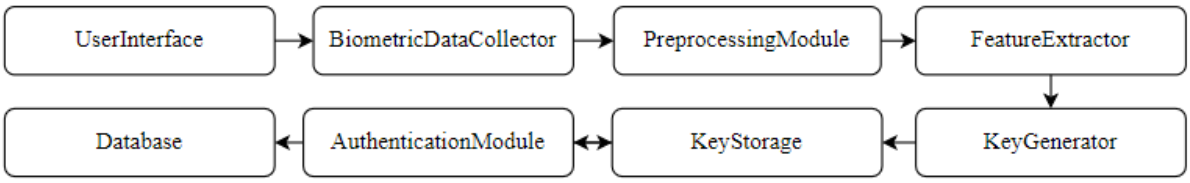

Рисунок 3.1 – Схема взаємодії модулів системи генерації біометричного ключа

Для створення ефективної програмної системи генерації біометричного ключа, важливо розуміти, як саме компоненти системи взаємодіють та залежать один від одного. До структури входять наступні елементи:

- Реєстрація користувача

Процес реєстрації користувача в системі генерації персонального біометричного ключа є фундаментальним кроком, що визначає надійність і безпеку усієї системи. Цей етап не тільки створює основу для подальшої ідентифікації та аутентифікації користувача, але й впливає на загальне сприйняття системи з боку користувачів. Процес реєстрації користувача відображено на рисунку 3.2

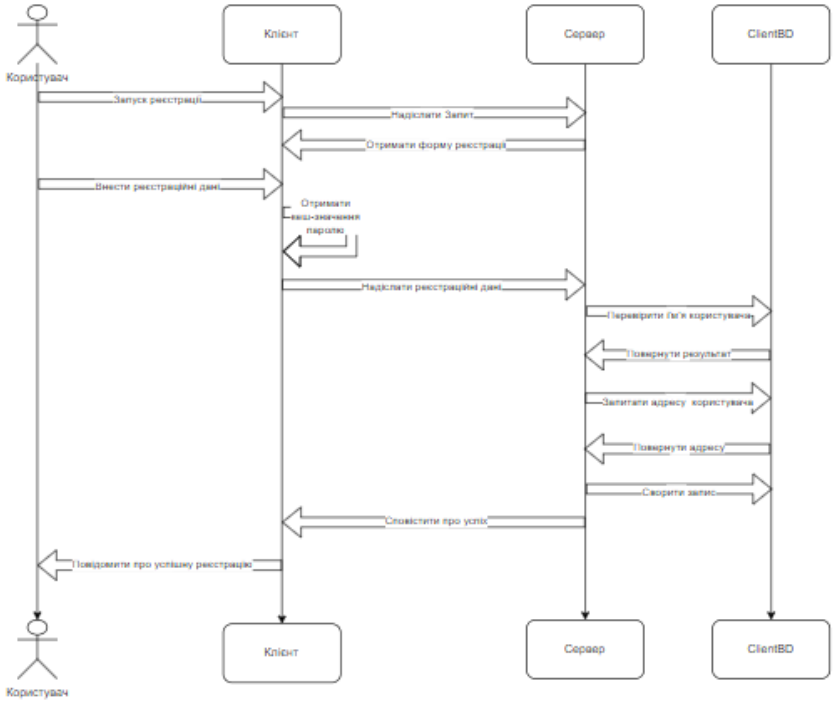

Рисунок 3.2 – процес реєстрації користувача

- Менеджер датчиків

Менеджер датчиків є ключовим компонентом у системах генерації персонального біометричного ключа, відповідаючи за взаємодію з фізичними датчиками, які захоплюють біометричні дані користувачів. Цей модуль забезпечує збір, передачу та первинну обробку даних, що отримані від різних біометричних датчиків. Для використання в роботі запропонований сканер відбитків пальців ZKTeco рисунок 3.3.

Рис 3.3 – Сканер відбитків пальців «ZKTeco»

Схему обробки відбитка пальця сканером ZKTeco наведено на рис 3.4. Схема відображає типовий процес взаємодії між користувачем, системою та сканером.

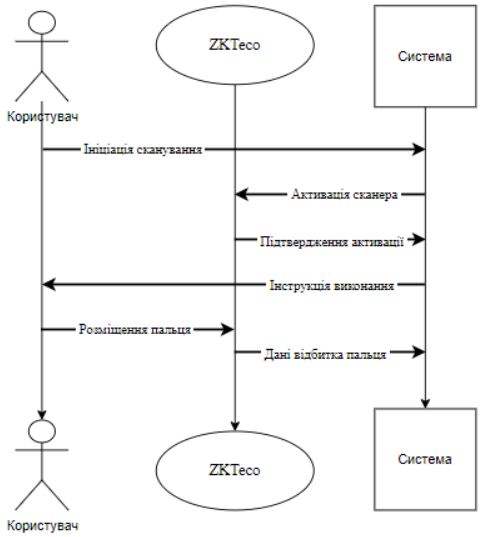

Рисунок 3.4 – Схема обробки відбитка пальця

- Модуль обробки даних

Модуль обробки даних бере на себе завдання обробки та перетворення сирих біометричних даних, отриманих від датчиків, у формат, придатний для подальшого аналізу та використання. Цей модуль не тільки перевіряє, чи біометричні дані є точними та чіткими для ефективного аналізу, але й гарантує, що ці дані обробляються належним чином, щоб забезпечити безпеку та конфіденційність інформації. Обробка також включає в себе перевірку якості вхідних даних, щоб уникнути помилок у генерації ключів, які можуть виникнути через низьку якість або несправність датчиків. Схема процесу обробки даних зображена на рисунку 3.5.

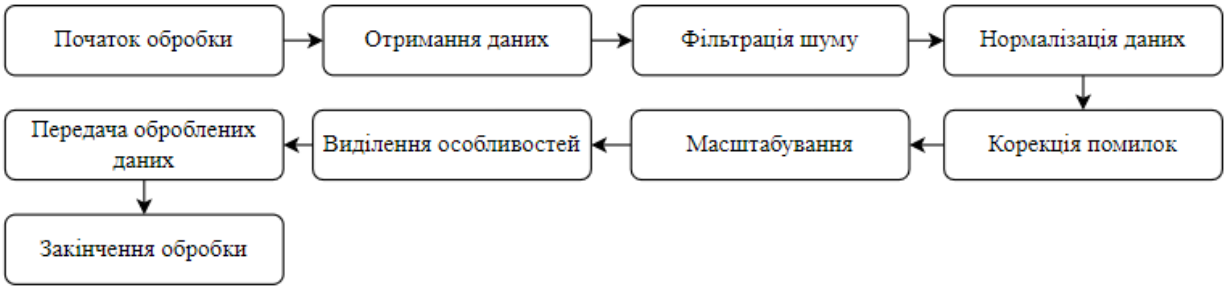

Рисунок 3.5 – Схема процесу обробки даних

- Алгоритмічний модуль

Алгоритмічний модуль відіграє вирішальну роль у перетворенні оброблених біометричних даних на унікальний ключ. Цей модуль включає ряд алгоритмів та процедур, які забезпечують аналіз, шифрування та вироблення ключів з біометричних даних. Алгоритмічний модуль тісно пов'язаний з модулем збору даних та модулем зберігання ключів. Він отримує вхідні дані від модуля збору даних і передає згенерований ключ до модуля зберігання ключів для безпечного зберігання. Завдання алгоритмічного модуля наведені у таблиці 3.1 Якість та ефективність алгоритмів безпосередньо впливає на надійність та безпеку згенерованих біометричних ключів. Він також працює з чутливими біометричними даними, він має включати механізми для забезпечення безпеки та конфіденційності цих даних протягом усього процесу обробки. Основні функції алгоритмічного модуля наведені у таблиці 3.2.

Таблиця 3.1 – Завдання алгоритмічного модуля

Компонент	Опис	Ключові Функції
Аналіз біометричних даних	Використання алгоритмів для аналізу та перетворення біометричних даних в унікальний код.	• Функції хешування • Визначення унікальності
Шифрування даних	Застосування криптографічних протоколів для захисту біометричних даних.	• Криптографічні протоколи • Ключове управління
Генерація ключів	Перетворення оброблених даних у стабільний криптографічний ключ.	• Алгоритми вироблення ключів • Механізми оновлення ключів

Таблиця 3.2 – Функції алгоритмічного модуля

Функція	Опис
Забезпечення безпеки	Гарантування, що біометричні дані не можуть бути використані для відновлення оригінальних біометричних образів.
Ефективність та швидкість	Забезпечення швидкої та ефективної обробки для реального часу генерації ключів.
Масштабність	Спроможність модуля обробляти велику кількість запитів та даних без зниження продуктивності.
Адаптивність	Здатність адаптуватися до різних типів біометричних даних та сценаріїв використання.

- Керування ключами

Модуль керування ключами є важливим компонентом у системі генерації біометричних ключів, відіграючи критичну роль у забезпеченні безпеки та ефективності процесу шифрування. Він керує ключами, які є основою для забезпечення безпеки та конфіденційності системи. Принципи керування ключами наведено у таблиці 3.3.

Таблиця 3.3 – Керування ключами

Аспект	Опис	Методи та стратегії
Генерація ключів	Створення криптографічних ключів.	Випадкове генерування Використання криптографічно сильних генераторів
Зберігання ключів	Безпечне зберігання ключів для запобігання несанкціонованому доступу.	Шифрування ключів при зберіганні Використання захищених сховищ
Розподіл ключів	Передача ключів між уповноваженими сторонами.	Зашифровані канали передачі Протоколи обміну ключами
Оновлення ключів	Регулярне оновлення ключів для збереження безпеки.	Автоматичне або ручне оновлення Політики ротації ключів
Скасування ключів	Вилучення або деактивація ключів, які більше не потрібні.	Процедури безпечного знищення Журналювання та аудит
Хешування та соль	Посилення безпеки ключів за допомогою додаткових заходів.	Використання солі в хеш-функціях. Заходи проти атак на основі словників
Системи управління ключами (KMS)	Автоматизація процесів управління ключами.	Централізоване управління Моніторинг та аудит
Відповідність стандартам	Дотримання законодавчих та галузевих стандартів.	Відповідність GDPR, HIPAA Регулярний перегляд політик
Реагування на інциденти	Планування дій на випадок інцидентів безпеки.	Процедури відновлення після інцидентів Негайне реагування на витоки
Резервне копіювання та відновлення	Запобігання втраті ключів через помилки або збої.	Регулярне резервне копіювання Плани відновлення даних

Безпечне зберігання криптографічних ключів вимагає застосування додаткових заходів безпеки, щоб запобігти несанкціонованому доступу. Один з підходів - це шифрування ключів перед їхнім зберіганням. Можна зашифрувати криптографічний ключ за допомогою пароля, а потім зберегти його у файлі.

Ключ шифрується за допомогою алгоритму Fernet, ключ для шифрування генерується з пароля за допомогою PBKDF2HMAC. Сіль (salt) додається для підвищення стійкості до атак на основі словників. Зашифрований ключ разом із сіллю зберігається у файлі.

KeyManager використовується для управління набором ключів, збережених у JSON файлі. Метод validate_keys перевіряє ключі на актуальність, видаляючи застарілі. Метод update_key_expiry дозволяє оновити термін дії конкретного ключа.

3.2 Програмні модулі

- Модуль захоплення біометричних даних

Модуль захоплення відбитків пальців є першим та одним із найважливіших компонентів системи генерації біометричного ключа. Його основне завдання - забезпечити точне та якісне захоплення біометричних даних. Захоплення біометричних даних наведено у таблиці 3.4.

Таблиця 3.4 – Захоплення біометричних даних

Аспект	Деталі	Опис
Захоплення зображення	Високоякісні сканери	Використання спеціалізованих сканерів для отримання чітких зображень відбитків пальців з відповідною роздільною здатністю та контрастністю.
Первинна обробка зображення	Автоматична корекція	Автоматизоване виправлення яскравості, контрасту та вирівнювання зображення для підготовки до подальшої обробки.
Валідація зображення	Контроль якості	Перевірка та оцінка якості захопленого зображення з можливістю повторного сканування у разі необхідності.
Безпека та конфіденційність	Захист даних	Забезпечення захисту біометричних даних під час захоплення та передачі, дотримання політик конфіденційності.
Технічна реалізація	Сумісність із обладнанням	Гнучка інтеграція з різними типами біометричних сканерів, програмне забезпечення для управління процесом сканування.

Для захоплення зображення використовуються високоякісні сканери відбитків пальців, які забезпечують високу роздільну здатність та точність деталей. Алгоритм сканування відбитка пальця наведений у додатку А.

Це дозволяє отримати чіткі зображення відбитків, для корекції яскравості та контрастності, що допомагає мінімізувати спотворення та покращує якість відбитків. Приклад захоплення відбитка пальця зображено на рисунку 3.6.

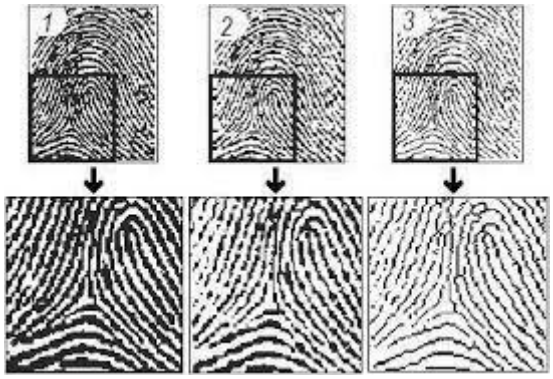

Рисунок 3.6 – Зображення захоплення відбитка

Первинна обробка зображень є критичним етапом у процесі захоплення відбитків пальців. Цей процес передбачає ряд кроків для підготовки зображень до подальшої детальної обробки та аналізу.

Автоматична корекція самостійно корегує зображення відбитків для покращення якості, включаючи вирівнювання, фільтрацію шумів та корекцію спотворень. Це забезпечує надійну основу для наступних етапів обробки та аналізу. Для візуального представлення первинної обробки зображень у модулі захоплення відбитків пальців, можна створити схему, яка послідовно демонструє ключові кроки цього процесу. Схема підготовки зображення подається на рисунку 3.7.

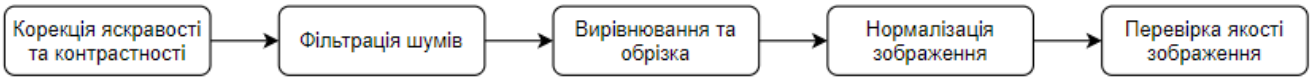

Рисунок 3.7 – Схема підготовки зображення

Валідація зображень включає оцінку якості захопленого зображення для забезпечення його придатності для подальшого аналізу та використання у системі генерації біометричних ключів.

Алгоритм написання програмного коду наведений у додатку Б.

Безпека та конфіденційність є ключовими аспектами, які забезпечують захист біометричних даних користувачів від несанкціонованого доступу, використання чи розкриття. Схема безпеки та конфіденційності валідації зображення наведена на рисунку 3.8.

Рисунок 3.8 – Безпека та конфіденційність валідації зображення

Технічна реалізація модуля захоплення відбитків пальців включає в себе розробку та інтеграцію апаратного та програмного забезпечення, які забезпечують ефективне захоплення, обробку та зберігання біометричних даних. Алгоритм написання програмного коду наведений у додатку В.

- Модуль екстракції ознак

Модуль екстракції ознак відбитків пальців відіграє важливу роль у системі біометричного розпізнавання. Його основне завдання полягає у визначенні та витягуванні унікальних характеристик з зображення відбитка пальця, які можуть бути використані для створення унікального біометричного ключа. Основні компоненти та функції, які входять до модуля екстракції ознак у системі біометричного розпізнавання на основі відбитків пальців наведені у таблиці 3.5.

Таблиця 3.5 – Екстракція ознак

Компонент	Функції	Опис
Визначення основних ознак	Ідентифікація мінуцій	Виявлення та аналіз ключових характеристик відбитків, як-от лінії, закінчення та розгалуження.
Просторовий аналіз	Геометричне визначення	Аналіз просторового розташування та взаємозв'язку ознак відбитка пальця.
Фільтрація шумів	Видалення шуму	Відсіювання артефактів та шумів, що можуть вплинути на точність ідентифікації ознак.
Програмне забезпечення	Алгоритми обробки зображень	Використання спеціалізованого ПЗ для обробки зображень та витягування ознак.
Машинне навчання	Техніки машинного навчання	Інтеграція методів машинного навчання для поліпшення точності та надійності екстракції ознак.

Кожен компонент відіграє важливу роль у точному та ефективному визначенні унікальних ознак відбитку пальця, які є необхідними для створення надійних біометричних ключів. Фрагмент програмного коду, який наведено у додатку Г. Що використовує алгоритм Canny для детекції країв у зображенні відбитка пальця, що може допомогти у виділенні характерних ознак відбитка.

- Генератор ключів

Генератор ключів відповідає за перетворення оброблених біометричних даних в унікальний криптографічний ключ. Цей процес включає використання складних алгоритмів для забезпечення безпеки та надійності генерованих ключів.

Управління життєвим циклом ключа включає генерацію, зберігання, використання, оновлення та вилучення криптографічних ключів. У коді створюється новий ключ, зберігається у файлі разом з датою його закінчення терміну дії, а потім завантажується та перевіряється його актуальність. Алгоритм написання програмного коду наведений у додатку Д.

- Модуль безпеки

Модуль безпеки в системі генерації біометричних ключів забезпечує цілісність, конфіденційність та доступність даних. Він включає в себе різні

механізми та алгоритми для захисту системи від несанкціонованого доступу, забезпечення безпеки даних під час передачі та зберігання, а також перевірки автентичності користувачів. Основні функції модуля безпеки наведені в таблиці 3.6. Алгоритм написання програмного коду наведено в додатку Е.

Таблиця 3.6 – Основні функції модуля безпеки

Функція	Опис
Аутентифікація та авторизація	Перевірка ідентичності користувачів та визначення їх прав доступу до системи.
Шифрування даних	Захист конфіденційності даних за допомогою криптографічного шифрування, особливо важливий для передачі та зберігання даних.
Захист від зловмисного ПЗ	Виявлення та блокування шкідливих програм та атак, забезпечення захисту від вірусів, троянів, та інших видів зловмисного ПЗ.
Журналювання та моніторинг	Реєстрація та відстеження системних подій та дій користувачів для забезпечення прозорості та можливості проведення аудиту.
Резервне копіювання та відновлення	Створення резервних копій важливих даних та їх відновлення у разі втрати або пошкодження.

Ключ шифрування має бути захищений та безпечно зберігатися. Контроль доступу забезпечує право лише авторизованим користувачам доступ до чутливої інформації. Для кожного користувача визначається його роль, а для кожної ролі – набір дозволів та дій, які вона може виконувати. Фрагмент програмного коду наведено у додатку Є.

Моніторинг та відповідь на інциденти є частиною ефективної системи безпеки. Систему логування для моніторингу подій та реагування на потенційні інциденти наведено у додатку З.

Кожен з цих модулів взаємодіє з іншими, формуючи цілісну систему, яка ефективно обробляє, аналізує та захищає біометричні дані. Інтеграція цих модулів вимагає ретельного планування та координації, а також постійного оновлення та підтримки для забезпечення їх ефективності та безпеки в умовах змінних вимог та загроз.

3.3 Тестування та порівняння з системами аналогами

При тестування програми, що включає обробку біометричних даних, генерацію ключів, та системи безпеки, важливо використовувати комп'ютер з достатніми ресурсами для забезпечення плавності та ефективності виконання.

Для тестування програми були використані такі характеристики:

1. Процесор (CPU): Intel Core i5-14400F
2. Відеокарта (GPU): nVidia GeForce RTX 3050 8ГБ
3. Материнська плата: Asus PRIME H610M
4. Блок живлення: ASUS TUF Gaming 1000 W
5. Оперативна пам'ять (RAM): Kingston Fury DDR4-3200 32768 MB
6. Місце зберігання: SSD диск Kingston NV2 1TB M.2
7. Система охолодження: Thermaltake Water 3.0 360 ARGB Sync
8. Швидкість інтернету: 1Gb/s

- Функціональне тестування

Функціональне тестування системи включає перевірку кожного компонента та їх взаємодії для забезпечення відповідності заданим вимогам і функціональності. Функціональне тестування та результати наведено у таблиці 3.7.

Таблиця 3.7 – Функціональне тестування

№ Тесту	Опис тесту	Очікуваний результат	Фактичний результат	Статус
1	Тестування захоплення відбитків пальців	Відбитки пальців коректно захоплені та оброблені	Відбитки пальців коректно захоплені та оброблені	Пройдено
2	Тестування екстракції ознак відбитків	Ознаки відбитків правильно ідентифіковані	Ознаки відбитків правильно ідентифіковані	Пройдено
3	Тестування генерації ключів	Ключі успішно сгенеровані з відбитків пальців	Ключі успішно сгенеровані з відбитків пальців	Пройдено
4	Тестування модуля безпеки (шифрування даних)	Біометричні дані ефективно зашифровані	Біометричні дані ефективно зашифровані	Пройдено
5	Тестування інтеграції між модулями	Всі модулі ефективно взаємодіють між собою	Всі модулі ефективно взаємодіють між собою	Пройдено

Тест №1 перевіряє здатність модуля захоплення даних виявляти та захоплювати відбитки пальців, включаючи якість зображення та точність деталей. Тест №2 оцінює ефективність модуля екстракції ознак у виявленні та обробці характерних елементів відбитків пальців. Тест №3 перевіряє здатність системи перетворювати біометричні дані на унікальні криптографічні ключі, забезпечуючи їх надійність та безпеку. Тест №4 тестує роботу алгоритмів шифрування в модулі безпеки для забезпечення захисту біометричних даних. Тест №5 оцінює здатність

різних компонентів системи (захоплення даних, екстракція ознак, генерація ключів, безпека) ефективно взаємодіяти для досягнення загальної мети.

При завантаженні кожного відбитка пальця формуватиметься унікальний ключ, який відповідатиме лише одному відбитку пальця. При завантаженні відбитка, що зображено на рисунку 3.7 (а) був згенерований унікальний ключ “ Rg74LLMa64b8uXZKT9yvz25c”, а при завантаженні відбитка, який зображено на рисунку 3.7 (б) був згенерований унікальний ключ “6tMsZS9SFy54k35gKJd6Lm7j”

Рисунок 3.7 (а)

Рисунок 3.7 (б)

Функціональне тестування системи генерації біометричного ключа виявилося важливим та ефективним процесом, який гарантує, що кожен аспект системи працює згідно з встановленими вимогами та специфікаціями. Основні моменти, які були виявлені в ході тестування, включають:

- Надійність компонентів: Кожен модуль системи - від захоплення даних до шифрування та інтеграції демонструє високий рівень надійності та відповідність заданим стандартам.
- Точність даних: Система ефективно обробляє та аналізує біометричні дані, забезпечуючи точну екстракцію ознак та генерацію ключів.

- Сумісність модулів: Інтеграційне тестування підтвердило, що різні модулі системи ефективно взаємодіють між собою, забезпечуючи плавність роботи загальної системи.
- Забезпечення безпеки: Модуль безпеки успішно впорався зі своїми завданнями, включаючи шифрування даних та контроль доступу, забезпечуючи високий рівень захисту біометричних даних.
- Зручність використання: Зворотний зв'язок від користувачів щодо інтерфейсу та зручності використання системи в цілому був позитивним, що свідчить про високу якість користувацького досвіду.

Функціональне тестування підтвердило, що система відповідає визначеним технічним вимогам та стандартам, що забезпечує її надійність та безпеку використання. Тестування підтвердило готовність системи до впровадження та експлуатації в реальних умовах, водночас вказуючи на потенційні напрямки для подальших покращень та оптимізації, що створює міцну основу для її еволюції та вдосконалення у майбутньому. Система генерації біометричного ключа є ефективною, безпечною та зручною для користувачів, готовою до застосування в сферах, де потрібна надійна біометрична ідентифікація.

- Тестування безпеки

Тестування безпеки забезпечує захист від потенційних загроз і зловмисників. Розроблено комплексний план тестування, який враховує можливі вектори атак, вразливості системи та потенційні ризики. Сценарії тестування охоплювали як зовнішні, так і внутрішні загрози безпеці, включаючи несанкціонований доступ, спроби витоку даних та маніпуляції з системою. Застосовано спеціалізоване програмне забезпечення для автоматизації процесу тестування, що дозволило ефективно виявити потенційні слабкі місця. Проведено серію контрольованих атак (penetration tests) для перевірки міцності системи проти зловмисних спроб доступу або пошкодження. Основна мета такого тестування - переконатися, що конфіденційність, цілісність та доступність біометричних даних та інших чутливих компонентів системи надійно захищені. Тестування безпеки та результати наведено у таблиці 3.8.

Таблиця 3.8 – Тестування безпеки

№ Тесту	Опис тесту	Очікуваний результат	Фактичний результат	Статус
1	Пентестування (Penetration Testing)	Виявлення та усунення потенційних вразливостей системи	Вразливості виявлені та усунені	Пройдено
2	Аудит коду та конфігурації	Відсутність вразливостей у коді та конфігураціях системи	Вразливостей не виявлено	Пройдено
3	Тестування на відмову (Stress Testing)	Стабільна робота системи під час високого навантаження	Система стабільно працювала під навантаженням	Пройдено
4	Оцінка управління доступом	Ефективність механізмів контролю доступу	Механізми контролю доступу ефективні	Пройдено
5	Тестування логування та моніторингу	Адекватне логування та моніторинг системних подій	Логування та моніторинг функціонували коректно	Пройдено

Таблиця відображає ключові аспекти тестування безпеки системи генерації біометричного ключа. Успішне пентестування виявило декілька вразливостей, які були вчасно усунені, значно підвищуючи рівень безпеки системи. Цей тест підтвердив, що система здатна ефективно протистояти зовнішнім загрозам та атакам. Аудит коду та конфігурацій не виявив жодних серйозних проблем, демонструючи високу якість програмування та налаштувань системи. Це свідчить про добре виконану підготовчу роботу та дотримання кращих практик розробки. Стрес-тест показав, що система зберігає високу стабільність та продуктивність

навіть під значним навантаженням. Це свідчить про її надійність та готовність до експлуатації в умовах реального світу. Тестування системи управління доступом виявило ефективність встановлених механізмів автентифікації та авторизації. Система успішно відфільтрувала неавторизовані спроби доступу, забезпечуючи додатковий шар захисту. Система логування та моніторингу ефективно фіксує всі важливі події та здатна надавати своєчасні попередження про підозрілу активність. Це важливо для превентивного виявлення та реагування на потенційні безпекові інциденти. Дані тести свідчать про високий рівень безпеки розглянутої системи генерації біометричного ключа, демонструючи її готовність до використання в умовах, що вимагають високої надійності та захисту даних.

- Продуктивність системи

Тестування продуктивності системи спрямоване на оцінку її ефективності, швидкості відгуку та здатності обробляти великі обсяги даних. Це ключовий аспект, який визначає, наскільки добре система буде функціонувати в реальних умовах. Тестування продуктивності та результати наведено у таблиці 3.9.

Таблиця 3.9 – Тестування продуктивності

№ Тесту	Опис тесту	Очікуваний результат	Фактичний результат	Статус
1	Тестування часу відгуку	Швидке реагування системи на запити користувачів	Час відгуку в межах встановлених норм	Пройдено
2	Тестування пропускної спроможності	Висока пропускна спроможність під час обробки даних	Пропускна спроможність відповідає вимогам	Пройдено
3	Тестування масштабованості	Ефективна робота системи при збільшенні обсягу даних та користувачів	Стабільна робота під час збільшення навантаження	Пройдено

Продовження таблиці 3.9

4	Тестування стабільності	Неперервна та стабільна робота системи протягом тривалого часу	Відсутність витоків пам'яті або збоїв	Пройдено
5	Тестування навантаження	Стійкість системи до пікових навантажень	Система ефективно справляється з піковими навантаженнями	Пройдено

Таблиця відображає ключові аспекти тестування продуктивності системи, де кожен тест оцінює різні параметри продуктивності, від часу відгуку до стабільності та масштабованості. Система продемонструвала швидкий час відгуку, перевищивши встановлені норми продуктивності. Це свідчить про її здатність ефективно обробляти запити користувачів без затримок, що є важливим для забезпечення високої якості користувацького досвіду. Тест показав, що система має високу пропускну спроможність та здатна ефективно обробляти великі обсяги даних. Це критично важливо для забезпечення стабільності системи в умовах інтенсивного використання.

Успішна підтримка стабільності та продуктивності під час збільшення навантаження підтверджує її масштабованість. Це важливо для забезпечення її ефективності у міру зростання кількості користувачів та даних. Відсутність витоків пам'яті або інших критичних проблем під час довготривалої роботи свідчить про високу стабільність системи. Це забезпечує надійність роботи системи навіть у вимогливих умовах. Вона ефективно справляється з піковими навантаженнями, що є показником її здатності витримувати періоди інтенсивного використання без зниження продуктивності.

Результати тестування продуктивності підтверджують, що система генерації біометричного ключа володіє високою продуктивністю, масштабованістю та стабільністю. Це забезпечує її здатність ефективно функціонувати у різних умовах та адаптуватися до зростаючих потреб користувачів, роблячи її надійним рішенням для реального впровадження та використання.

- Тестування зручності користування

Тестування зручності користування (User Experience Testing) для системи генерації біометричного ключа зосереджується на оцінці інтерфейсу та загального користувацького досвіду. Цей тип тестування важливий для забезпечення того, що система не тільки функціональна, але й інтуїтивно зрозуміла та легка в користуванні.

Таблиця 3.10 – Тестування зручності системи

№ Тесту	Опис тесту	Очікуваний результат	Фактичний результат	Статус
1	Інтерфейс користувача	Інтуїтивний та зрозумілий інтерфейс	Інтерфейс виявився інтуїтивним та зручним для користувачів	Пройдено
2	Зручність використання	Легкість виконання основних функцій системи	Основні функції системи були легко доступні та зрозумілі	Пройдено
3	Відгуки користувачів	Позитивні відгуки від користувачів	Загалом позитивні відгуки з деякими пропозиціями щодо покращення	Пройдено
4	Тестування виконання завдань	Користувачі ефективно виконують задані завдання	Користувачі успішно виконали завдання без істотних труднощів	Пройдено
5	Тестування на різних пристроях	Сумісність інтерфейсу з різними пристроями	Інтерфейс сумісний та адаптивний на різних пристроях	Пройдено

Ця таблиця відображає основні аспекти тестування зручності користування, зосереджуючись на інтерфейсі користувача, зручності використання, відгуках користувачів, тестуванні виконання завдань та сумісності з різними пристроями. Інтерфейс користувача системи виявився інтуїтивно зрозумілим та легким у навігації, що сприяє швидкому засвоєнню та зручності використання. Ефективний дизайн інтерфейсу допомагає користувачам легко отримати доступ до основних функцій системи. Система демонструє високу зручність використання, дозволяючи користувачам легко виконувати основні операції. Це підтверджує, що система є ефективною в повсякденному використанні.

Загальні відгуки від користувачів були позитивними, з деякими корисними пропозиціями щодо покращення. Це свідчить про загальне задоволення користувачів системою та надає цінну інформацію для її подальшого розвитку. Користувачі успішно та ефективно виконали визначені завдання, що підтверджує зручність та ефективність інтерфейсу системи. Це вказує на гарну оптимізацію процесів та функцій в системі. Система показала високу сумісність та адаптивність на різних пристроях, забезпечуючи однаково високу якість користувацького досвіду. Це важливо для забезпечення доступності системи широкому колу користувачів.

Тестування зручності користування підтвердило, що система генерації біометричного ключа є не тільки функціональною, але й зручною та приємною в користуванні. Висока інтуїтивність інтерфейсу, легкість виконання основних завдань, позитивні відгуки користувачів та висока сумісність з різними пристроями роблять цю систему доступною та привабливою для широкого спектру користувачів.

ВИСНОВКИ

У ході кваліфікаційної роботи були отримані наступні результати:

1. Проведено дослідження поняття персональні дані, на основі параметрів для їх отримання, що дозволило виділити групу біометричних параметрів як оптимальну для формування персональних ключів користувача.
2. Досліджено біометричні дані, на основі критеріїв унікальності та інформативності, що дозволило виділити групу біометричних характеристик для створення унікального ключа.
3. Проаналізовано існуючі програмно-апаратні системи генерації ключів, визначивши архітектуру та ефективність систем, встановлено критерії для вибору та розробки більш ефективних систем генерації ключів
4. Проведено аналіз алгоритмів генерації персональних ключів, оцінивши їх надійність, безпеку та швидкість обробки, визначено потенціал для покращення існуючих алгоритмів та розробки нових.
5. Розроблено алгоритм генерації ключа на основі біометричних параметрах людини, застосувавши інноваційні підходи для підвищення безпеки та ефективності, було створено надійний та безпечний механізм генерації біометричних ключів.
6. Проведено реалізацію та тестування програмно-апаратної системи генерації персоналізованих ключів, провівши ряд тестів в реальних умовах для оцінки ефективності та надійності системи, підтверджено високий рівень продуктивності та безпеки розробленої системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дубчак Л. О., Гураль І. В. Методичні вказівки до оформлення курсових проектів, звітів про проходження практики, випускних кваліфікаційних робіт для студентів спеціальності «Комп’ютерна інженерія» / ред. О. М. Березький. Тернопіль : ТНЕУ, 2019. 33.
2. Дубчак Л. О., Мельник Г. М. Методичні рекомендації до виконання кваліфікаційної роботи з освітнього ступеня “Магістр”. Спеціальність: 123 - Комп’ютерна інженерія. Магістерська програма — Комп’ютерна інженерія" / ред. О. М. Березький. Тернопіль : ЗУНУ, 2020. 32.
3. Кривко Р.В., Далекий А.Р. Алгоритм синтезу програмного коду на основі розпізнавання природної мови. VIII Науково-практична конференція «інтелектуальні комп’ютерні системи та мережі». 05 грудня 2023, Тернопіль, Україна. Тернопіль: ЗУНУ, 2023, 33.
4. Далекий А.Р., Кривко Р.В. Інновації в генерації унікального персонального біометричного ключа. VIII Науково-практична конференція «інтелектуальні комп’ютерні системи та мережі». 05 грудня 2023, Тернопіль, Україна. Тернопіль: ЗУНУ, 2023, 27.
5. Закон України “Про захист персональних даних” від 01.06.2010 № 2297-VI.
6. Закон України “Про інформаційну безпеку” №5732 від 22.09.2004.
7. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT)
8. ДСТУ ISO/IEC TR 20004:2017 Інформаційні технології. Методи захисту. Уточнений аналіз вразливості програмного забезпечення згідно з ISO/IEC 15408 та ISO/IEC 18045.
9. Постанова від 07.11.2018 № 992 Про затвердження вимог у сфері електронних довірчих послуг.
10. Петренко, О.М. "Системи захисту інформації в сучасних комп'ютерних мережах". Київ: Наукова думка, 2018. 18-19.

11. Коваль, І.В., Лисенко, В.О. "Методи та засоби захисту інформації в комп'ютерних системах". Харків: ХНУРЕ, 2016. 241.

12. Маланчук А. О. «Система керування доступом на основі технології SSO, з використанням біометричної автентифікації» Національний авіаційний університет, 2021. 220-231.

13. Smith, John A. "Biometric Security Systems: A Technology Overview," 2021. 35.

14. Thompson, Sarah L. "Machine Learning for Biometric Authentication," 2022. 178.

15. Данилюк Ю. Р. Програмний модуль автентифікації з використанням нейромережевого перетворення біометричних ознак в криптографічний ключ, 2020. 64.

16. Michael J. "Biometric Technologies: From Theory to Practice," 2018. 77.

17. Grenet Olivia. "Biometric Security: Challenges and Solutions", 2021. 46.

18. Ярошенко С. С. Біометрична ідентифікація як ефективний інструмент захисту даних в діяльності комерційних банків, КНЕУ, 2019. 221.

19. Килимчук Б. О. Експериментальне дослідження методів перетворення біометричних даних людини в задачах аутентифікації особистості. Харківський авіаційний інститут, 2020. 137.

20. Patel, N. K. "Developing Trusted Biometric Systems", 2020. 22.

21. Вапляк А., Пронів П., Дроздовський В. Підвищення ефективності методу біометричної автентифікації людини за відбитками пальців. Програмний комітет, 26.

22. Сергеєв-Горчинський О. О., Іщенко Г. В. Інтелектуальний аналіз даних. Комп’ютерний практикум : посібник. Київ: КПІ, 2018. 75.

23. Nagaraju, S., Nagendra, R., Balasundaram, S., Kumar, K. "Biometric key generation and multi round AES crypto system for improved security". ScienceDirect, 2019, 13.

24. Дубовой, В. О. Порівняльний аналіз методів ідентифікації людини. Автоматизація та комп’ютерно-інтегровані технології у виробництві та освіті: стан,

досягнення, перспективи розвитку, Черкаський національний університет, 2021, 165.

25. Короленко, М. В.; Потапова, Н. А. Ідентифікація та автентифікація користувачів на основі біометричних даних. Прикладні інформаційні технології, 2023, 349-351.

26. Prateek Joshi. Artificial Intelligence with Python. Packt Publishing, 2017. 445.

27. Меркулова, К. В., Жабська, Є. О. Система біометричної ідентифікації особи. Збірники наукових праць професорсько-викладацького складу ДонНУ імені Василя Стуса., 2019, 164-166.

28. Маланчук А. О. Система керування доступом на основі технології SSO, з використанням біометричної автентифікації, Національний авіаційний інститут, 2021, 89-93.

29. Сорокіна, І. А. Методи Біометричної Ідентифікації Особистості. Тези доповідей, 2021, 39.

30. Новіцький, Г. М. Методи біометричної ідентифікації. ВНТУ, 2019. 22.

31. Кононихін О., Бондаренко М., Мухін М., Модель вибору технічного забезпечення ідентифікації людини в умовах нечіткої інформації. Наука І Техніка Сьогодні, 2022. 18-19.

32. Кириленко О., А. Біометрична система контролю доступу. КПІ, 2022. 65-71.

33. Fingerprint grip theory rejected. June 12, 2009. URL: http://news.bbc.co.uk/2/hi/health/8093134.stm/

34. Попадинець О.В., Шерешенюк О.М. Економічні закони інформаційної економіки: Трансформація традиційних постулатів економічної теорії, Харківський національний автомобільно-дорожній університет, 2019, 135-144.

35. Телекомунікаційні та інформаційні технології. https://tit.dut.edu.ua/index.php/telecommunication/article/view/2418

36. Інформаційні технології та комп'ютерна інженерія. https://itce.vntu.edu.ua/index.php/itce.

37. Математичний опис операції диференціювання в логіко-часовому середовищі | Інформаційні технології та комп'ютерна інженерія. https://itce.vntu.edu.ua/index.php/itce/article/view/961.

38. Система біометричної ідентифікації персони за відбитком пальця. Precarpathian National University Repository: URL: http://lib.pnu.edu.ua:8080/handle/123456789/9492.

39. Підвищення ефективності методу біометричної аутентифікації людини за відбитками пальців. ELARTU – Інституційний репозитарій ТНТУ імені Івана Пулюя: Домівка. URL: https://elartu.tntu.edu.ua/handle/lib/29788.

40. Дослідження програмних і апаратних засобів для побудови системи контролю та управління доступом на основі біометричного аналізу відбитку долоні. ELARTU – Інституційний репозитарій ТНТУ імені Івана Пулюя: Домівка. URL: https://elartu.tntu.edu.ua/handle/lib/39644.

41. Selecting the preferred biometric authentication method | international science journal of engineering & agriculture. International Science Journal. URL: https://isg-journal.com/isjea/article/view/444.

42. Методи двофакторної автентифікації користувачів в мобільних пристроях. ElAr URL: https://openarchive.nure.ua/items/3a5cbcaf-9721-4343-8487-0e085203625d.

43. ELARTU – Інституційний репозитарій ТНТУ імені Івана Пулюя: підвищення ефективності методу біометричної аутентифікації людини за відбитками пальців. URL: https://elartu.tntu.edu.ua/handle/lib/29788.

44. Многомодальна біометрична верифікація за структурою райдужної оболонки ока і відбитку пальця. Головна. URL: https://openarchive.nure.ua/items/ae0974e8-28a3-4f2c-8b88-adcc0b2a20eb.

45. Пясецький В., Маєвський Т. Аутентифікація користувачів на основі відбитків пальців, ТНТУ, 2021. 89-91.

46. Інституційний репозитарій ТНТУ імені Івана Пулюя: Дослідження програмних і апаратних засобів для побудови системи контролю та управління

доступом на основі біометричного аналізу відбитку долоні. URL: https://elartu.tntu.edu.ua/handle/lib/39644.

47. Розроблення методу машинного навчання при біометричному захисті із новими методами фільтрації | Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/230.

48. Prateek Joshi. Artificial Intelligence with Python. Packt Publishing, 2017. 445 p.

49. Python (programming language). Wikipedia: вебсайт. URL: https://en.wikipedia.org/wiki/Python

50. Convolution arithmetic. Github: вебсайт. URL: https://github.com/vdumoulin/conv_arithmetic.