Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інформаційних радіотехнологій і технічного захисту інформації*

Кафедра *Комп'ютерної інженерії та систем технічного захисту інформації*

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти *другий (магістерський)*

Методи захисту інформації
в системах електронного документообігу

Виконав:
студент *2* курсу, групи *СТЗІАм-22-1*
Федотов Віталій Васильович

Спеціальність *125 «Кібербезпека»*

Тип програми *освітньо-професійна*

Освітня програма *«Системи технічного захисту інформації, автоматизація її обробки»*

Керівник *доц. Горелов Д.Ю.*

Допускається до захисту
Зав. кафедри _____ *проф. Антіпов І.Є.*
(підпис)

2024 р.

Харківський національний університет радіоелектроніки

Факультет *Інформаційних радіотехнологій і технічного захисту інформації*
Кафедра *Комп'ютерної інженерії та систем технічного захисту інформації*
Рівень вищої освіти *другий (магістерський)*
Спеціальність *125 «Кібербезпека»*
Тип програми *освітньо-професійна*
Освітня програма *«Системи технічного захисту інформації, автоматизація її обробки»*

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«___» _____ 20 _____ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Федотову Віталію Васильовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Методи захисту інформації в системах електронного документообігу*

затверджена наказом по університету від « 03 » 11 2023 р. № 1281 Ст
2. Термін подання студентом роботи до екзаменаційної комісії *10 січня 2024 р.*
3. Вихідні дані до роботи *Системи захищеного електронного, змішаного та гібридного документообігу. Дослідна схема «зв'язування» секретних ключів з біометричними параметрами користувача: нечіткий екстрактор. Дослідні інформативні ознаки клавіатурного почерку: монографи (часові характеристики поодиноких подій клавіатури)*
4. Перелік питань, що потрібно опрацювати в роботі *Дослідити можливість використання клавіатурного почерку в задачах підвищення інформаційної захищеності систем документообігу на основі біометричних технологій. Для досягнення поставленої мети необхідно розв'язати наступні задачі: 1) дослідити концепцію системи захисту змішаного документообігу, що використовує засоби електронного підпису з біометричною активацією без використання спеціального обладнання та біометричних сканерів; 2) запропонувати модель перетворювача біометрія-код, орієнтованого на обробку параметрів клавіатурного почерку; 3) запропонувати алгоритм створення та перевірки електронного підпису з біометричною активацією для документів на електронних та паперових носіях.*

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

1. Мета та задачі кваліфікаційної роботи. А4. Ел.ф.

2. Труднощі виконання вимог «рівного захисту» документів на електронних та паперових носіях. А4. Ел.ф.

3. Схема маршруту документу в гібридному документообігу. А4. Ел.ф.

4. Структурна схема системи захищеного гібридного документообігу. А4. Ел.ф.

5. Перетворювачі біометрія-код. А4. Ел.ф.

6. Типова схема нечіткого екстрактору. А4. Ел.ф.

7. Пропонована схема нечіткого екстрактору. А4. Ел.ф.

8. Схема експерименту. А4. Ел.ф.

9. Результати проведених досліджень. А4. Ел.ф.

10. Висновки. А4. Ел.ф.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Аналіз проблеми побудови систем захищеного документообігу*	*01.09.23 – 20.09.23*	
2	*Аналіз сучасних методів та алгоритмів побудови перетворювачів біометрія-код*	*21.09.23 – 31.10.23*	
3	*Проведення експериментальних досліджень*	*01.11.23 – 31.12.23*	
4	*Перевірка роботи на антиплагіат*	*03.01.24 – 05.01.24*	
5	*Представлення кваліфікаційної роботи на кафедрі*	*10.01.2024*	

Дата видачі завдання *02 вересня 2023 р.*

Студент _____
(підпис)

Керівник роботи _____ _____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 102 с., 22 рис., 7 табл., 41 джерел, 1 додаток.

НЕЧІТКИЙ ЕКСТРАКТОР, ЗАВАДОСТІЙКЕ КОДУВАННЯ, БІОМЕТРИЧНА АУТЕНТИФІКАЦІЯ, КЛАВІАТУРНИЙ ПОЧЕРК.

Метою роботи є підвищення інформаційної захищеності систем документообігу на основі біометричних технологій.

Запропоновано декілька варіацій нечітких екстракторів для генерації криптографічних ключів та паролів на основі параметрів клавіатурного почерку. Проведено серію обчислювальних експериментів з оцінки ефективності запропонованих методик, визначено оптимальні параметри нечітких екстракторів. Найкращий результат становив: FRR=0.054, FAR=0.018 при довжині ключа 200 біт.

ABSTRACT

Master thesis: 102 p., 7 tables, 22 fig., 41 sources, 1 annex.

FUZZY EXTRACTOR, ERROR CORRECTION CODES, BIOMETRIC AUTHENTICATION, KEYSTROKE.

The objective of the work is to increase the information security of document circulation systems based on biometric technologies.

Several variations of fuzzy extractors are proposed for generating cryptographic keys and passwords based on keyboard handwriting parameters. A series of computational experiments was conducted to evaluate the effectiveness of the proposed methods, and the optimal parameters of fuzzy extractors were determined. The best result was: FRR=0.054, FAR=0.018 with a key length of 200 bits.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ТЕРМІНІВ

EER (Equal Error Rate) – коефіцієнт рівної імовірності помилок 1 і 2-го роду;

FAR (False Acceptance Rate) – помилка другого роду – випадок надання системою доступу неавторизованому користувачеві;

FRR (False Rejection Rate) – помилка першого роду – доступ заборонений користувачеві, зареєстрованому в системі;

OCR (Optical Character Recognition) – оптичне розпізнавання тексту;

ЕП – електронний підпис;

ЖЦ – життєвий цикл;

ЗКЗІ – засоби криптографічного захисту інформації;

ІС – інформаційна система;

КЗ – контрольована зона;

НПБК – нейромережевий перетворювач біометрія-код;

НСД – несанкціонований доступ;

ОРД – організаційно-розпорядчі документи;

ПБК – перетворювач біометрія-код;

ПЗ – програмне забезпечення.

ВСТУП

За останні десятиліття електронні системи формування та керування паперовими документами стали необхідним засобом оснащення офісу будь-якої компанії. Переважна більшість офісних документів сьогодні створюється за допомогою засобів інформаційних технологій. З широким поширенням технології електронно-цифрового підпису стало відбуватися стирання межі між електронними та неелектронними документами. Однак в Україні швидкий перехід найближчим часом на «безпаперові технології» не станеться з кількох причин.

По-перше, в нашій країні існують вимоги законодавства та нормативних актів щодо оформлення найбільш значущих у діловій діяльності документів виключно на папері (статутні документи, ліцензії, кадрове діловодство тощо). Склалася ціла система роботи державних архівів, де висуваються вимоги щодо зберігання паперових документів, які можуть терміново знадобитися у разі різноманітних життєвих ситуацій та надзвичайних подій, коли електронні документи можуть виявитися недоступними. Звичайно, в наш час відбувається впровадження інформаційних технологій у цій системі, але процес переходу виключно на електронні форми документів буде тривалим.

По-друге, більшості сучасних керівників в процесі прийняття рішень зручніше працювати з папером. Ще не виросло покоління управлінців, яке б використовувало електронні засоби комунікацій зі школи.

Тому сьогодні реально можна говорити про перехід від традиційного паперового документообігу не до електронного, а до гібридного документообігу. Ключовим атрибутом електронного документа є електронно-цифровий підпис, який формується на основі секретного (закритого) ключа користувача та хеш-функції документа.

Виданий в центрі сертифікації електронний підпис використовується для того, щоб зберігати юридичну значущість електронних документів, проте

існує проблема передачі цього підпису іншій особі, тобто на відміну від традиційного підпису електронний є відчужуваним від свого власника. При цьому зберігатиметься юридична значимість документів, підписаних електронним підписом сторонньою особою, що в деяких випадках може виявитися неприпустимим. Крім того, в наш час все ще використовуються паперові версії документів, і при перекладі документа з електронного формату до паперового, звичайний електронний підпис втрачає свої захисні функції.

Виходом з подібних ситуації може бути використання біометричних ознак користувача, на основі яких формуватиметься електронний підпис, а також створення для паперової версії документа спеціального аналогу електронного підпису у вигляді штрих-коду.

Метою роботи є підвищення інформаційної захищеності систем документообігу на основі біометричних технологій.

Для досягнення поставленої мети необхідно розв’язати наступні задачі:

1) дослідити концепцію системи захисту змішаного документообігу, що використовує засоби електронного підпису з біометричною активацією без використання спеціального обладнання та біометричних сканерів;

2) запропонувати модель перетворювача біометрія-код, орієнтованого на обробку параметрів клавіатурного почерку;

3) запропонувати алгоритм створення та перевірки електронного підпису з біометричною активацією для документів на електронних та паперових носіях.

1 ПРОБЛЕМА ЗАХИСТУ ДОКУМЕНТІВ В ЕЛЕКТРОННОМУ ДОКУМЕНТООБІГУ

1.1 Нормативно-правове регулювання електронного документообігу в Україні

Електронний документообіг з'явився із поширенням комп'ютерів як більш вигідна економічна й екологічна альтернатива паперовому. У США та країнах ЄС ним активно користуються вже понад десяток років. В Україні ж електронний документообіг набирає популярності лише зараз, стаючи must have для бізнесу, а судячи з тенденцій, які ми спостерігаємо останні кілька років: курс на всеохопну диджиталізацію, держава у смартфоні, – і для держави також.

Існують кілька визначень терміну «документ», зокрема, в ДСТУ 2732:2004 «Діловодство й архівна справа. Терміни та визначення понять» [1]: «Документ – інформація, зафіксована на матеріальному носії, основною функцією якого є зберігати та передавати її в часі та просторі». Також в стандарті визначено поняття «підпису» – реквізиту документа, який свідчить про відповідальність особи за його зміст та є єдиний чи один з реквізитів, що надають документові юридичної сили.

Останній термін за змістом повністю збігається з поняттям «автограф», тобто мається на увазі рукописний відкритий біометричний образ. Крім відкритих образів, існують секретні (таємні) образи – рукописні паролі. Далі в кваліфікаційній роботі термінами « підпис» або «рукописний образ» буде позначатись сукупність кількох рукописних символів або слів, які відтворюються рукою підписувача, а також всі дані про цей процес, що реєструється з використанням пристрою введення. Терміни «автограф» та «рукописний пароль» будуть використовуватись для позначення відкритого та таємного рукописного образу відповідно.

Основні організаційно-правові засади електронного документообігу та

використання електронних документів передбачені Законом України «Про електронні документи та електронний документообіг», де, зокрема вводяться наступні поняття [2]:

1) адресат – фізична або юридична особа, якій адресується електронний документ;

2) дані – інформація, яка подана у формі, придатній для її оброблення електронними засобами;

3) посередник – фізична або юридична особа, яка в установленому законодавством порядку здійснює приймання, передавання (доставку), зберігання, перевірку цілісності електронних документів для задоволення власних потреб або надає відповідні послуги за дорученням інших суб’єктів електронного документообігу;

4) обов’язковий реквізит електронного документа – обов’язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили;

5) автор електронного документа – фізична або юридична особа, яка створила електронний документ;

6) суб’єкти електронного документообігу – автор, підписувач, адресат та посередник, які набувають передбачених законом або договором прав і обов’язків у процесі електронного документообігу.

У зв'язку з простотою створення копій електронних документів слід розглянути поняття «реалізації електронного документа», тобто елемента деякої множини, що представляє електронний документ, який існує або який може існувати в частині електронного чи цифрового середовища. У електронного документа може існувати безліч еквівалентних реалізацій, що мають юридичну силу. Для документів багаторазової дії (закони, керівні документи, накази тощо) досить довести існування безлічі його реалізацій, що можливо на основі єдиної, що має відповідні атрибути. Для документів одноразової або кратної дії (квитки, абонементи тощо) необхідно додатково гарантувати кратність застосування. Наприклад, обмежити термін дії документа або відс-

тежувати кратність реєстрації його реалізацій протягом терміну його дії [3].

Електронний документ визнається рівнозначним документу на паперовому носії, якщо його підписано електронним підписом або іншим аналогом власноручного підпису. В законі України «Про електронні довірчі послуги» [4] дано визначення цього терміну: електронний підпис (ЕП) – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов’язуються і використовуються ним як підпис. Також в цьому окремо виділені:

1) кваліфікований електронний підпис – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа;

2) удосконалений електронний підпис – електронний підпис, створений за результатом криптографічного перетворення електронних даних, з якими пов’язаний цей електронний підпис, з використанням засобу удосконаленого електронного підпису та особистого ключа, однозначно пов’язаного з підписувачем, і який дає змогу здійснити електронну ідентифікацію підписувача та виявити порушення цілісності електронних даних, з якими пов’язаний цей електронний підпис.

Наведемо інші важливі визначення, що стосуються електронного підпису [4]:

1) аутентифікація – електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних;

2) відкритий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;

3) електронна довірча послуга – послуга, яка надається для забезпечення електронної взаємодії двох або більше суб’єктів, які довіряють надавачу

електронних довірчих послуг щодо надання такої послуги;

4) електронна ідентифікація – процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи;

5) електронна позначка часу – електронні дані, які пов’язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу;

6) засвідчення чинності відкритого ключа – процедура формування сертифіката відкритого ключа;

7) засіб електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які використовуються для створення та/або перевірки електронного підпису чи печатки;

8) засіб електронної ідентифікації – носій інформації, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг;

9) засіб кваліфікованого електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки;

10) засіб удосконаленого електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення удосконаленого електронного підпису чи печатки, та/або перевірки удосконаленого електронного підпису чи печатки, та/або зберігання особистого ключа удосконаленого електронного підпису чи печатки;

11) ідентифікаційні дані особи – унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи;

12) ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи;

13) кваліфікований сертифікат відкритого ключа – сертифікат відкритого ключа, який видається кваліфікованим надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом;

14) компрометація особистого ключа – будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа;

15) особистий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;

16) пара ключів – особистий та відповідний йому відкритий ключі, що є взаємопов’язаними параметрами алгоритму асиметричного криптографічного перетворення;

17) реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів – електронна база даних, в якій містяться відомості про сертифікати відкритих ключів, сформовані надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом, їх статус та списки відкликаних сертифікатів відкритих ключів;

18) самопідписаний сертифікат відкритого ключа – сертифікат відкритого ключа, який формується центральним засвідчувальним органом або засвідчувальним центром з використанням особистого ключа центрального засвідчувального органу або засвідчувального центру;

19) сертифікат відкритого ключа – електронний документ, який засвідчує належність відкритого ключа фізичній або юридичній особі, підтверджує її ідентифікаційні дані та/або надає можливість здійснити автентифікацію веб-сайту;

20) скасування сертифіката відкритого ключа – зупинення чинності сертифіката відкритого ключа.

Незважаючи на очевидні переваги електронного документообігу, наразі з багатьох причин (існують вимоги законодавства щодо оформлення найбільш значущих документів на папері, більшості керівників при прийнятті юридично важливих рішень зручніше працювати з папером) майже в будь-якій організації в тому чи іншому вигляді реалізується змішаний документообіг.

1.2. Загрози безпеці інформації обмеженого доступу та способи протидії ним у системах змішаного документообігу

Документ у будь-якій формі його подання на будь-якому етапі його життєвого циклу (ЖЦ) схильний до загроз інформаційної безпеки, тому необхідно своєчасно ідентифікувати їх джерела.

Як правило, початковим базисом класифікації зловмисників є їх розташування щодо середовища обігу документів, тобто. наявність у них прав доступу та можливостей доступу до інформації та (або) до компонентів інформаційної системи:

1) зовнішні зловмисники – особи, які не мають права доступу до інформаційної системи, її окремих компонентів та реалізують загрози безпеці інформації з-за кордонів інформаційної системи;

2) внутрішні зловмисники – особи, які мають право постійного чи разового доступу до інформаційної системи, її окремих компонентів;

При цьому важливо враховувати, що, як правило, останні мають найбільші можливості при реалізації загроз, зовнішній зловмисник може діяти спільно з внутрішнім зловмисником, а також у складі групи, реалізація загрози можлива в будь-якій точці інформаційної системи (ІС), в якості точки атаки на всю ІС або її частину порушник вибере найслабшу ланку ІС, за наявності підключення до мережі Інтернет висока ймовірність дії з боку зовнішнього

зловмисника. Дані два види зловмисників з урахуванням зазначених вище факторів поділяються на категорії. Опис кожної категорії порушників інформаційної безпеки, а також способів доступу та наявність повноважень при реалізації загрози наведено у табл. 1.1.

Таблиця1.1 – Категорії порушників інформаційної безпеки [5]

Тип порушника	Спосіб доступу та повноваження доступу до персональних даних
Зовнішній або категорія А	Особи, які не мають санкціонованого доступу до ІС і даних, що захищаються, але мають можливість самостійно планувати і здійснювати атаки, тільки за межами контрольованої зони (КЗ), а також в межах КЗ без фізичного доступу до апаратних елементів ІС
Внутрішній або категорія В	Зареєстровані користувачі ІС, які мають санкціонований доступ до апаратних компонентів ІС, на яких у тому числі реалізовані засоби криптографічного захисту інформації (ЗКЗІ), але не мають доступу до даних, що захищаються. Особи, які здійснюють розробку, постачання, супровід та ремонт технічних засобів ІС
Внутрішній або категорія С	Зареєстровані користувачі ІС, які мають доступ до ресурсів ІС з робочого місця. Зареєстровані користувачі ІС, які здійснюють віддалений доступ до даних, що захищаються за локальними та (або) розподіленими системами. Мають можливість залучати фахівців, які мають досвід розробки та аналізу ЗКЗІ
Внутрішній або категорія Д	Зареєстровані користувачі ІС з повноваженнями системного адміністратора, адміністратора безпеки мережі (сегменту мережі) ІС. Мають можливість залучати фахівців, які мають досвід розробки та аналізу ЗКЗІ
Внутрішній або категорія Е	Програмісти-розробники (постачальники) прикладного програмного забезпечення та особи, які забезпечують його супровід до ІС. Мають можливість залучати фахівців, які мають досвід розробки та аналізу ЗКЗІ

Склад і зміст самих загроз визначається, у тому числі, сукупністю умов і факторів, що створюють небезпеку несанкціонованого (навмисного або випадкового) доступу до відомостей, що захищаються. Обґрунтування актуаль-

ності / неактуальності загроз супроводжується описом організаційно-технічних заходів, що дозволяють нейтралізувати такі загрози. Типова модель загроз для ІС, що мають підключення до мереж загального користування, включає такі класи загроз:

1) загрози витоку інформації з технічних каналів;

2) загрози несанкціонованого доступу (НСД) до даних, оброблюваних на автоматизованому робочому місці, зокрема загрози із зовнішніх мереж.

В табл. 1.2 наведено модель загроз системам змішаного документообігу, в яких виконується обробка відомостей виключно конфіденційного характеру. Оскільки ця модель є абстрактною без прив'язки до конкретної ІС, тому значення ймовірностей реалізації загроз відсутні.

З наведеної моделі можна зробити висновок, що більшість загроз нейтралізується використанням організаційно-розпорядчих документів (ОРД), ознайомленням з ними співробітників організації, розподілом обов'язків по організаційно-технічному забезпеченню системи захисту інформації, і також встановленням спеціальних програмно-технічних засобів, які пройшли сертифікацію відповідно до вимог захисту інформації.

Розробка та використання, а також проведення інструктажів спрямовані у значній частині на нейтралізацію «людського фактору», проте навіть якщо користувач, дотримуючись вказівок парольної політики, вірно згенерує пароль, уникнути такої властивості паролю, як його відчужуваність від користувача, практично неможливо – пароль може бути втрачений, забутий, вкрадений, переданий третій особі тощо, що є найбільшим недоліком цього типу аутентифікації.

Таблиця1.2 – Узагальнена модель загроз змішаному документообігу

<table>
<tr><th>Загроза</th><th>Реалізація загрози</th><th>Заходи захисту</th></tr>
<tr><td colspan="3">1. Загрози витоку інформації з технічних каналів</td></tr>
<tr><td>Витік видової інформації</td><td>Може бути здійснена:
1) за рахунок віддаленого перегляду із засобів відображення інформації; 2) за допомогою прихованих пристроїв відеоспостереження</td><td>Встановлення на вікнах жалюзі або штор.
Розташування засобів відображення конфіденційної інформації з урахуванням запобігання можливому перегляду на них такої інформації, в тому числі за допомогою оптичних засобів</td></tr>
<tr><td colspan="3">2. Загрози НСД до інформації
2.1 Загрози знищення, розкрадання апаратних засобів ІС, носіїв інформації шляхом фізичного доступу до елементів ІС</td></tr>
<tr><td>Крадіжка елементів ІС</td><td rowspan="3">Може бути здійснена:
1) за рахунок виносу користувачами машинних носіїв інформації (МНІ); 2) за рахунок несанкціонованого копіювання інформації на особисті МНІ; 3) за рахунок відправлення конфіденційної інформації мережею Інтернет за допомогою персональних комп'ютерів та смартфонів</td><td rowspan="4">Цілодобова охорона приміщень ІС
Фізична охорона засобів обчислювальної техніки з боку співробітників охорони та співробітників організації
Розробка та використання організаційно-розпорядчих документів (ОРД), що регламентують порядок доступу до приміщень співробітників та сторонніх осіб</td></tr>
<tr><td>Крадіжка носіїв інформації</td></tr>
<tr><td>Крадіжка ключів та атрибутів доступу</td></tr>
<tr><td>Виведення з ладу вузлів мережі, каналів зв'язку</td><td>Може бути здійснена за рахунок НСД до приміщень, де розташовані елементи мережевої інфраструктури та проходять канали зв'язку, з подальшим деструктивним впливом на них</td></tr>
<tr><td>НСД до інформації при технічному обслуговуванні вузлів мережі</td><td>Може бути здійснена: 1) за рахунок НСД до приміщень, де розташовані елементи мережевої інфраструктури та проходять канали зв'язку, з подальшим деструктивним впливом на них; 2) за межами КЗ при технічному обслуговуванні (ремонті) елементів ІС; 3) під час безконтрольного виконання робіт сторонніми організаціями всередині КЗ</td><td>Розробка та використання ОРД, які регламентують порядок доступу до приміщень працівників та сторонніх осіб, а також правила проведення технічного обслуговування елементів ІС, у тому числі при винесенні за межі КЗ</td></tr>
<tr><td>Несанкціонована зміна налаштувань та відключення засобів захисту</td><td>Може бути здійснена: 1) шляхом НСД до приміщень, де розташовані засоби захисту ІС при отриманні зазначеними користувачами прав адміністратора внаслідок ненавмисних дій адміністраторів; 2) навмисне відключення, зміна налаштувань засобів захисту системними адміністраторами, спрямовані на НСД до інформації</td><td>Розробка та використання ОРД роботи з встановленими засобами захисту.
Призначення відповідальних осіб у ІС організації (адміністратора безпеки)</td></tr>
</table>

Продовження таблиці 1.2

Загроза	Реалізація загрози	Заходи захисту
2.2 Загрози розкрадання, несанкціонованої модифікації або блокування інформації за рахунок НСД із застосуванням програмно-апаратних та програмних засобів		
Загрози програмно-математичних впливів	Можуть бути здійснені: 1) у разі деструктивного програмного впливу порушником на деякі програми чи систему загалом шляхом зміни компонентів програмного середовища; 2) за рахунок впровадження програмних компонентів, у тому числі шкідливого ПЗ; 3) при перехопленні даних, що надходять від периферійних пристроїв, 4) при спотворенні коду прикладного та системного ПЗ; 5) при вбудовуванні шкідливого коду в прикладне та системне ПЗ; 6) при використанні вразливостей коду прикладного та системного ПЗ; 7) при відновленні некоректно видалених даних із зовнішніх / внутрішніх носіїв інформації	Встановлення ліцензійного ПЗ. Розробка та використання ОРД щодо організації заходів антивірусного захисту, у тому числі своєчасного оновлення антивірусних баз, а також про правила зберігання та видалення даних із зовнішніх / внутрішніх носіїв інформації. Призначення відповідальних осіб у ІС організації (адміністратора безпеки)
Загроза вбудовування апаратних закладок сторонніми особами, зокрема	Може бути здійснена: 1) за безпосереднього доступу до ресурсів ІС шляхом вбудовування апаратних закладок	Розробка та використання ОРД, які регламентують порядок доступу до приміщень працівників та
обслуговуючим персоналом (ремонтними організаціями), після початку експлуатації ІС	2) при технічному обслуговуванні елементів ІС	сторонніх осіб, і навіть правила проведення технічного обслуговування елементів ІС, зокрема під час виносу елементів за межі КЗ
Загроза внесення помилок, закладок у програмне забезпечення; використання недекларованих можливостей ПЗ	Може бути здійснена особами (програмістами-розробниками) у процесі розробки програмного забезпечення	Встановлення ліцензійного ПЗ. Періодичне оновлення ПЗ. Призначення відповідальних осіб у ІС організації (адміністратора безпеки)

Продовження таблиці 1.2

Загроза	Реалізація загрози	Заходи захисту
2.3 Загрози ненавмисних дій користувачів та порушень безпеки функціонування ІС та системи захисту інформації у її складі через збої у програмному забезпеченні, а також від загроз неантропогенного та стихійного характеру		
Загрози ненавмисних дій користувачів, внаслідок яких порушник отримує НСД до інформації	Може бути здійснена: 1) за рахунок надання користувачем / адміністратором своїми ненавмисними діями (бездіяльністю) можливості зовнішньому порушнику отримання НСД до інформації в ІС	Розробка та використання ОРД щодо необхідності дотримання конфіденційності оброблюваних даних та що містять правила і порядок обробки / знищення відомостей конфіденційної інформації; ознайомлення користувачів та відповідальних осіб із зазначеними ОРД
Загроза компрометації реквізитів доступу (втрата ключів доступу, розголошення чи крадіжка пароля тощо), НСД до аутентифікаційної інформації	Може бути здійснена: 1) за рахунок дій користувачів ІС при порушенні ними парольної політики, передачі ключів доступу третім особам тощо); 2) за умови успішного здійснення НСД до ОЗУ чи ПЗУ, в яких зберігається аутентифікаційна інформація	Розробка та використання вимог до вибору паролів та періодичності зміни паролів (парольної політики). Проведення інструктажів про дії у разі втрати чи компрометації паролів
Загроза ненавмисної модифікації (знищення) інформації працівниками	Може бути здійснена: 1) за рахунок дій користувачів ІС при невиконанні ними правил по роботі з конфіденційною інформацією	Розробка та використання ОРД, що містять правила та порядок обробки інформації конфіденційного характеру, а також порядок резервного копіювання та відновлення такої інформації
Загроза виходу з ладу програмно-апаратних засобів	Може бути здійснена при збоях у роботі апаратно-програмних засобів, що входять до складу ІС	Розробка та використання ОРД щодо реалізації заходів із резервного копіювання баз даних, що містять відомості конфіденційного характеру. Призначення відповідальних осіб (адміністратора безпеки)

Продовження таблиці 1.2

Загроза	Реалізація загрози	Заходи захисту
2.4 Загрози навмисних дій внутрішніх порушників		
Загроза доступу до інформації, модифікація, знищення співробітниками, не допущеними до обробки інформації, що захищається	Може бути здійснена внутрішнім порушником, не допущеним до обробки інформації, що захищається, але здатним тими чи іншими способами отримати інформацію обмеженого поширення	Розробка та використання ОРД, що регламентують порядок доступу до приміщення співробітників та сторонніх осіб. Цілодобова охорона приміщень ІС. Фізична охорона засобів обчислювальної техніки з боку співробітників охорони та співробітників організації. Встановлення на вікнах жалюзі або штор. Розташування засобів відображення інформації, що захищається з урахуванням запобігання можливому перегляду на них такої інформації, у тому числі за допомогою оптичних засобів
Загроза розголошення інформації, модифікація, знищення працівниками, допущеними до її опрацювання	Може бути здійснена внутрішніми порушниками, які допущені до інформації, що захищається, і які переслідують корисливі цілі	Розробка та використання ОРД, що містять правила та порядок обробки відомостей конфіденційного характеру. Отримання письмового зобов'язання про нерозголошення інформації, що захищається
2.5 Загрози безпосереднього доступу до операційної системи (ОС)		
Загрози, що реалізуються в ході завантаження ОС	Може бути здійснена при отриманні доступу до середовища ОС, порушник може скористатися як стандартними функціями операційних систем або будь-якої прикладної програми загального користування, так і спеціально створеними для виконання НСД програмами	Встановлення на ПК засобів довіреного завантаження. Розробка та використання ОРД, що регламентують порядок доступу до приміщення співробітників та сторонніх осіб. Цілодобова охорона приміщень ІС
Загрози, що реалізуються після завантаження ОС та спрямовані на виконання НСД із застосуванням стандартних функцій ОС та прикладного ПЗ	Може бути здійснена за допомогою зовнішнього носія для завантаження сторонньої операційної системи або шкідливого програмного забезпечення	Фізична охорона засобів обчислювальної техніки з боку працівників охорони та співробітників організації

Продовження таблиці 1.2

Загроза	Реалізація загрози	Заходи захисту
2.6 Загрози НСД каналами зв'язку		
Загрози, пов'язані з використанням WEB-сервісів в мережі, що захищається, а також сервісів клієнт-серверної архітектури, що використовуються в цій мережі при передачі інформації зовнішніми каналами зв'язку	Може бути здійснена при використанні внутрішніх / зовнішніх сервісів у мережі, що захищається, з можливостями обмеження доступності сервісів, зовнішнім порушником шляхом доступу / перехоплення / зміни HTTP cookies, зараження DNS-кешу, спотворення XML-схеми, використання альтернативних шляхів доступу до ресурсів	Встановлення міжмережевого екрану, що дозволяє фільтрувати вхідний та вихідний трафік. Криптографічне перетворення інформації, що передається за межі КЗ каналами зв'язку. Встановлення ліцензійного ПЗ. Розробка та використання ОРД щодо організації заходів антивірусного захисту, у тому числі своєчасного оновлення антивірусних баз, а також про правила зберігання та видалення даних із зовнішніх / внутрішніх носіїв інформації. Призначення відповідальних осіб у ІС організації (адміністратора безпеки)
Загрози сканування, спрямовані на виявлення мережевих адрес робочих станцій, типу ОС, відкритих портів та служб, топології мережі, доступності вузлів використовуваних сервісів	Може бути здійснена із застосуванням спеціального програмного забезпечення – мережевий сканер	
Загроза вбудовування додаткового незареєстрованого об'єкта мережі, а також загрози НСД шляхом заміни довіреного об'єкта	Може бути здійснена шляхом підміни довіреного об'єкта мережі, з метою подальшого отримання доступу до інформації, що захищається, отримання доступу до гіпервізора, до механізмів адміністрування середовища віртуалізації та тощо	
Загрози перехоплення інформації	Може бути здійснена шляхом перехоплення інформації, що передається каналами зв'язку, з метою подальшого аналізу цієї інформації та отримання НСД до сервісів ІС	
Загроза приведення системи в стан «відмовав обслуговуванні»	Може бути здійснена при лавиноподібному збільшенні кількості мережевих з'єднань з метою відмови доступу легальним користувачам	
Загроза вбудовування через мережу шкідливих програм та загроза їх негативних наслідків	Може бути здійснена шляхом поширення мережею шкідливого програмного забезпечення з метою подальшого отримання НСД до ресурсів інформаційної системи, ідентифікаційної / аутентифікаційної інформації, обмеження доступу до ресурсів та сервісів тощо	

1.3. Життєвий цикл документа у системі документообігу

Будь-який документ незалежно від його структури чи змісту проходить основні стадії свого ЖЦ:

1) створення та редагуваня його змісту;

2) вжиток (поширення, публікація);

3) зберігання та архівування;

4) знищення.

Обмеження на документ поділяються на три групи [6].

1. Обмеження контролю доступу – заборона або дозвіл на конкретні дії з певними фрагментами документа до певного кола осіб.

2. Обмеження цілісності – це забезпечення того, що дані, до яких є легітимний доступ, не були змінені або пошкоджені з моменту останньої коректно вчиненої дії з цим документом.

3. Обмеження життєвого циклу – це обмеження на порядок, у якому можуть бути виконані коректні дії.

Змішаний документообіг (рис. 1.1) має такі особливості.

1. Доступність та поширеність засобів обчислювальної техніки сприяють оцифруванню паперових архівів. В свою чергу це призводить до того, що проблеми перевірки змісту паперового документа на цілісність та підтвердження авторства цього документу.

2. Наявність проблеми перетворення документа з паперової версії до електронної. Мова не про просте сканування документу та зберігання його як зображення, а про розпізнавання тексту для того, щоб надалі можна було здійснювати повноцінний пошук за вмістом. Для вирішення цієї проблеми використовують системи оптичного розпізнавання тексту (OCR-бібліотеки). Але, незважаючи на постійне вдосконалення цього напряму, OCR-бібліотеки не можуть гарантувати стовідсоткової надійності. Навіть дотримання рекомендованих умов для кращого результату розпізнавання (тип шрифту, його розмір та інше) не дає гарантій повного правильного розпізнавання тексту.

3. Для змішаного документообігу рекомендують використовувати ідентичні засоби забезпечення захисту документів. При цьому постає проблема одночасного застосування ЕП для паперових версій документів, а рукописного підпису – для електронних.

Рисунок 1.1 – Життєвий цикл документа у змішаному документообігу

Забезпечити високий рівень захищеності документів, використовуючи для цього схожі інструменти, одночасно в аналоговому (паперовий носій) та електронному середовищі неможливо:

1) електронний підпис неможливо застосувати до документа на паперовому носії;

2) ЕП є відчужуваним від власника, тобто за ЕП неможливо точно ідентифікувати підписувача;

3) зображення автографа, який застосовується у паперовому документі для збереження та підтвердження юридичної значущості може бути скопійоване з метою подальшої фальсифікації інших документів (як електронних, так і паперових);

4) застосування зображення автографа під час роботи з електронними документами не гарантує, що сам автограф створено підписувачем. Немає

швидкого способу автоматизованої перевірки автентичності автографа. Почеркознавча експертиза — дорога та тривала процедура;

5) міграцію документів на паперовому носії за межі контрольованої зони складно відстежити чи запобігти, «людський фактор» завжди впливатиме на безпеку систем. Проте дії щодо створення паперових документів контролюються інформаційними технологіями. Якщо документ конфіденційного змісту виводиться на друк, ця дія не повинна залишатися поза увагою, потрібно підтвердити особу суб'єкта, який ініціював цю дію. Процедуру підтвердження особистості потрібно проводити безперервно у процесі роботи суб'єкта із документом.

Ключем до вирішення описаних проблем є надійна прив'язка всіх аутентифікаторів суб'єкта (паролей, ключів шифрування та ЕП, кодів доступу тощо) до його біометричних характеристик. При цьому слід враховувати наступне:

1) процедура надання користувачем біометричних даних має бути ненав'язливою, не повинна порушувати чи ускладнювати існуючі бізнес-процеси в організації;

2) впровадження методів біометричного захисту документів має бути економічно обґрунтованим. Плюсом у ситуації, що склалася, буде можливість реалізації засобів захисту на стандартному обладнанні комп'ютерних систем;

3) пов'язаний з аутентифікатором біометричний образ суб'єкта має бути таємним або його копіювання чи відтворення іншими особами має бути нездійсненним (дуже малоймовірним).

1.4. Перетворювач біометрія-код у біометричній системі

Ключовим поняттям, що безпосередньо вирішує задачу «зв'язування» ключів шифрування та паролів з біометричними параметрами суб'єкта є перетворювач «біометрія-код» (ПБК).

Відповідно до ISO/IEC JTC 1/SC27 WD 24745–2006 [7] ПБК – перетворювач, здатний перетворювати вектор нечітких, неоднозначних біометричних параметрів «Свій» на чіткий однозначний код ключа (пароля). У разі впливу випадкового вхідного вектора, що не належить безлічі образів «Свій» на ПБК, він генерує на своєму виході випадковий код.

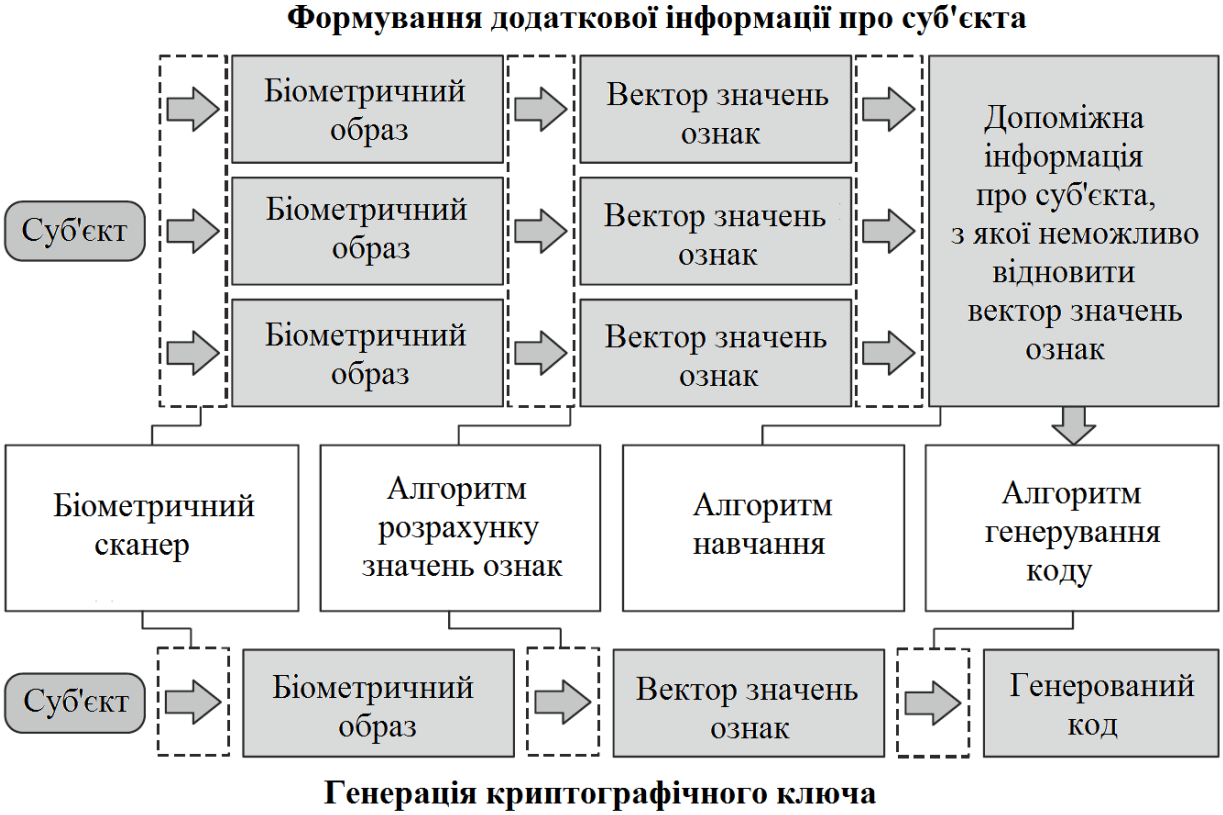


Рисунок 1.2 – Загальна схема перетворювача біометрія-код

Для посилення стійкості біометричного захисту до атак вивчення та модифікації програмного забезпечення (ПЗ) варіанти його технічної реалізації не повинні містити біометричних образів користувача, біометричного еталону користувача та коду ключа (пароля) користувача. Ця інформація є конфіденційною і має бути захищена під час зберігання. Крім того, сліди цієї конфіденційної інформації повинні бути гарантовано знищені після виконан-

ня кожної конкретної процедури аутентифікації.

Іншими словами: біометричні еталони (і зразки) не можна компрометувати. Під захищеністю від компрометації мається на увазі забезпечення неможливості або технічної (обчислювальної) складності отримання знань (даних навчальної вибірки) з навченого класифікатора.

1.5. Висновки

1. Розглянуто основні стадії життєвого циклу документу в процесі змішаного документообігу, а також проведено аналіз основних загроз інформаційній безпеці на кожному із зазначених етапів. Найчастіше методами нейтралізації загроз виступають організаційно-технічні заходи, які не вирішують проблему «людського фактора» – недбалість, некомпетентність, несумлінність тощо. Використання надійних паролів та криптографічних ключів не виключає їх відчужуваності з цієї ж причини. Це призводить до фальсифікації юридично важливих документів та реалізації інших загроз (застосування сертифікованих засобів ЕП до шкідливого контенту, уникнення винними особами відповідальності).

Одним з можливих рішень проблем документообігу, пов'язаних з «людським фактором», є комплексування криптографічних та біометричних методів аутентифікації.

2. Захищеність інформаційної системи визначається найслабшою ланкою в системі безпеки, тому в змішаному документообігу потрібно намагатись забезпечити приблизно рівний рівень захисту для документів на будь-яких видах носіїв за наявності одних і тих же реквізитів, що забезпечують їх автентичність. Неможливість автоматизованої перевірки цілісності та автентичності, а також застосування ЕП та інших криптографічних механізмів для «паперових» реалізацій документа призводить до більш низької захищеності документа при його розповсюдженні «на папері».

Отже, актуальними є задачі:

1) дослідити концепцію системи захисту змішаного документообігу, що використовує засоби ЕП з біометричною активацією без використання спеціального обладнання та біометричних сканерів;

2) запропонувати модель ПБК, орієнтованого на обробку параметрів клавіатурного почерку;

3) запропонувати алгоритм створення та перевірки ЕП з біометричною активацією для документів на електронних та паперових носіях.

2 МЕТОДИ ЗАХИСТУ ЗМІШАНОГО ДОКУМЕНТООБІГУ

Як було зазначено у попередньому розділі, під гібридним документом мається на увазі юридично значимий документ, що перебуває в електронному чи паперовому вигляді, містить зображення підпису, захищений за допомогою ЕП, для формування якого враховуються біометричні дані автора, що дозволяє швидко перевірити цілісність і автентичність документа незалежно від типу носія. Додатково документ може містити гриф обмеження доступу для захисту конфіденційності під час роботи з його електронними реалізаціями.

Особливістю гібридного документу є наявність наступних атрибутів: електронно-цифровий підпис (ЕП), для формування якого використовуються секретний ключ, біометричні дані користувача, хеш-функція документу і рукописний підпис суб'єкта. Використання біометричних параметрів для захисту документів для формування ЕП є ключовою відмінністю гібридного документообігу [8-9] від змішаного.

В роботі [10] запропоновано один із можливих варіантів побудови гібридного документу з використанням зображення підпису та двох електронних підписів (одним підписується текст документа, другим – весь документ разом із зображенням підпису). Послідовно виконуються наступні дії:

1. Створюється пара з відкритого та особистого ключа автора.
2. Реєструється відкритий ключ автора в засвідчу вальному центрі (Certificate Authority).
3. Формується перший електронний цифровий підпис під інформацією електронного документу за допомогою особистого ключа автора.
4. Автор електронного документа формує свій підпис, відтворюючи його на екрані комп'ютера.
5. Підпис перетворюється на бінарний файл, який об'єднується з підписаним електронним документом, при цьому також вносяться в документ

дані про розмір графічного бінарного файлу з підписом.

6. Створена комбінація даних підписується другим електронним цифровим підписом.

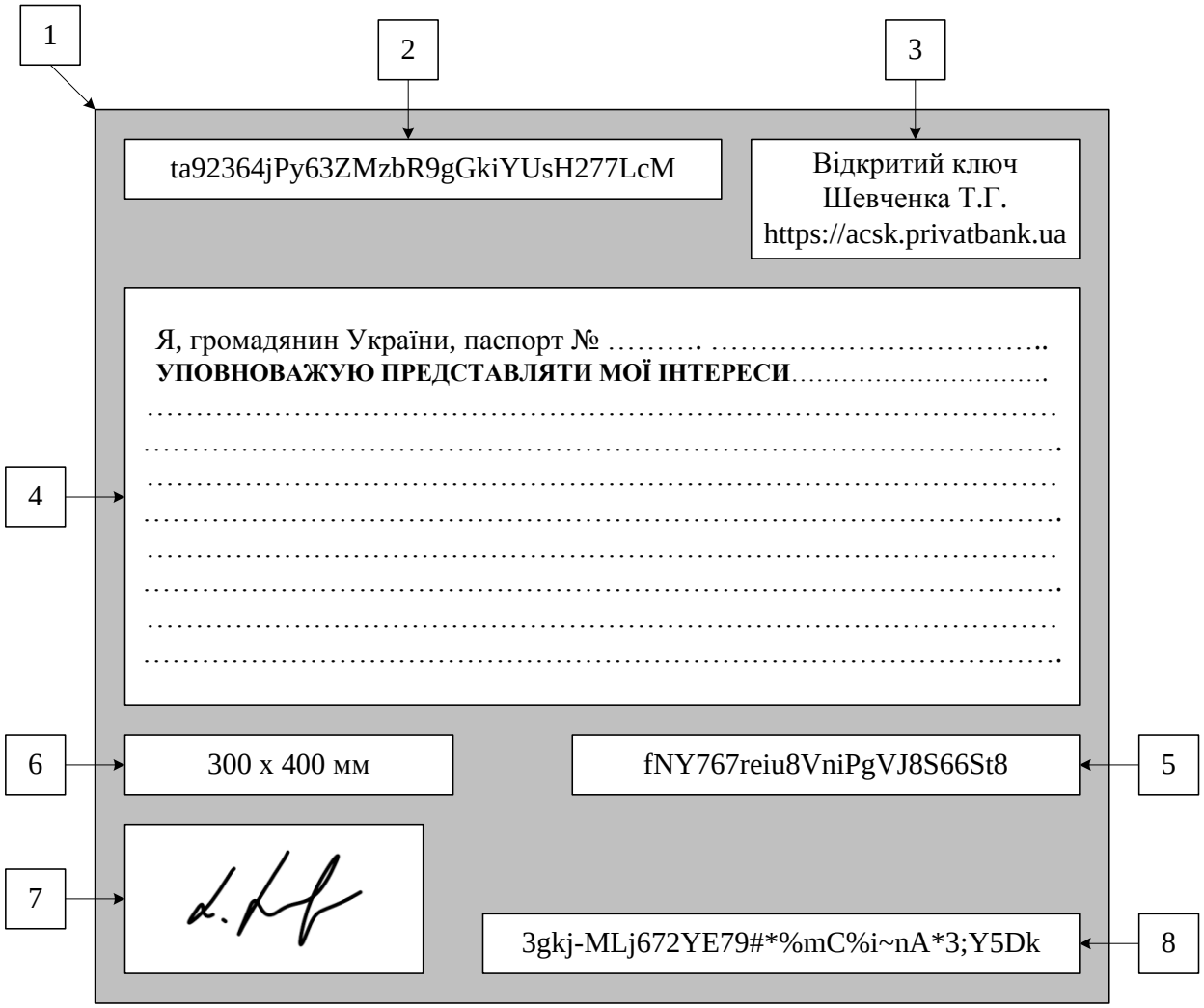


Рисунок 2.1 – Початковий формат гібридного документа

На рис. 2.1 наведено варіант реалізації гібридного документа, тобто він зберігається у форматі «PDF» та може бути роздрукований на паперовому носії. Тут:

1 – повне інформаційне поле всього достовірного документа;

2 – поле для розміщення коду відкритого ключа автора документа у вигляді штрих-коду;

3 – поле для розміщення інформації про засвідчувальний центр, в якому зареєстровано відкритий ключ документа та звідки можна скачати серти-

фікат відкритого ключа;

4 – поле достовірного тексту документу;

5 – поле, де розміщується перший електронний цифровий підпис, що підписує текст документа в полі 4;

6 – поле, де розміщено інформацію про розмір графічного файлу з рукописним підписом автора електронного документу;

7 – поле, де розміщено образ рукописного підпису автора електронного документу;

8 – другий електронний цифровий підпис, що підписує текстовий документ і графічний файл з рукописним підписом автора електронного документу.

2.1. Система захисту змішаного документообігу на основі електронного підпису з біометричною активацією

До недоліків рішення, наведеного на рис. 2.1, можна віднести обмеженість біометричного захисту – секретний ключ ЕП не генерується безпосередньо з біометричних даних автора. З цієї причини і застосовуються два електронні підписи. Тому слід запропонувати інший спосіб побудови гібридного документу на основі захисту змішаного документообігу з використанням процедури генерації секретного ключа ЕП із біометричних даних та всього одного ЕП. Пропонована схема маршруту документу наведена на рис. 2.2.

Наведена схема ілюструє інтеграцію у звичну схему змішаного документообігу методів підтвердження автентичності документа незалежно від форми його представлення. Тут важливим моментом є те, що спочатку документ створюється на ПК, бо сучасний розвиток інформаційних технологій дозволяє стверджувати, що рукописні юридично значущі документи створюються з використанням сучасної обчислювальної техніки (заяви, що заповнюються «від руки», також можна надрукувати), а потім можуть передаватися далі в електронному або паперовому вигляді. Але під час підписання

документ обов'язково трансформується в електронний формат без втрати інформації (контексту).

Рисунок 2.2 – Модифікована схема маршруту документу в змішаному документообігу

Для генерації ключа користувачеві – власнику документу – необхідно ввести за допомогою стандартного периферійного обладнання (клавіатура, камера, планшет тощо) ряд динамічних біометричних образів, які потім подаються на вхід надійного ПБК. Причому подібна генерація проводиться при кожному підписанні / перевірці документа, що виключає, як у випадку зі звичайним ЕП, втрату його носія та / або передачу третім особам чи підробку.

Генерація пари відкритого та закритого ключів, обчислення хеш-суми адаптованого тексту документу, формування ЕП реалізується в особистому кабінеті / акаунті користувача. Доступ до облікового запису здійснюється за парою логін / аутентифікатор (таємний біометричний образ – біометричний пароль, посилений статичним за необхідності, або звичайний пароль, посилений біометричним), після чого користувач має доступ до свого облікового запису.

Рисунок 2.3 – Алгоритм створення гібридного документу

Після завантаження фінальної версії електронного документу до облікового запису користувача до нього додається графічне зображення підпису. Потім відбувається розрахунок хеш-суми інформативного тексту документу, а також синдрому помилок для їх виправлення після розпізнавання. На підставі отриманого біометричного образу формується пара відкритий-закритий ключ, за допомогою закритого ключа та хеш-суми відбувається генерація ЕП документу.

До документу додаються реквізити, бланк організації, а також QR-коди, в яких розміщується інформація про ЕП та синдроми помилок (для відновлення текстового вмісту документа), відкритий ключ та посилання на документ на хмарному сервері. Важливо відмітити, що посилання на документ формується лише після введення користувачем вірного біометричного образу.

Кожне наступне редагування документа його власником супроводжується генерацією нового посилання на хмарний сервер, що забезпечує отримання довіреною стороною актуальної та автентичної версії документу (рис. 2.3).

Приклад того, як може виглядати гібридний документ, отриманий за розглянутою схемою, наведено на рис. 2.4.

Слід зазначити, що реалізація запропонованого способу формування гібридних документів, не накладає обмежень на взаємне розміщення інфор-

маційних полів документу. Місце розташування полів задається програмним забезпеченням, що реалізує запропонований спосіб. Критичною є наявність у документі відповідної інформації та рамок, що обмежують поля з інформацією. Рамки необхідні для того, щоб інформація з різних полів не переплутувалася під час її вилучення з документа у форматі «PDF» або з відсканованого електронного образу достовірного документа на паперовому носії.

Рисунок 2.4 – Зовнішній вигляд гібридного документу

Після того, як довірена сторона отримала гібридний документ у будь-якій формі, вона може перевірити його автентичність. Якщо документ було отримано у паперовому вигляді, його необхідно відсканувати, розпізнати текст за допомогою спеціального програмного забезпечення, обчислити його хеш-суму. Потім зчитати перший QR-код, в якому розміщується ЕП, розши-

фрувати його відкритим ключем (другий QR-код), порівняти їх. Навіть якщо отримана хеш-сума не збігаються необхідно перейти за посиланням (третій QR-код) на хмарний сервер і порівняти отриману хеш-суму з розміщеною на сервері, а також всю інформацію, що знаходиться там, включаючи дату підписання документа, дані про власника ЕП тощо (рис. 2.5). Для електронної версії документу зникає необхідність сканувати текст і розпізнавати його – можна одразу перейти до обчислення його хеш-суми.

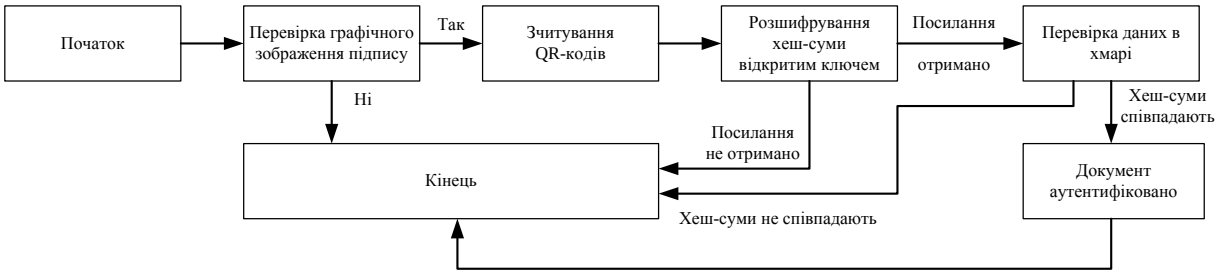


Рисунок 2.5 – Схема перевірки автентичності гібридного документу

Розглянута схема гібридного документообігу включає також схему електронного документообігу, в якій засобом підтвердження цілісності та автентичності документа виступає посилений кваліфікований ЕП, тобто сертифікат якого виданий акредитованим посвідчувальним центром. В такому разі хмарний сервер повинен перебувати під контролем ПЦ, при цьому немає необхідності розміщувати на сервері самі документи та біометричні образи користувачів, замість цього достатньо зберігати хеш-суму документу, а закритий ключ генерувати з біометричних даних, що пред'являються, за допомогою налаштованого перетворювача «біометрія-код », що безпечно зберігає секретний ключ ЕП і біометричний еталон.

Якщо документ містить конфіденційну інформацію, то при переході за посиланням, де розміщено оригінал або під час відкриття електронної копії, користувач, який здійснює доступ, повинен також пройти аутентифікацію. Без автентифікації можна отримати доступ лише до частини документа, яка не є конфіденційною.

Таким чином, передбачається, що робота з електронною версією доку-

мента (з оригіналом на сервері або локальною копією) може здійснюватись лише через спеціальний сервіс – компонент програмного комплексу, що реалізує гібридний документообіг.

На папері у відкритому вигляді розміщується лише інформація неконфіденційного характеру, інформація обмеженого доступу не роздруковується, замість неї розміщуються спеціальні хеш-блоки, що містять контрольні суми відповідного конфіденційного контенту. Вони потрібні для обчислення загальної контрольної суми всього документу та перевірки його цілісності та автентичності з використанням ЕП. Для доступу до конфіденційних текстових блоків документу необхідно перейти за посиланням та пройти автентифікацію.

Таким чином, можна виділити такі основні аспекти (етапи) роботи з гібридним документом:

1. Навчання біометричної системи. При реєстрації нового користувача він пред'являє кілька навчальних прикладів біометричного образу, після чого ПБК налаштовується на генерування певного ключа (пароля) при пред'явленні біометричного образу цього користувача. Може створюватися кілька ПБК, кожен із яких налаштовується на певний ключ чи пароль, якщо є кілька незалежних сервісів ІС організації, кожен із яких має власну функцію авторизації. Для зміни ключа (пароля) користувача потрібно повторно ввести біометричний образ. Для зміни еталону образу необхідно повторно навчати ПБК.

2. Біометрична аутентифікація користувача, що відбувається під час здійснення доступу до сервісу ІС організації або до гібридного документу. Процедура автентифікації може бути багатофакторною залежно від реалізації концепції захисту документообігу. Залежно від типу сервісу або грифа документу, біометричні дані та пароль можуть не запитуватися.

3. Формування гібридного документу за допомогою певного сервісу, який потребує аутентифікації. Користувач готує проект документу в електронній формі та вводить біометричні дані. Далі з наданих біометричних даних за допомогою ПБК формується ключ ЕП. На основі тексту документу

формується ЕП гібридного документу. Документ не буде автентичним, якщо біометричні дані фальсифіковані, бо в цьому випадку ПБК видасть неправильний ключ ЕП. Створений автентичний оригінал документу зберігається на хмарному сервері, на нього формується посилання резервного відновлення. Власник може обмежити доступ інших осіб до електронної реалізації документу, і навіть до окремих його параграфів. Можна також заборонити певні дії (друк, редагування тощо). Нарешті. відповідний вміст документу шифрується за допомогою комбінацій асиметричного та симетричного шифрування з використанням ключів користувача, якому надається доступ (вміст шифрується симетричним алгоритмом на сеансовому ключі, який шифрується асиметричним алгоритмом). При цьому до документу додається відповідний гриф. Шифрування необхідно аби до документу неможна було здійснити доступ в обхід сервісу. ЕП документу створюється з урахуванням відкритих блоків інформації та контрольних сум зашифрованих блоків. При розрахунку контрольної суми документу зашифровані блоки попередньо хешуються та конкатенуються з відкритими блоками, з об'єднаного рядка обчислюється загальний хеш.

4. Доступ до гібридного документу та його редагування. Залежно від грифу конфіденційності користувачеві може знадобитися пройти біометричну автентифікацію. У процесі подальшої роботи з документом проводиться безперервний збір біометричних даних для більш надійної верифікації особи користувача.

В процесі накопичення ідентифікаційної інформації про користувача блоки даних документа, що містять конфіденційні відомості, дешифруються, в результаті документ змінює параметри відображення та редагування на ходу, приховуючи або замінюючи певні фрагменти, блокуючи і надаючи окремі функції (рис. 2.6). Самі дії щодо приховання / заміни вмісту визначаються автором документу та залежать від реалізації концепції на практиці.

5. Друк документу. Під час створення паперової версії гібридного документу розміщуються обмежувальні рамки та всі основні реквізити (рукописні підписи, печатки, логотип – рис. 2.4). На документі розміщуються QR-коди. Перший містить ЕП та синдроми помилок (для коригування невірних біт при перекладі «паперової» версії документа в електронну). Другий QR-код містить посилання на оригінал документа в електронному вигляді, що зберігається на захищеному сервері, доступ до якого здійснюється через сервіс ІС організації. Також на документ може бути розміщений додатковий QR-код із відкритим ключем ЕП.

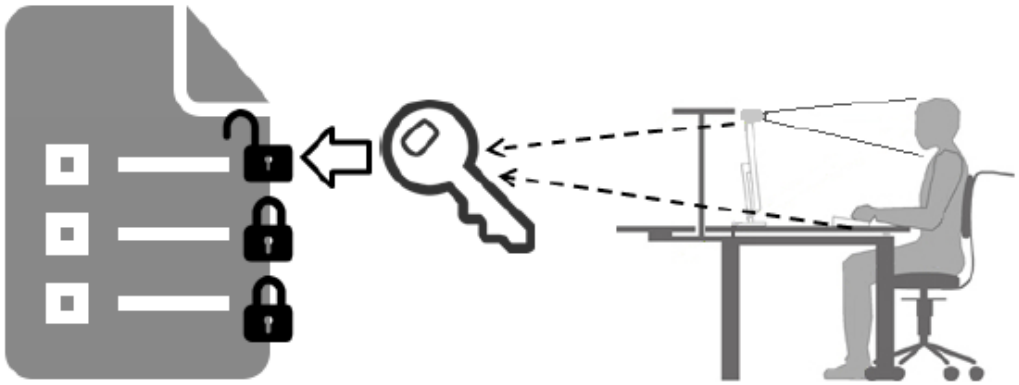


Рисунок 2.6 – Отримання доступу до фрагменту
електронної версії документу

6. Верифікація документу. Для перевірки гібридного документу на цілісність і автентичність з документа відновлюється основна змістовна частина. Якщо документ представлений на паперовому носії, він сканується або фотографується, після чого до зображень застосовуються методи оптичного розпізнавання символів і коди, що виправляють помилки. При виявленні порушення цілісності, суб'єкт має можливість відновити зміст документа, перейшовши за посиланням, відновленим із QR-коду, за невідповідності якому документ визнається недійсним.

2.2. Висновки

Розглянуто концепцію захисту гібридного документообігу.

Гібридний документообіг на основі електронного підпису з біометричною активацією є модифікацією схеми змішаного документа, в якому:

1) наявна надійна прив'язка всіх аутентифікаторів суб'єкта (паролів, ключів шифрування та ЕП, кодів доступу тощо) до його біометричних характеристик;

2) з'являється можливість оперативно перевірити цілісність та автентичність документів незалежно від типу носія та відновити оригінал, якщо документ пошкоджений;

3) документи на всіх видах носіїв захищені від порушення конфіденційності;

4) забезпечується рівний захист документу, як в електронному, так і в паперовому вигляді (під рівним захистом мається на увазі використання однакових механізмів захисту для обох форматів документу).

Реалізація розглянутої системи документообігу забезпечує дотримання принципу економічної доцільності, бо немає потреби закуповувати дороге апаратне забезпечення – є можливість реалізації засобів біометричного захисту на стандартному обладнанні комп'ютерних систем.

Перевагою розглянутої системи документообігу також є можливість застосування колективного підписання документів. Документ формують кілька осіб, і його користувачі переконуються у достовірності документа. Вся інформація, необхідна для перевірки, у створених документах вже є. У разі, якщо людина, яка формує колективний документ, не згодна з його інформаційним змістом, вона вносить корективи в інформаційну частину, вставляє в документ свій автограф, далі підписує ці зміни та документ своїм ЕП. Ініціатор правки до документа відсилає його іншим особам, які формують цей документ.

Документ як активний елемент документообігу збагачується постійними та змінними атрибутами: мітка доступу, час внесення змін тощо. Для при-

ховування цих метаданих можна використовувати алгоритми стеганографії. Для документу, одержуваного в електронному вигляді доцільно змінювати молодші біти в послідовності бітів, що кодують колір тесту – це не вносить надмірності в документ, не впливає на хеш-суму документу, тому повідомлення може бути вбудоване до формування ЕП; секретний ключ визначення символів, у яких приховані біти повідомлення, зашифрований відкритим ключем учасників групи, і може бути розшифрований лише особистим ключем авторизованого користувача. Для документа, отриманого у паперовому вигляді, доцільно ховати повідомлення у QR-кодах – обов'язкових реквізитах гібридного документа. Наведений спосіб приховування даних у гібридному документі дозволить забезпечити додатковий захист даних у процесі життєвого циклу у гібридному документообігу.

3 АНАЛІЗ ІСНУЮЧИХ БІОМЕТРИЧНИХ КРИПТОГРАФІЧНИХСИСТЕМ

В наш час сформувались два основні напрямки застосування біометрії: аутентифікація особистості та криптографія.

Використання біометрії для аутентифікації особистості є традиційним, має велику історію вивчення та застосування. Загалом методи біометричної аутентифікації добре відпрацьовані та успішно застосовуються на практиці. Ці методи постійно розвиваються та вдосконалюються, що робить їх привабливими для масового застосування, наприклад, у системах контролю та управління доступом до режимних приміщень та до джерел інформації, у тому числі до комп'ютерів та обчислювальних мереж.

Застосування біометричних методів у криптографії має особливості. Криптографічні методи широко застосовуються для забезпечення таємності та автентичності інформації. Їх стійкість заснована на припущенні, що секретний ключ відомий тільки законному користувачеві. Насправді збереження секретності ключа одна із основних задач під час експлуатації криптосистем. Ключі зазвичай зберігаються в безпечному місці і для контролю доступу до них найчастіше використовується парольна аутентифікація, яка має ряд недоліків: паролі можуть бути легко втрачені, вкрадені, забуті тощо. Недоліки парольної автентифікації можна подолати за допомогою методів біометричної аутентифікації, що мають низку переваг у порівнянні з традиційними, а саме: 1) біометричні ознаки дуже складно фальсифікувати; 2) унікальність біометричних ознак забезпечує дуже високу достовірність аутентифікації; 3) біометричний ідентифікатор не можна забути як пароль або втратити як пластикову картку; 4) для біометричної аутентифікації потрібна наявність власника біометричних ознак. Таким чином, біометричні системи надають природне та надійне вирішення задачі аутентифікації в криптографічних системах.

Останнім часом сформувався новий напрямок застосування біометрії в системах криптографічного захисту інформації: біометрія стала застосовуватися не тільки для захисту від несанкціонованого доступу до ключів, але і як джерело ключового матеріалу.

Однак застосування біометричного матеріалу як джерела ключів наштовхується ряд складнощів: біометричні дані нечітко відтворювані і не мають рівномірного розподілу, тоді як більшість криптографічних перетворень вимагають точного значення ключа. Залежно від мети застосування біометрії в криптографії виділяються кілька видів біометричних криптографічних систем [11-13]. Їхню загальну класифікацію за результатами проведеного аналізу зображено на рис. 3.1:

− системи зі звільненням ключа (англ. Key Release Cryptosystems);

− системи зі зв'язуванням ключа (англ. Key Binding Cryptosystems);

− системи з генерацією ключа (англ. Key Generation Cryptosystems).

3.1 Біометричні криптосистеми зі звільненням ключа

У режимі звільнення ключа біометрична автентифікація здійснюється незалежно від механізму звільнення ключа, біометричний еталон і ключ зберігаються окремо один від одного, сам ключ звільняється після успішної біометричної автентифікації [11-13]. Схематичне зображення такої біометричної криптографічної системи наведено на рис. 3.2.

Отже, біометрична автентифікація відокремлена від криптографічної частини системи. В такому випадку, як пароль від ключа використовуються результати порівняння отриманого біометричного зображення з шаблоном. Даний вид біометричних криптосистем непридатний у більшості випадків, оскільки існує можливість заміни модуля порівняння під час виконання автентифікації. Цей метод буде добре працювати в додатках фізичного доступу, де біометричні шаблони та ключі можуть зберігатися в безпечному місці, фізично відокремленому від пристрою захоплення біометричних зображень.

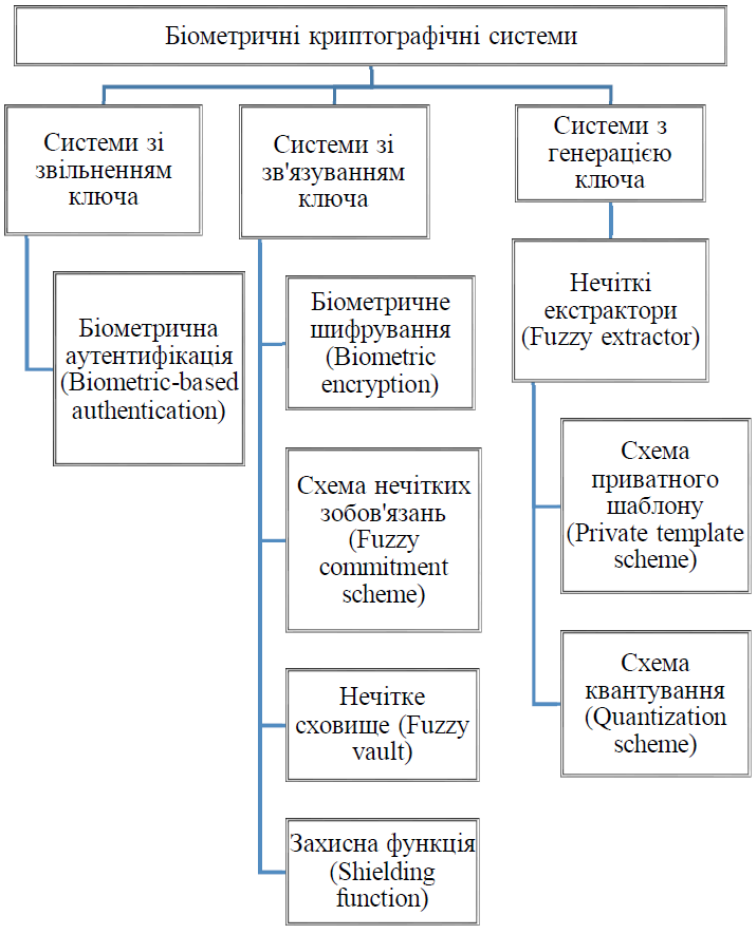


Рисунок 3.1 – Види та підвиди біометричних криптографічних систем

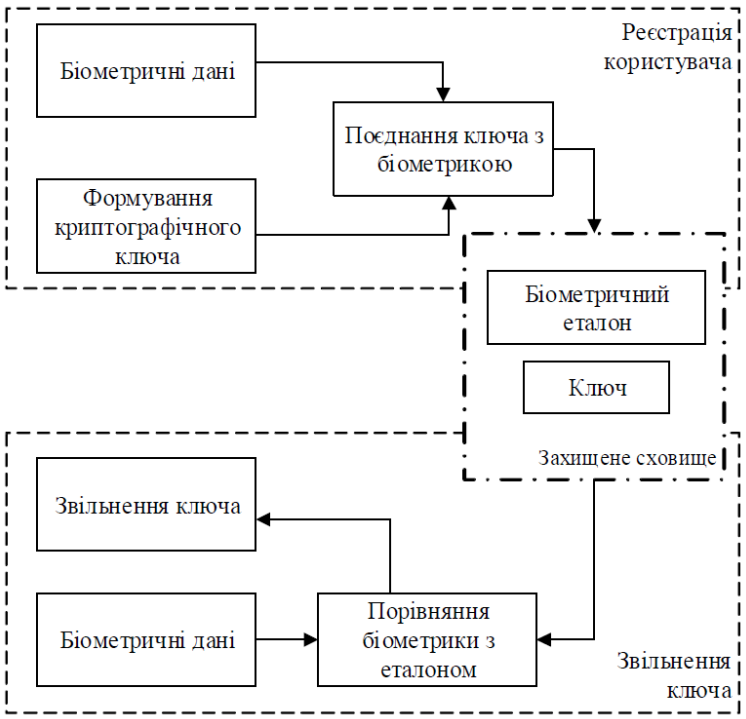


Рисунок 3.2 – Схематичне зображення біометричної криптографічної системи зі звільненням ключа

3.2 Біометричні криптосистеми зі зв'язуванням ключа

У криптографічних системах такого типу ключ і біометричний еталон криптографічно пов'язані між собою [12-14]. Ключ за певним алгоритмом пов’язується з біометричним еталоном користувача і зберігається в такому вигляді в базі даних, відповідно розкрити ключ представляється можливим тільки власникові біометричних параметрів. У таких системах передбачається, проте не є необхідним, використання допоміжних даних (англ. Helper Data), для демаскування зашумлених біометричних даних. Схематично приклад біометричних систем зі зв’язуванням ключа подано на рис. 3.3.

Рисунок 3.3 –
Схематичне зображення біометричної
криптографічної системи зі зв'язуванням ключа

Цей спосіб включає приховування криптографічного ключа в самому біометричному шаблоні реєстрації за допомогою надійного (секретного) алгоритму бітової заміни. Після успішної автентифікації користувачем цей довірений алгоритм просто витягає біти ключа, після цього ключ придатний для користування. На жаль, це означає, що криптографічний ключ буде вилу-

чено з того ж розташування в шаблоні щоразу, коли інший користувач автентифікується системою. Таким чином, якщо зловмисник міг визначити бітові розташування, які вказують ключ, то зловмисник може відновити вбудований ключ із будь-якого шаблону інших користувачів. Якщо зловмисник мав доступ до системи, то він міг визначити місця розташування ключа, наприклад, додаючи кількох людей у систему, використовуючи однакові ключі для кожної реєстрації. В такому випадку, зловмиснику потрібно лише знайти ці місця розташування біт з загальною інформацією в шаблонах.

3.2.1 Біометричне шифрування

Біометричне шифрування є процесом, який надійно пов'язує криптографічний ключ з біометричним, тому що ні ключ, ні біометричні дані не можуть бути вилучені зі збереженого шаблону [14].

Криптографічний ключ генерується випадковим чином при реєстрації так, що ніхто, включаючи користувача, не знає його. Сам ключ повністю незалежний від біометрії і, отже, завжди може бути змінений або оновлений. Після отримання біометричного зразка створюється захищений шаблон, так званий «приватний шаблон» (англ. private template). По суті, криптографічний ключ шифрується за допомогою біометричного. Під час перевірки користувач представляє свій біометричний зразок, який в ході застосування до легітимного шаблоном дозволить отримати той самий ключ. Ключ відтворюється тільки в тому випадку, якщо під час перевірки представлений правильний біометричний зразок. Таким чином, біометрія служить ключем дешифрування Алгоритм розроблений так, що незначна розбіжність отриманих біометричних образів від однієї особи не впливає на коректну роботу алгоритму.

Підходи, засновані на біометричному шифруванні, чутливі до атаки змішаної заміни, атаки сходження і атаки найближчого самозванця. Більш того, зловмисник може використовувати відновлений секрет для вилучення оригінальних біометричних даних з захищених шаблонів.

Mytec1 був першою реалізацією такої біокріптографічної схеми. Пізні-

ше Mytec2 був розроблений для забезпечення більш складного захисту шаблону відбитка пальця, що зберігається. Схематичне зображення біометричної криптографічної системи наведено на рис. 3.4.

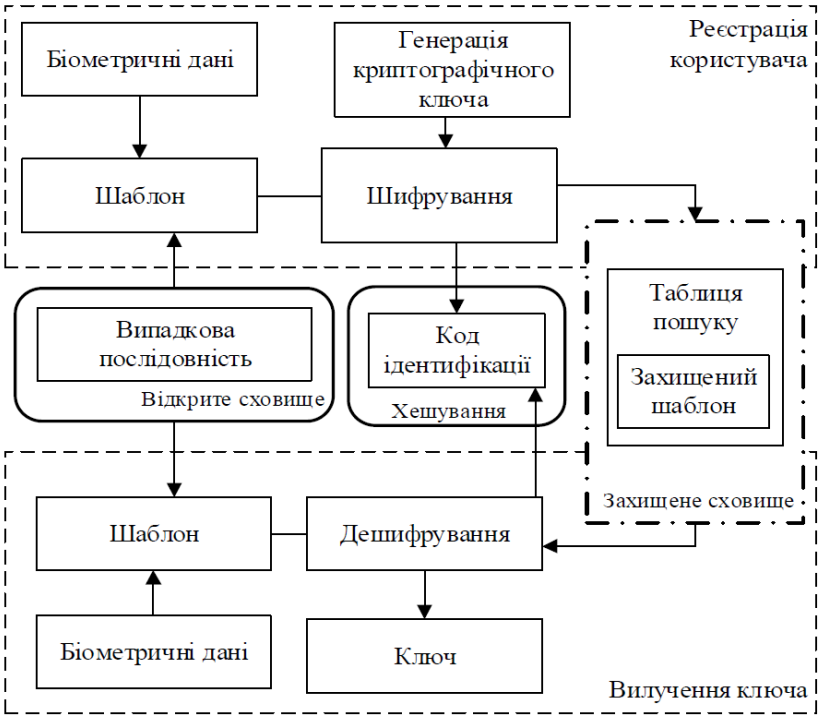


Рисунок 3.4 – Схематичне зображення біометричної криптографічної системи зі зв'язуванням ключа: біометричне шифрування

3.2.2 Схема нечітких зобов'язань

Схема нечітких зобов'язань [15] є криптографічним алгоритмом, який забезпечує збереження біометричних даних за допомогою методів криптографії та кодування з виправленням помилок. Алгоритм пов'язує секретну інформацію з даними, щоб приховати дані і не дозволити власникові даних розкрити її більш ніж одним способом. Нечіткі схеми зобов'язань використовувалися для збереження біометричних шаблонів. Ця схема, що застосовується до біометричних шаблонів, розглядає сам шаблон без будь-якої модифікації як пошкоджене кодове слово, яке підлягає декодуванню. У таких системах для формування шаблону та вилучення даних використовується так званий свідок (або ключ шифрування). Також вважається, що для коректного функціонування алгоритму свідок може мати схожі, проте не ідентичні мет-

рики. Схематичне зображення біометричної криптографічної системи наведено на рис. 3.5.

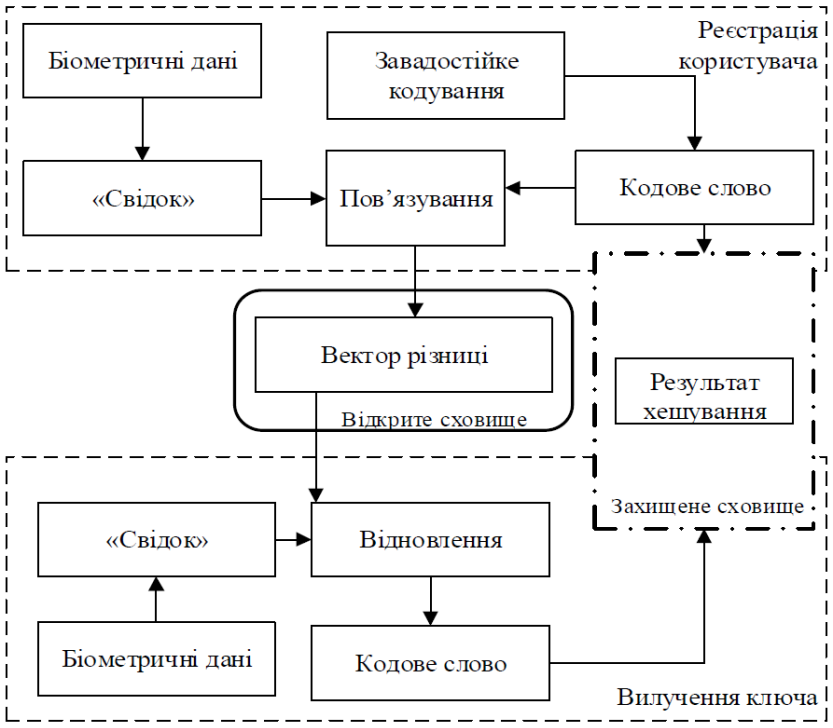


Рисунок 3.5 – Схематичне зображення біометричної криптографічної системи зі зв'язуванням ключа: схема нечітких зобов'язань

Основною слабкістю схеми нечітких зобов'язань є сприйнятливість до атак у середовищах, які залучають довірену третю сторону. Схеми нечітких зобов'язань з максимальним розміром ключів забезпечують оптимальну продуктивність для абсолютно безсистемного випадку. Також було виявлено, що нечіткі схеми зобов'язань забезпечують обмежену безпеку секретного ключа та біометричних даних у загальних випадках без пам'яті та у стаціонарних ергодичних випадках. Нечіткі схеми зобов'язань також сприйнятливі до атаки грубою силою. Атаки через множинність записів також можуть бути використані для декодування захищених біометричних даних.

3.2.3 Нечіткі сховища

У роботі [16] вперше було описано конструкцію нечіткого сховища (англ. Fuzzy vault). Узагальнено основну ідею можна описати так. Нехай користувач 1 помістить деяке секретне значення k у нечітке сховище та «заблокує» його, використовуючи набір (підмножину) елементів з деякої відкритої універсальної множини A. Якщо користувач 2 спробує «розблокувати» таке сховище, використовуючи набір B елементів (потужності підмножини A та B співпадають), то він успішно отримає секретне значення лише у випадку, якщо B подібно A. Тобто тільки, якщо A та B значною мірою є множинами, що перетинаються. Відмінною особливістю цього алгоритму за думкою авторів є те, що ця схема володіє інваріантністю порядку значень в наборах, вважається, що упорядкування підмножин A та B не впливає на роботу схеми. У такому випадку схема має доказану криптографічну стійкість до обчислювальних атак типу груба сила. Схематичне зображення біометричної криптографічної системи наведено на рис. 3.6.

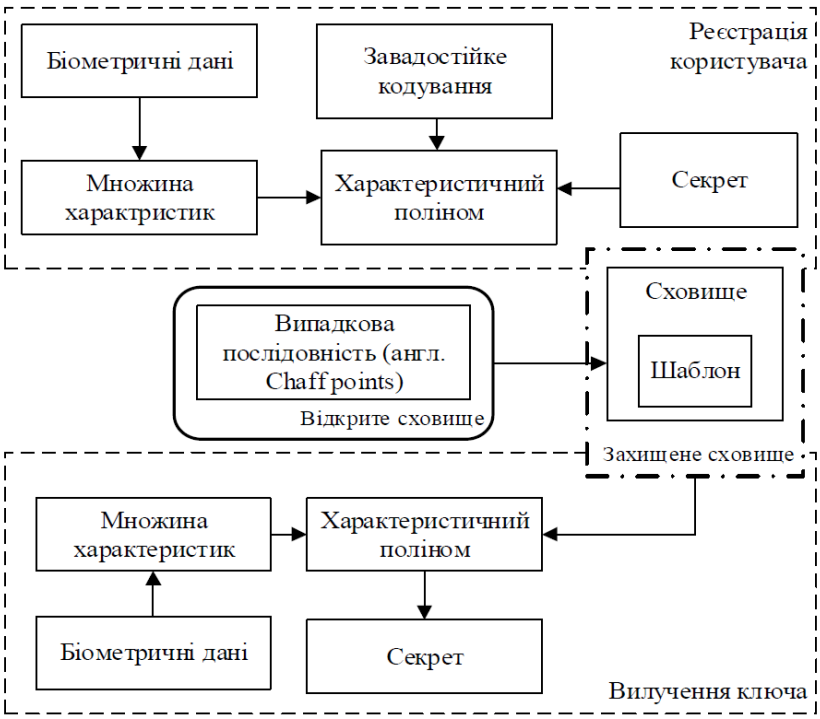


Рисунок 3.6 – Схематичне зображення біометричної криптографічної системи зі зв'язуванням ключа: схема нечітких сховищ

Розглянемо основні принципи схеми нечіткого сховища на прикладі. Нехай користувач 1 – любитель кіно. Він шукає того, хто розділяє його інтереси, але не хоче розкривати інформацію про свої уподобання всім людям. Один з підходів, який він може зробити, полягає в тому, щоб створити набір його улюблених фільмів і опублікувати його в прихованій формі. Наприклад, користувач 1 може опублікувати зашифрований текст C_A, який представляє його зашифрований на наборі (в даному випадку, ключі) A телефонний номер tel_A. В цьому випадку, якщо користувач 2 склав свій список улюблених фільмів B, і якщо вони ідентичні A, він зможе розшифрувати C_A і отримати телефонний номер tel_A користувача 1. Якщо ж користувач 2 спробує розшифрувати C_A за допомогою множини даних, що відрізняються від множини інтересів користувача 1, він не зможе отримати його номер телефону. Недоліком цього підходу є його точність у визначенні подібності двох множин або відсутність допущення помилок. Якщо інтереси користувача 2 дуже схожі на інтереси користувача 1, але, наприклад, якщо йому подобаються кілька фільмів, які користувач 1 не любить, то користувач 2 не дізнається його телефон. Цілком ймовірно, що в цьому випадку користувач 1 все одно хотів би, щоб користувач 2 отримав його номер телефону, оскільки їх смаки дуже схожі. Автори ж пропонують поняття нечіткого сховища. Це криптографічна конструкція, відповідно до якої користувач 1 може заблокувати свій номер телефону tel_A , використовуючи набір даних A, помістивши його в сховище, позначене V_A. Якщо користувач 2 намагатиметься розблокувати сховище V_A використовуючи свій власний набір, йому це вдасться, якщо множини A та B значно перетинаються. З іншого боку, будь-який, хто намагатиметься розблокувати сховище V_A за множиною даних, що істотно відрізняються від набору Аліси, зазнає невдачі. Таким чином, нечітке сховище можна розглядати як схему перевірки помилок, у якій ключі складаються з наборів.

На думку авторів, їхня система може знайти застосування системах, в яких безпека залежить від людських чинників. Наприклад, нечіткі сховища можуть знайти застосування:

1) для захисту конфіденційних даних. У такому випадку, схема може використовуватися для кола людей (наприклад, сім'ї), що володіють деякими схожими параметрами, щоб зберегти деякі дані в таємниці;

2) для відновлення пароля або інших даних. Зараз поширена практика, що для відновлення пароля при реєстрації в системі користувач вигадує відповіді на деякі стандартні запитання, потім в разі відновлення пароля йому необхідно дати відповіді на ці запитання, тобто сформувати деякий набір даних, які ідентифікують системі цього користувача. Оскільки дана схема може бути застосована до набору даних, то можливо її використання для відновлення пароля користувача навіть з урахуванням того, що користувач міг дати неправильні відповіді на кілька запитань;

3) біометрія. Нечіткі сховища можна застосовувати щодо біометричних зразків. Наприклад, як ключ шифрування. Користувач 1 міг би зберігати пароль, заблокований в нечіткому сховище і зашифрований на її наборі даних отриманих з її біометричного зразка, наприклад, відбитка пальця, тим самим забезпечуючи стійкість системи до помилок і конфіденційність, даних що зберігаються в системі.

3.2.4 Захисна функція

Захисна функція або схема допоміжних даних була розроблена для забезпечення безпеки збережених біометричних даних і гарантування конфіденційності законних користувачів [11-14]. Цей підхід дозволяє системі автентифікації перевіряти ідентичність користувача без будь-яких знань про біометричні дані користувача. Дельта-договірні і епсілон-виявляючі функції забезпечують основу цієї схеми. Функція дельта-контрактування пов'язує таємницю з біометричними даними, а функція епсилон-виявлення гарантує, що захищений шаблон відкриває лише невелику кількість інформації про випадкові та біометричні дані.

Захисна функція не стійка до атак типу спуфінг та атак грубою силою. Попередні реалізації схем такого типу виробляють ключі, які менше 50 біт.

Це не відповідає мінімальним вимогам для біометричних ключів. Також такі системи сприйнятливі до атак з використанням кратності записів і перехресного нападу. Більш того, зловмисник може використовувати реконструйований секрет для отримання оригінальних біометричних даних з компрометованих допоміжних даних. Схематичне зображення біометричної криптографічної системи наведено на рис. 3.7.

Порівняння переваг та недоліків біометричних криптографічних систем зі зв’язуванням ключа наведено в табл. 3.1.

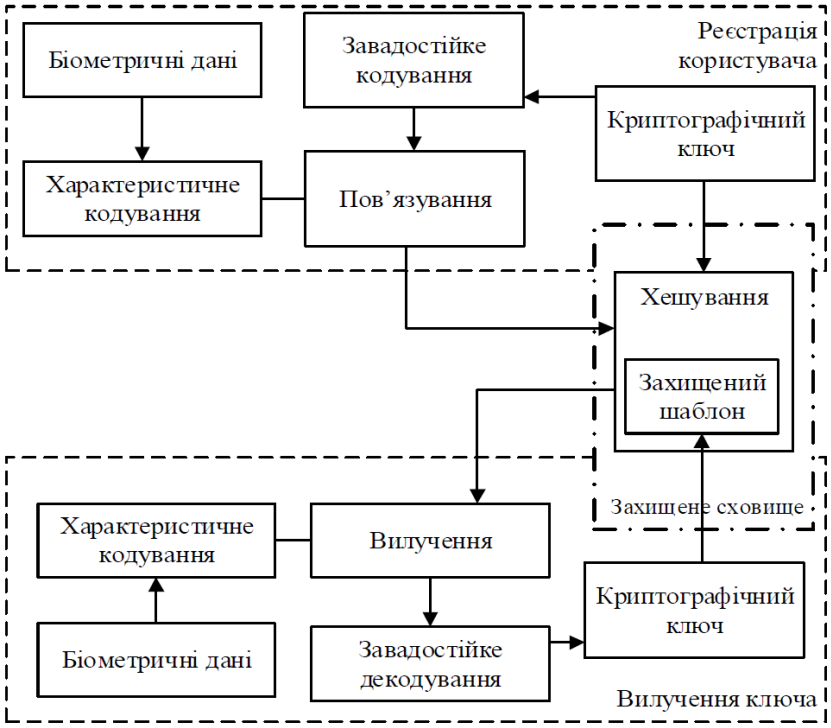


Рисунок 3.7 – Схематичне зображення біометричної криптографічної системи зі зв'язуванням ключа: схема захисної функції

3.3 Біометричні криптосистеми з генерацією ключа

У такій біометричній криптосистемі ключ формується безпосередньо з біометричних даних користувача і не зберігається в базі даних [11-14, 17]. Можливість не зберігати ключ, отриманий з біометричних даних, є незаперечною перевагою методу генерації криптографічних ключів з біометричних даних користувача порівняно з іншими існуючими методами.

Таблиця 3.1 – Порівняльний аналіз біометричних криптографічних систем зі зв’язуванням ключа

Схема	Переваги	Недоліки
Схема біометричного шифрування	1. Застосовує стандартний криптографічний алгоритм для створення безпечного біометричного шаблону 2. Зловмисник не має можливості розшифрувати захищені шаблони без знання алгоритму і криптографічного ключа	1. Існує можливість використання реконструйованого секрету для отримання оригінальних біометричних даних із захищеного шаблону 2. Не стійкі до атак змішаної заміни, атак сходження (атака маскарад) і атак найближчого самозванця, атак множинного запису
Схема нечітких зобов’язань	"Зобов'язання", отримані з біометричних даних і секретного ключа, захищають біометричний шаблон. Також секретний ключ захищений завдяки тому, що зберігається лише його хеш-значення	1. Вразливі перед усіма відомими атаками на завадостійке кодування (залежить від обраного алгоритму кодування) 2. Не стійкі до атак сходження, атак грубою силою, атак декодування та перехресних атак
Схема нечітко-го сховища	Сховище не може бути декодовано без біометричних даних, які мають майже ідентичні характеристики з первинними	1. Сприйнятливі до атак грубою силою та колізій 2. Вразливі до атак вторгнень, атак зв'язків, комбінованих та ін'єкційних атак
Схема захисної функції	1. Допоміжні дані та хеш-функції захищають від відтворення біометричні дані та випадкові секрети відповідно 2. Оригінальні біометричні дані не можуть бути відновлені з захищеного шаблону без знання секретного ключа	1. Коротка довжина ключів, що отримуються 2. Можливість використання реконструйованого секрету для отримання оригінальних біометричних даних із компрометованих допоміжних даних 3. Не стійкі до атак грубою силою та перехресних атак, до атак множинного запису

Таким чином, головною відмінністю двох останніх видів біометричних криптосистем є те, що в одному з них криптографічний ключ тільки закривається за допомогою біометричного зразка, а в іншому ключ генерується безпосередньо з біометричних даних користувача. Схематичне подане такої системи наведено на рис. 3.8.

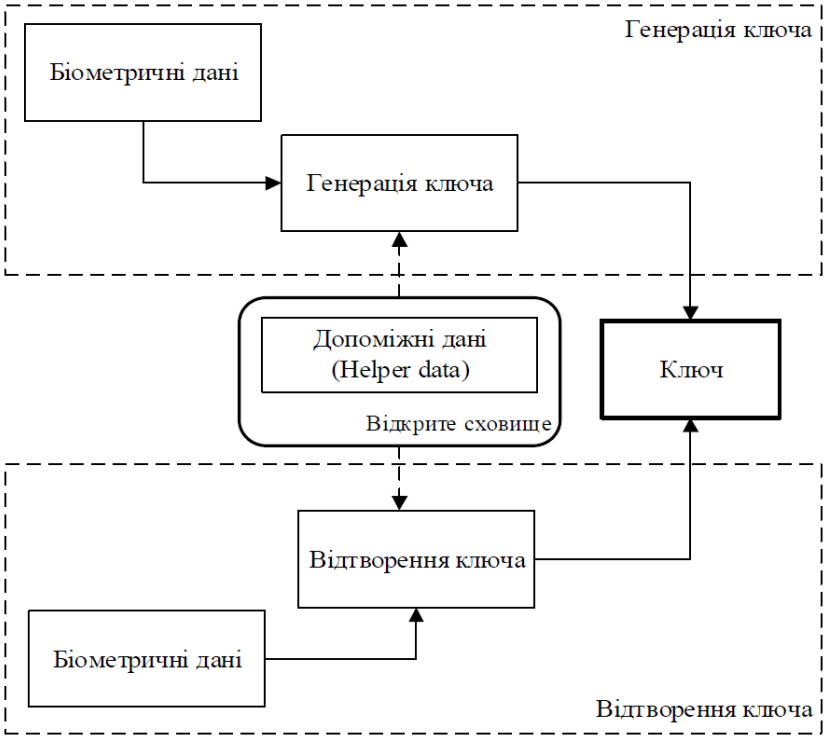


Рисунок 3.8 – Схематичне зображення біометричної криптографічної системи з генерацією ключа

Такі системи є більш безпечними, але їх важко застосовувати через навіть незначну мінливість біометричних характеристиках, оскільки необхідно з приблизно схожих даних генерувати той самий ключ знову і знову. Також недоліком таких систем є неможливість (або обмеженість кількості можливостей) сформувати новий ключ. Отже, якщо криптографічний ключ колинебудь буде скомпрометований, то використання цього конкретного біометричного образу та конкретного алгоритму генерації ключа буде неможливе. У системі, де потрібне періодичне оновлення криптографічного ключа, це неприйнятно.

3.3.1 Нечіткі екстрактори

Найпоширенішою технологією, на якій базуються біометричні криптографічні системи з генерацією ключа, – це нечіткі екстрактори (НЕ) [17-19]. Базова логіка використання нечітких екстракторів схожа з логікою нечітких сховищ. Даний спосіб дозволяє однозначно відновлювати секретний ключ з неточно відтворюваних (зашумленних) біометричних даних. Метод нечітких екстракторів передбачає формування випадкової рівномірно розподіленої послідовності з початкових даних і подальше коректне її відновлення з будь-яких даних, досить схожих з початковими. Такі методи базуються на теорії інформації та завадостійкого кодування. Використовування методу нечітких екстракторів здатне компенсувати помилки, що виникають внаслідок технічної неможливості отримання однакових значень біометричних характеристик під час їхнього повторного введення користувачем.

Метод нечітких екстракторів дозволяє отримувати ключ, який задовольняє всі критерії якості криптографічних ключів. У деяких реалізаціях передбачається формування ключа шляхом об'єднання допоміжних даних (отриманих з даного біометричного шаблону) та самого біометричного зразка. Допоміжні дані можуть бути отримані з заданого біометричного еталону і зберігатися у вигляді поновлюваного ключа або хеш-значення.

Загальна концепція побудови такого генератора криптографічних ключів полягає в наступному. Спочатку випадковим чином генерується бітова послідовність, яка кодується завадостійким кодом. Як завадостійкий код, що виправляє помилки, можуть використовуватися коди Хеммінга, Адамара, Боуза-Чоудхурі-Хоквінгема (БЧХ-коди), Ріда-Соломона (є окремим випадком БЧХ). Згенерована бітова послідовність може бути призначена для ідентифікації, автентифікації або генерації криптографічних ключів шифрування. Дана послідовність об'єднується з еталонними характеристиками біометричних ознак суб'єкта (біометричних еталоном).

Способи об'єднання можуть бути різними: від додавання за модулем 2 до використання алгоритмів, що більше орієнтовані на оброблювані дані. Ре-

зультатом об'єднання є відкритий рядок, який може зберігатися на загальнодоступному сервері. Щоб отримати згенеровану раніше послідовність (криптографічний ключ) користувач вводить власні біометричні ознаки, які обробляються відповідним чином і «віднімаються» з відкритого рядка. Після вилучення біометричних даних отримана бітова послідовність буде змінена внаслідок нечіткості введених біометричних даних відносно еталонних. Після застосування коду, що виправляє помилки до отриманого рядка, в разі високого ступеня «схожості» представленого біометричного образу і еталонного (тобто, якщо кількість розбіжних біт еталонних і висунутих даних не перевищує виправлячу здатність коду), буде відновлена послідовність бітів, яка і є криптографічним ключем. Описаний метод схематично зображено на рис. 3.9.

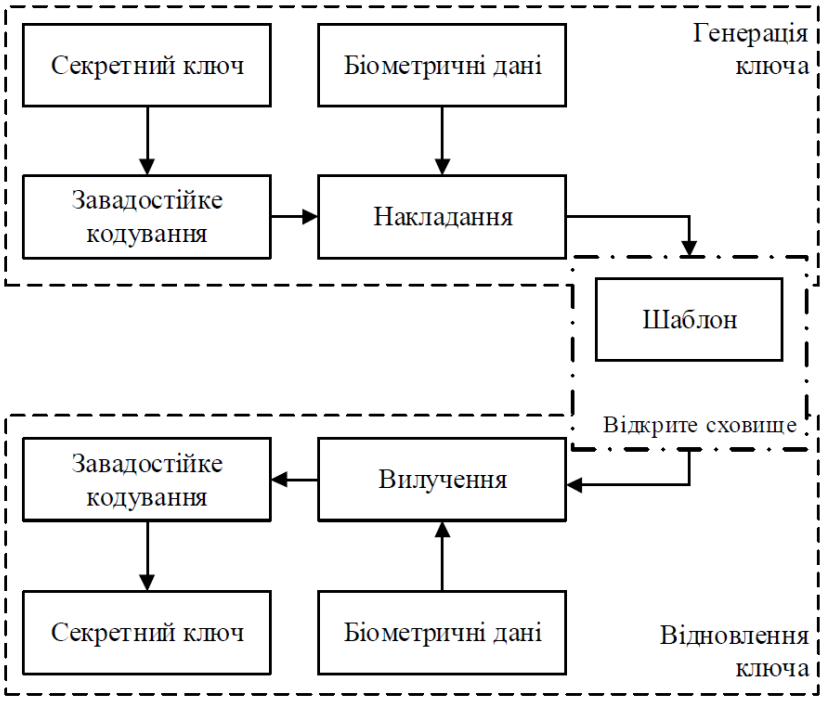


Рисунок 3.9 – Схематичне зображення методу нечітких екстракторів

Два основних підходи, що використовуються для генерації біометричних ключів – схема приватного шаблону та схема квантування.

У схемах приватного шаблону (англ. Private template scheme) [17-19] використовуються допоміжні дані – послідовності бітів перевірки для виправлення помилок завадостійким кодом. Сам ключ формується безпосередньо з

біометричного образу або з хешу цього біометричного образу. Наведемо як приклад алгоритм схеми приватного шаблону, в якій ключ формується з хешу.

Алгоритм генерації ключа:

1. До біометричного образу довжиною M біт, застосовується завадостійке декодування. У результаті формується вектор $Vec(V) = (V_1, V_2, \ldots, V_n)$ для n-бітного коду.

2. Отриманий після декодування характеристичний вектор $Vec(T)$ поєднується з вектором контрольної суми $Vec(C)$, тобто $Vec(T) \cup Vec(C)$, де вектор $Vec(C)$ є частиною коду, виправляючого помилки.

3. Для формування ключа виконується хешування вектору $Vec(T) \cup Vec(C)$ та, залежно від реалізації, з допоміжними даними:

$$Key = Hash[Vec(T) \cup Vec(C), helper\_data].$$

Алгоритм відтворення ключа:

1. До біометричного образу довжиною M біт, застосовується мажоритарне декодування. Формується вектор $Vec(V') = (V_1', V_2', \ldots, V_n')$ для n-бітного коду.

2. Отриманий після декодування характеристичний вектор $Vec(T')$ поєднується з вектором контрольної суми $Vec(C)$, тобто $Vec(T') \cup Vec(C)$, де вектор $Vec(C)$ є частиною коду, виправляючого помилки.

3. Для формування ключа виконується хешування $Vec(T') \cup Vec(C)$ та, залежно від реалізації, з допоміжними даними:

$$Key = Hash[Vec(T') \cup Vec(C), helper\_data].$$

Відтворений ключ можна використовувати за призначенням.

Схематичне зображення такого алгоритму наведено на рис. 3.10. Експериментальні результати та аналіз безпеки показують, що схема приватних шаблонів є простою та ефективною, також слід зазначити, що під час використання такої схеми відновлення початкових біометричних даних із захищених шаблонів неможливе.

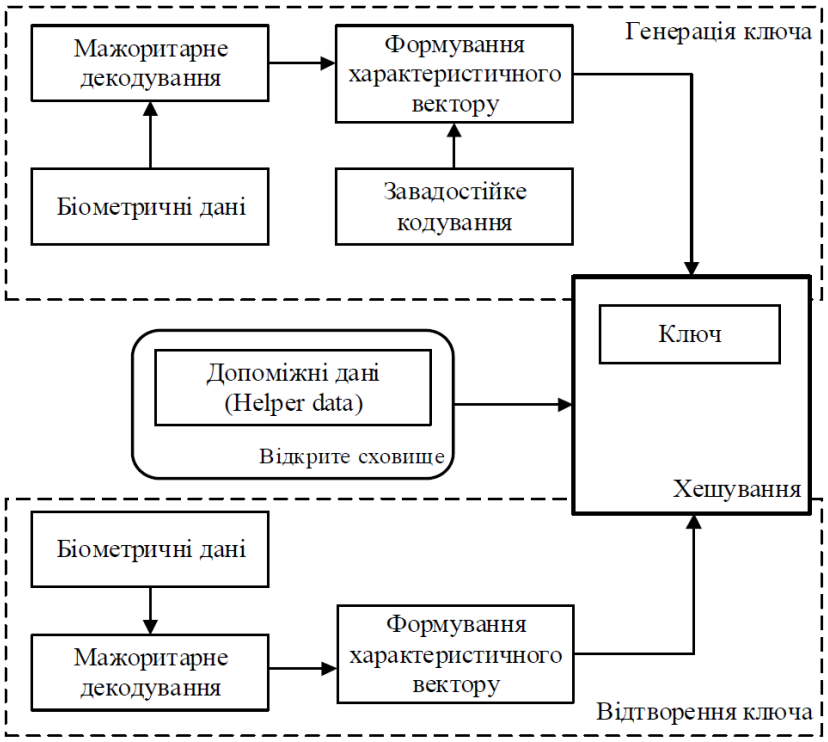


Рисунок 3.10 – Схематичне зображення біометричної криптографічної системи з генерацією ключа: схема приватного шаблону

Схеми квантування (англ. Quantization scheme) [17-19] створюють біометричні ключі, використовуючи допоміжні дані та бінаризовані (або квантовані) біометричні характеристики. Унікальною особливістю схем квантування є можливість отримувати одні і ті самі ключі з досить різноманітних біометричних образів людини, навіть якщо вони отримані за допомогою різних сканерів. Схематично функціонування схеми квантування подано на рис. 3.11.

Схеми квантування можуть бути реалізовані як мультимодальні системи; тобто унікальний ключ може бути отриманий з об'єднання двох або більше біометричних метрик.

Слабкістю схем квантування на основі допоміжних даних є можливість відновлення оригінальних біометричних зображень із захищених шаблонів. Зловмисник може отримати характеристичні вектори з захищених шаблонів, а потім відновити реальний біометричний образ. Схеми квантування, які використовують допоміжні дані, вразливі для атаки за допомогою множинності

записів. Отже, існує потреба в мінімізації обсягу корисної інформації, яка може бути доступна зловмиснику, якщо система буде скомпрометована.

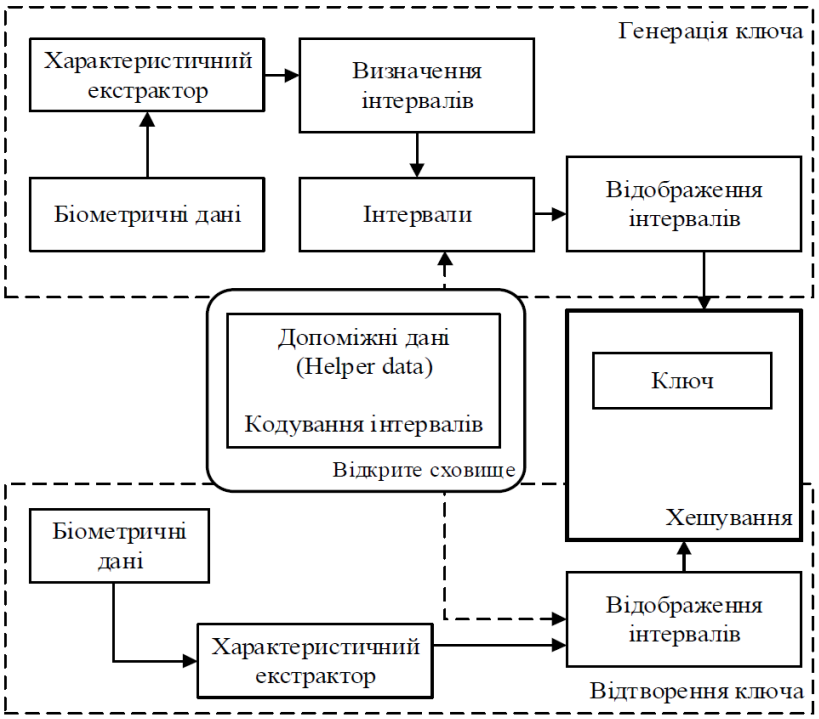


Рисунок 3.11 – Схематичне зображення біометричної криптографічної системи з генерацією ключа: схема квантування

Для функціонування схеми квантування необхідні характеристичні вектори декількох біометричних зразків для обчислення відповідних інтервалів для кожного елемента характеристики (необхідні характеристичні вектори з реальними значеннями). Ці інтервали кодуються та зберігаються у вигляді допоміжних даних. Під час ідентифікації знову фіксуються біометричні характеристики суб'єкта та відображаються у попередньо визначені інтервали, генеруючи хеш-ключ. Для того, щоб забезпечити оновлюванні ключі або хеші, більшість схем забезпечують параметризоване кодування інтервалів.

Схеми квантування дуже пов'язані з захисними функціями (англ. shielding function), оскільки обидва методи виконують квантування біометричних характеристик шляхом побудови відповідних інтервалів функцій. На відміну від захисних функцій, загальні схеми квантування визначають інтервали для кожної окремої біометричної характеристики, виходячи з її дисперсії.

Це дає змогу покращувати коректування збережених допоміжних даних до характеру застосованої біометрії.

Таблиця 3.2 – Порівняльний аналіз біометричних криптографічних систем з генерацією ключа на основі нечітких екстракторів

	Переваги	Недоліки
Схема приватного шаблону	1. Формує конкретні ключі безпосередньо з біометричних даних 2. Забезпечує захист шаблонів та конфіденційність користувачів, оскільки біометричні дані відсутні в системі автентифікації. 3. Використання сильних хеш-алгоритмів для генерації випадкових ключів з біометричних даних забезпечує криптографічну стійкість до атак грубою силою	Ключі не підлягають оновленню в разі компрометації
Схема квантування	1. Генерує біометричні ключі, використовуючи допоміжні дані та квантовані біометричні характеристики. 2. Можливо відновлювати одні і ті самі ключі з декількох екземплярів біометричних даних, отриманих навіть від різних джерел (сканерів, датчиків) 3. Забезпечує безпеку та конфіденційність, оскільки не зберігає інформацію про користувача, таку як біометричні дані.	Вразлива для атаки через множинність запису

До принципових недоліків нечітких екстракторів відносять:

1. Усі класичні коди вносять надмірність. В нечіткому екстракторі довжина ключа жорстко залежить від коректуючої здатності коду. Наприклад, при виправленні 14 % помилок за допомогою найбільш ефективних на сьогодні коректуючих кодів надлишкова частина відкритого рядка (додаткова ін-

формація, що зберігається у відкритому вигляді та необхідна для генерації ключа) складе 1600 % [20]. Отже, довжина ключа в 17 разів менше довжини відкритого рядка.

2. Класичні коди не можуть виправити велику кількість помилок, тому їх неможливо використовувати разом із малоінформативними біометричними характеристиками.

3. Нечіткі екстрактори не навчаються та квантують «сирі» біометричні дані, не враховуючи особливості простору ознак.

3.3.2 Нейромережеві перетворювачі біометрія-код

В алгоритмах нейромережевих перетворювачів біометрія-код (НПБК) використовується багатошарова штучна нейронна мережа. У процесі навчання нейронної мережі вхідними значеннями є значення біометричних параметрів (БП) прикладів біометричного образу «Свій» та значення БП прикладів біометричних образів «Чужий». При цьому вихідними значеннями нейронної мережі для прикладів біометричного образу «Свій» є значення послідовності ключової інформації, яка представляє криптографічний ключ «КК». Для прикладів біометричних образів «Чужою» вихідними значеннями є значення послідовності випадково згенерованої інформації, що не збігається із заздалегідь сформованою ключовою інформацією. Для відновлення ключової інформації при тестуванні та використанні навченої нейронної мережі надаються тестові значення БП біометричного образу «Свій» та архітектура навченої нейронної мережі (кількість шарів, нейронів, вагові коефіцієнти тощо). У цьому випадку, якщо користувач має БП біометричного образу "Чужий", то нейронною мережею формується марна послідовність випадкових значень, а не ключова інформація.

Перевагою НПБК в порівнянні з «нечітким екстрактором» є процедура збагачення. Збагачення дозволяє працювати з «поганими біометричними даними» та відновлювати до 50 % помилок вихідних даних [21].

Таблиця 3.3 – Переваги та недоліки перетворювачів біометрія-код

Переваги НЕ	Недоліки НЕ	Переваги НПБК	Недоліки НПБК
Не вимагає наявності в базі даних біометричних образів «Чужий»	Відносно високі показники помилок 1-го та 2-го родів	Відносно низькі показники помилок 1-го та 2-го родів	Потребує наявності в базі даних біометричних образів «Чужий»
Криптографічний ключ і біометричні параметри не зберігаються в базі даних	Висока надмірність коректуючих кодів, в результаті погана якість роботи при високому ступені розкиду значень біометричних параметрів	Криптографічний ключ і біометричні параметри не зберігаються в базі даних	Ресурсні витрати, складна програмна реалізація
Не вимагає наявності великої довжини послідовності, що описує біометричний параметр	Фіксована кількість розрядів (біт), що визначають значення біометричного параметру	Невимогливий до процесу відбору якісних біометричних параметрів	Вимагає наявності досить великої довжини послідовності, що описує біометричний параметр
Простий у реалізації	Відносно низька стійкість до зміни значень біометричного параметру з плином часу	Відносно висока стійкість до зміни значень біометричного параметру з плином часу	Складність реалізації системи
	Можливість перебору значень послідовності, що описує біометричний параметр, для фальсифікації ключа доступу		

3.4 Висновки

Людський фактор відіграє важливу (якщо не вирішальну) роль в проблемі захисту інформації від несанкціонованого доступу. Тому криптографічні засоби захисту інформації поєднують з біометричними, оскільки біометричні ознаки дозволяють «прив'язати» криптографічний ключ чи пароль до особистості суб'єкта.

Статичні біометричні образи дозволяють реалізувати надійну зв'язку ключ-суб'єкт при високому значенні довжини ключа, але мають обмеження

на кількість еталонних образів для однієї людини (кількість пальців, очей тощо), а також дозволяють виготовити фальсифікат ознак. Динамічні образи дають широкі можливості щодо вибору еталонного образу (наприклад, рукописний пароль можна змінити) при більш низькій надійності та довжині ключа. Використання пароля на основі параметрів клавіатурного почерку дає ряд переваг: є можливість прихованого отримання ознак, не потрібне спеціальне обладнання, не викликає психологічної неприязні.

Основною перевагою нечітких екстракторів у задачі формування криптографічного ключа на основі біометричних параметрів клавіатурного почерку є те, що в базі даних не зберігається криптографічний ключ, а лише допоміжна інформація для формування криптографічного ключа. Таким чином, інформація може бути розшифрована тільки при повторному наданні біометричних параметрів справжнім користувачем, який може зберігати ключову фразу, набрану на клавіатурі або вимовлену в мікрофон, в секреті. Нечіткі екстрактори можуть бути застосовані не тільки у задачі формування криптографічного ключа, але також у задачі аутентифікації та формування електронного цифрового підпису.

4 ПРОПОНОВАНИЙ АЛГОРИТМ ГЕНЕРАЦІЇ ПАРОЛІВ ДЛЯ КРИПТОГРАФІЧНИХ СИСТЕМ НА ОСНОВІ КЛАВІАТУРНОГО ПОЧЕРКУ

Традиційним методом захисту від несанкціонованого доступу є шифрування. Сучасні алгоритми шифрування надають досить високий рівень безпеки. Однак питання вибору ключів для асиметричного та симетричного шифрування, а також їх захисту під час зберігання та передачі досить остаточно не вирішені. Якщо знайти стійкі перетворення для здійснення однозначної та невід'ємної «прив'язки» ключа для шифрування до біометричних характеристик кожної конкретної особи, ці питання можна буде вважати закритими.

4.1. Досягнення в області генерації ключів на основі біометричних параметрів людини

Показниками надійності генерації ключа є ймовірності помилки першого роду (FRR – False Rejection Rate, розбіжності ключа, що генерується з біометричних ознак одного й того самого користувача) та другого роду (FAR – False Accept Rate, збіг ключів, що генеруються з ознак двох різних користувачів). Коефіцієнтом рівноймовірної помилки EER називається загальний відсоток (імовірність) помилкових рішень, якщо $EER = FRR = FAR$.

Аналітичний огляд методик генерації ключа показав низьку кількість робіт, що описують способи генерації ключів на основі параметрів клавіатурного почерку. Відомі системи генерації ключа на основі відбитка пальця [22-23], райдужної оболонки ока [24-26], геометрії обличчя суб'єкта [27-28], рукописного підпису [29-31], голосу [32], клавіатурного почерку [33], а також мультифакторні системи [34-38].

Таблиця 4.1 – Показники надійності генерації ключа

Тип задачі	Тип біометричного параметру	Вихідні дані експериментів	Тип ПБК	Середня оцінка якості роботи перетворювачів
Формування ключа	Голосовий відбиток	10 випробуваних; всього 100 дослідів	НПБК	FRR+FAR=0.16
		60 випробуваних по 50 спроб введення; 9000 реалізацій публічних, 6000 секретних парольних фраз		FRR=0.188 (публічна, у секреті); FAR=0.044-0.091 (у секреті); FAR=0.156-0.214 (публічна); FRR=0.14-0.151 FAR=0.101-0.153 (60 с)
	Клавіатурний почерк	80 випробуваних по 50 спроб введення; 3 публічні парольні фрази (всього 12000 реалізацій), одна в секреті (всього 4000 реалізацій), моніторинг (9000 символів)		FRR=0.064-0.104; FAR=0.009-0.01 (в секреті); FAR=0.021-0.025 (публічна); FRR.=0.061 FAR=0.023 (1500 символів)
	Динамічний рукописний підпис	-		FRR = 0,089 FAR=0,096
		65 випробуваних по 50 спроб введення	НПБК, мережі квадратичних форм	FRR=0.0288-0.045 FAR=0.0232-0.039 (НПБК); FRR=0.148 FAR=0.05 (НЕ)
	Біометрія обличчя	-	НПБК	EER=0,069
		70 піддослідних, зйомка тривалістю 30-60 сек.	НПБК, НЕ	FRR=0.032 FAR=0.014 (НЕ); FRR=0.0039-0,014 FAR=0.0022-0.029 (НПБК)
	Мультифакторна система (клавіатурний почерк, біометрія обличчя)	100 піддослідних при моніторингу тривалістю 1 годину	НПБК	FRR=0.002; FAR=0.0036 (30 с); FRR=0.002; FAR=0.0009 (60 с); FRR<0.0005 FAR<0.0005 (150 с)

Продовження таблиці 4.1

Тип задачі	Тип біометричного параметру	Вихідні дані експериментів	Тип ПБК	Середня оцінка якості роботи перетворювачів
Аутентифікація	Динамічний рукописний підпис	280 оригінальних підписів одного випробуваного, 1281 фальсифікацій підпису семи випробуваних	Нечіткі класифікатори	FRR=0.0057-0.038 FAR=0.0016-0.005
Верифікація	Динамічний рукописний підпис, голосовий відбиток	90 випробуваних, загальна кількість реалізацій 10000, період випробувань для кожного випробуваного терміном на 1 місяць	Штучні нейронні мережі	EER=0.023-0.043 FRR=0.17 FAR<0.001 (рукописний); EER=0.065-0.092 FRR=0.34 FAR<0.001 (голосовий)
Ідентифікація	Мультифакторна система (голосовий відбиток, клавіатурний почерк, динамічний рукописний підпис)	10 незареєстрованих користувачів зі 100 спробами введення; зразки 60 зареєстрованих користувачів по 10 спроб введення	Теорема Байєса	FRR=0.03 FAR=0.001

Як можна бачити з табл. 4.1, показники надійності генерації ключа на основі статичних біометричних ознак (відбиток пальця, райдужка) становлять порядку: $FRR = 0.005 - 0.055$ і $FAR \approx 0$. Довжина генерованого ключа становить 140-327 біт. Для динамічних біометричних ознак (підпис, клавіатурний почерк) ці показники орієнтовно дорівнюють: $FRR = FAR \approx 0.09 - 0.12$ при довжині ключа до 100 біт. Не рекомендується використовувати у цих системах голосовий відбиток (загроза копіювання біометричних образів, низькі показники якості роботи ПБК), відбитки пальців (неможливість зміни біометричного образу). Доцільно використовувати насамперед динамічний рукописний почерк та мультифакторні системи, що включають даний тип БП (високі показники якості роботи ПБК, можливість зміни біометричного образу та зберігання його в секреті).

4.2. Біометричні ознаки клавіатурного почерку

Ідентифікація користувача за клавіатурним почерком, як і генерація на його основі ключа (який також може бути використаний для ідентифікації), має ряд привабливих моментів. По-перше, не потрібне спеціальне обладнання. По-друге, введення пароля чи парольної фрази – звичний та основний спосіб підтвердження особистості користувача у комп'ютерних системах.

Зазвичай у якості ознак клавіатурного почерку використовуються часові інтервали між натисканням клавіш ($p_{key1,key2}$), що характеризують темп роботи з клавіатурою, і часові інтервали утримання клавіш (t_{key}), що характеризують стиль роботи з клавіатурою. Інформативність парольної фрази визначається її довжиною. Часові інтервали містять інформацію про користувача, який має формований клавіатурний почерк.

4.3 Метод нечітких екстракторів

Як було зазначено в третій главі нечітким екстрактором називають метод (або загальний алгоритм), що виділяє випадкові, рівномірно розподілені послідовності бітів з біометричних даних в умовах зашумленості.

Спочатку випадковим чином генерується бітова послідовність, яка кодується завадостійким кодом. Згенерована послідовність поєднується з еталонними характеристиками біометричних ознак користувача (біометричним еталоном),. Спосіб об'єднання зазвичай – додавання за модулем 2. Результат об'єднання – послідовність бітів (відкритий ключ), який може зберігатися на загальнодоступному сервері. Щоб отримати згенеровану раніше послідовність (ключ) користувач вводить нову реалізацію біометричних ознак, яка обробляється відповідним чином і віднімається з відкритого ключа. Після віднімання біометричних даних отримана бітова послідовність буде змінена внаслідок відмінності пред'явлених біометричних даних від еталонних. Після застосування коректуючого коду у разі високого ступеня «схожості» пред'явленого біометричного образу і еталонного (тобто якщо кількість неспівпадаючих біт не перевищує коректуючу здатність коду), буде отримано вірний ключ (S1 та S9 на рис. 4.1). На практиці можна здійснювати хешування відновлюваного рядка, якщо потрібно отримувати на виході рядок фіксованої довжини.

Таким чином, типова структура нечіткого екстрактора дозволяє проводити модифікації загального алгоритму за такими основними напрямками:

1) способи представлення еталонних та поточних значень біометричних ознак;

2) способи «об'єднання» і «віднімання» біометричної бітової послідовності та секретного паролю (ключа);

3) способи завадостійкого кодування і декодування.

Перший напрямок передбачає розробку способів округлення, трансляції, кодування та інших перетворень над значеннями ознак, результатом яких буде бітова послідовність, яка залежить від біометричних характеристик.

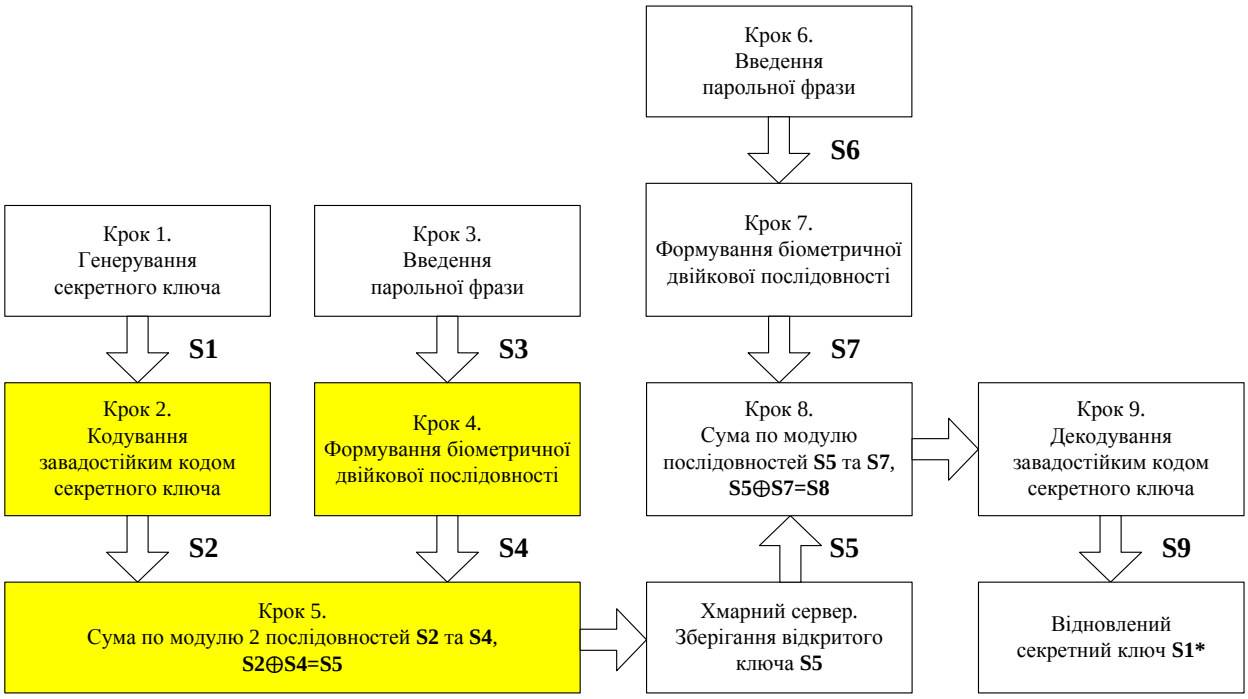


Рисунок 4.1 – Типова схема нечіткого екстрактору

Очевидно, що «сирі» біометричні дані здебільшого складаються з неінформативних елементів. Доцільно мінімізувати кількість нестабільних біт або ознак при їх перетворенні на бітову послідовність.

В пропонованому алгоритмі на першому кроці за допомогою процедури виключення грубих помилок (наприклад, «заліпла» клавіша. користувач задумався і припинив введення паролю тощо) виключаються значення часів натискання t та паузи p, що є викидами.

На другому кроці на основі N введених парольних фраз за наступними формулами розраховуються середні квадратичні відхилення (S), тобто ознаки стабільності, часів натискання на кожну клавішу та часів паузи між натисканнями:

$$S^{(i)} = \sqrt{\frac{1}{N-1}\sum_{n=1}^{N}\left(X_n^{(i)} - M_n^{(i)}\right)^2}, \tag{4.1}$$

де

$$M^{(i)} = \frac{1}{N}\sum_{n=1}^{N} X_n^{(i)}, \tag{4.2}$$

i – номер клавіші в парольній фразі; $X^{(i)}$ – значення ознаки (час утримання клавіші – $t^{(i)}$ чи час паузи – $p^{(i)}$); N – кількість використаних значень ознаки $t^{(i)}$ чи часу паузи $p^{(i)}$.

На третьому кроці множина розрахованих значень ознак ті $R = \left\{S_t^{(i)} \cup S_p^{(i)}\right\}$ ранжується за зростанням – формується вектор R_R. Далі вектор R_R скорочується – 25 % найбільших значень видаляються, бо вони характеризують 25 % найнестабільніших ознак клавіатурного почерку даного користувача.

На четвертому кроці формується біометричний еталон користувача – вектор E середніх значень часів утримання та паузи, причому їх послідовність визначається послідовністю членів вектору R_R.

На п’ятому кроці значення кожної складової вектору E трансформується в двійкове число, тобто квантується. Очевидно, що не всі біти, якими представлено значення довільної ознаки, є інформативними та значущими. Спочатку всі значення ознак представлені десятковими числами з різною областю значень. Щоразу при введенні даних значення ознаки кожного користувача змінюється (значно чи ні – все залежить від інформативності даного ознаки для даного користувача). Доцільно мінімізувати неінформативні біти або ознаки при їх перетворенні на бітову послідовність. Як вказано у попередньому розділі до вразливості нечітких екстракторів відносять наступну: нечіткі екстрактори, що здійснюють гамування «сирих» біометричних даних, виявляються без захисту від спостереження реальних багатовимірних статистик у просторах відстаней Хеммінга, середньої стабільності розрядів, модулів їх комбінацій. Якщо брати значення ознак у вихідному вигляді, змінюючи лише їхнє подання на двійкове, а потім накласти гаму (скласти за модулем 2 бітовий вектор з секретним ключем) для формування відкритого ключа, то атаку перебору значень ознак можна суттєво (багаторазово) прискорити, використовуючи різні техніки. Тому дуже важливо перетворювати «сирі» значення ознак перед гамуванням таким чином, щоб кількість помилок при по-

вторному введенні даних користувачем у бітовому векторі було мінімальним і було дуже складно виявити нестабільні області в бітовій послідовності, витягнутій з «сирих» біометричних даних.

В проведених дослідженнях було прийнято рішення використати три способи квантування значень ознак клавіатурного почерку виду $Y = f(x)$, де x – вхідне середнє значення $t^{(i)}$ чи $p^{(i)}$, а Y – відповідне двійкове число. Для першого способу вхідним x відповідає вісім значень $Y = \{0, 1, 3, 7, 15, 31, 63, 127\}$, для другого способу вхідним x відповідає 16 значень $Y = \{0, 1, 3, 7, 15, 31, 63, 127, 128, 192, 224, 240, 248, 252, 254, 255\}$, для третього Y – ціле число від 0 до 255. Далі всі значення Y замінюються відповідними двійковими послідовностями довжини 8 бітів.

На шостому кроці проводиться «склеювання» бітових послідовностей вектору E в одну результуючу послідовність.

На сьомому кроці двійкова біометрична послідовність об’єднується за модулем 2 зі згенерованою випадковою послідовністю для формування відкритого ключа. Отже, модифікації типової структури нечіткого екстрактора на кроці «об'єднання» і «віднімання» бітових послідовностей та рядка паролю (ключа) не проводилась.

Останній напрямок модифікації типової структури нечіткого екстрактора полягає у виборі оптимального алгоритму завадостійкого кодування та декодування. На цьому кроці потрібно забезпечити високий рівень відновлення ключа при найменшій надмірності коду. Потрібно знайти найбільш ефективний алгоритм та оптимальне співвідношення коректуючої здатності коду та інших параметрів, при яких ймовірності помилок 1-го та 2-го роду та надмірність завадодостійкого коду будуть найменшими. Стійкість генерованих ключів визначається їх довжиною і чим більша надмірність коду, тим довше закодований рядок і тим більше потрібно біометричних ознак, щоб «покрити» його цілком при «об'єднанні».

В проведених дослідженнях було прийнято рішення використати код Ріда-Соломона – циклічний коди, що дозволяє виправляти помилки в блоках

даних. Елементами кодового вектора є не біти, а групи бітів (блоки), що відповідає специфіці дослідної проблеми, коли кожен блок секретного ключа ладі об'єднується з блоком біометричної двійкової послідовності.

За умови, що коректуюча здатність коду Ріда-Соломона становить не більше $H/3$ (H – довжина інформаційної послідовності), надмірність коду складає не більше $(2/3)H$, тобто довжина кодової послідовності H^* на $2/3$ перевищить довжину H. Вважатимемо, що таке значення коректуючої здатності коду є максимальним у дослідженнях.

4.4. Оцінка ефективності способів генерації ключа на основі клавіатурного почерку

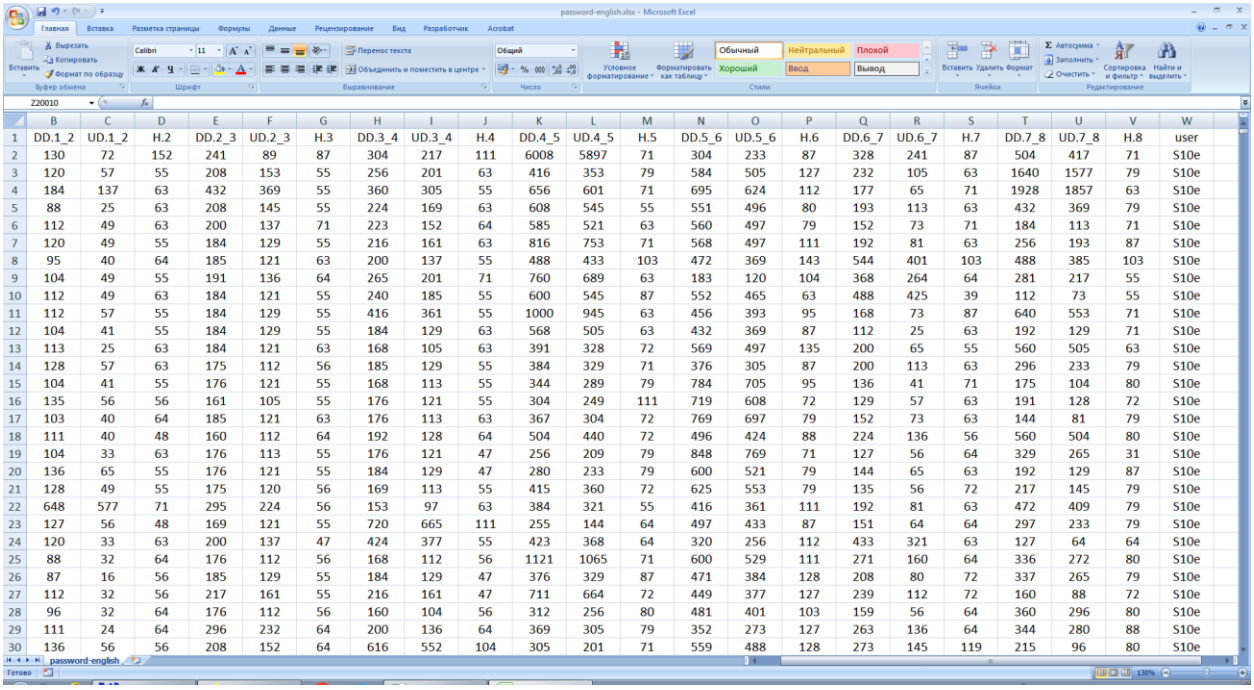
Математичний експеримент (див. рис. 4.2) проводився на базі датасету «Bilingual Keystroke Dynamics Dataset» [39], який складається з чотирьох датасетів. В дослідженнях використовувались два з них.

Перший датасет «BKSD Password-English» містить часові параметри вводу паролю «thug-173», який набирали 50 користувачів. Кількість вводів паролю – від 385 (користувач s15) до 400 (користувач s121) раз. Дані представляють файл Excel format з 23 стовпчиків (рис. 4.3). Поле «user» це ідентифікатор користувача. Останні 22 стовпчики – часові параметри (в секундах) вводу паролю: H.1, DD.1_2, UD.1_2, H.2, DD.2_3, UD.2_3, H.3, DD.3_4, UD.3_4, H.4, DD.4_5, UD.4_5, H.5, DD.5_6, UD.5_6, H.6, DD.6_7, UD.6_7, H.7, DD.7_8, UD.7_8, H.8. Тут «H.i» – час натискання клавіші i-ої клавіші паролю, «DD.i_j» – час між натисканням i-ої та j-ої клавіш паролю, «UD.i_j» – час між відпусканням i-ої клавіші та натисканням j-ої клавіші паролю.

Другий датасет «BKSD Phrase-English» містить часові параметри вводу парольної фрази «the queue shiver light false», яку набирали 35 користувачів. Кількість вводів парольної фрази – від 357 (користувач s76) до 400 (користувач s95) раз. Дані представляють файл Excel format з 46 стовпчиків. Поле «user» це ідентифікатор користувача. Останні 46 стовпчиків – часові параме-

три (в секундах) вводу парольної фрази: H.1, DD.1_2, UD.1_2, H.2, DD.2_3, UD.2_3, H.3, DD.3_4, UD.3_4, H.4, DD.4_5, UD.4_5, H.5, DD.5_6, UD.5_6, H.6, DD.6_7, UD.6_7, H.7, DD.7_8, UD.7_8, H.8, DD.8_9, UD.8_9, H.9, DD.9_10, UD.9_10, H.10, DD.10_11, UD.10_11, H.11, DD.11_12, UD.11_12, H.12, DD.12_13, UD.12_13, H.13, DD.13_14, UD.13_14, H.14, DD.14_15, UD.14_15, H.15, DD.15_16, UD.15_16, H.16. Тут «H.i» – час натискання клавіші i-ої клавіші парольної фрази, «DD.i_j» – час між натисканням i-ої та j-ої клавіш парольної фрази, «UD.i_j» – час між відпусканням i-ої клавіші та натисканням j-ої клавіші парольної фрази, порядковий номер клавіші визначається для послідовності «thequshivlighals».

Рисунок 3.2 – Схема експериментальних досліджень



	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	DD.1_2	UD.1_2	H.2	DD.2_3	UD.2_3	H.3	DD.3_4	UD.3_4	H.4	DD.4_5	UD.4_5	H.5	DD.5_6	UD.5_6	H.6	DD.6_7	UD.6_7	H.7	DD.7_8	UD.7_8	H.8	user
2	130	72	152	241	89	87	304	217	111	6008	5897	71	304	233	87	328	241	87	504	417	71	S10e
3	120	57	55	208	153	55	256	201	63	416	353	79	584	505	127	232	105	63	1640	1577	79	S10e
4	184	137	63	432	369	55	360	305	55	656	601	71	695	624	112	177	65	71	1928	1857	63	S10e
5	88	25	63	208	145	55	224	169	63	608	545	55	551	496	80	193	113	63	432	369	79	S10e
6	112	49	63	200	137	71	223	152	64	585	521	63	560	497	79	152	73	71	184	113	71	S10e
7	120	49	55	184	129	55	216	161	63	816	753	71	568	497	111	192	81	63	256	193	87	S10e
8	95	40	64	185	121	63	200	137	55	488	433	103	472	369	143	544	401	103	488	385	103	S10e
9	104	49	55	191	136	64	265	201	71	760	689	63	183	120	104	368	264	64	281	217	55	S10e
10	112	49	63	184	121	55	240	185	55	600	545	87	552	465	63	488	425	39	112	73	55	S10e
11	112	57	55	184	129	55	416	361	55	1000	945	63	456	393	95	168	73	87	640	553	71	S10e
12	104	41	55	184	129	55	184	129	63	568	505	63	432	369	87	112	25	63	192	129	71	S10e
13	113	25	63	184	121	63	168	105	63	391	328	72	569	497	135	200	65	55	560	505	63	S10e
14	128	57	63	175	112	56	185	129	55	384	329	71	376	305	87	200	113	63	296	233	79	S10e
15	104	41	55	176	121	55	168	113	55	344	289	79	784	705	95	136	41	71	175	104	80	S10e
16	135	56	56	161	105	55	176	121	55	304	249	111	719	608	72	129	57	63	191	128	72	S10e
17	103	40	64	185	121	63	176	113	63	367	304	72	769	697	79	152	73	63	144	81	79	S10e
18	111	40	48	160	112	64	192	128	64	504	440	72	496	424	88	224	136	56	560	504	80	S10e
19	104	33	63	176	113	55	176	121	47	256	209	79	848	769	71	127	56	64	329	265	31	S10e
20	136	65	55	176	121	55	184	129	47	280	233	79	600	521	79	144	65	63	192	129	87	S10e
21	128	49	55	175	120	56	169	113	55	415	360	72	625	553	79	135	56	72	217	145	79	S10e
22	648	577	71	295	224	56	153	97	63	384	321	55	416	361	111	192	81	63	472	409	79	S10e
23	127	56	48	169	121	55	720	665	111	255	144	64	497	433	87	151	64	64	297	233	79	S10e
24	120	33	63	200	137	47	424	377	55	423	368	64	320	256	112	433	321	63	127	64	64	S10e
25	88	32	64	176	112	56	168	112	56	1121	1065	71	600	529	111	271	160	64	336	272	80	S10e
26	87	16	56	185	129	55	184	129	47	376	329	87	471	384	128	208	80	72	337	265	79	S10e
27	112	32	56	217	161	55	216	161	47	711	664	72	449	377	127	239	112	72	160	88	72	S10e
28	96	32	64	176	112	56	160	104	56	312	256	80	481	401	103	159	56	64	360	296	80	S10e
29	111	24	64	296	232	64	200	136	64	369	305	79	352	273	127	263	136	64	344	280	88	S10e
30	136	56	56	208	152	64	616	552	104	305	201	71	559	488	128	273	145	119	215	96	80	S10e

Рисунок 4.3 – База даних «Bilingual Keystroke Dynamics Dataset»

Оскільки датасет «BKSD Password-English» містить 15 інформативних ознак для кожного введення парольної фрази (8 параметрів утримання клавіші та 7 параметрів часу паузи), то довжина біометричної двійкової послідовності складає $L_1 \leq [0.75 \cdot 15] \cdot 8 = 88$ бітів ([ ] – операція взяття цілої частини). Оберемо довжину біометричної двійкової послідовності $L_1 = 80$ бітів, що відповідає більш жорсткій умові – 70 відсотків (10 з 15) параметрів клавіатурного почерку віднесено до стабільних.

Оскільки датасет «BKSD Phrase-English» містить 31 інформативну ознаку для кожного введення парольної фрази (16 параметрів утримання клавіші та 15 параметрів часу паузи), то довжина біометричної двійкової послідовності складає $[0.75 \cdot 31] \cdot 8 = 184$ біти.

Оберемо довжину біометричної двійкової послідовності $L_2 = 200$ бітів, що відповідає менш жорсткій умові – 81 відсоток (25 з 31) параметрів клавіатурного почерку віднесено до стабільних.

На першому кроці за рівномірним законом генеруються ключові послідовності (секретні ключі). Оскільки для першого датасету довжина інформаційної послідовності H дорівнює 80 біт, тобто 80 бітів – це довжина комбіна-

ції, яку треба об’єднати з закодованим кодом Ріда-Соломона секретним ключем, то довжина генерованого секретного ключа повинна становити:

$$D_1 = \frac{3}{5} L_1 = \frac{3}{5} 80 = 48 \text{ бітів.}$$

Для другого датасету довжина генерованого секретного ключа повинна становити:

$$D_2 = \frac{3}{5} L_2 = \frac{3}{5} 200 = 120 \text{ бітів.}$$

На другому кроці біометричні дані подаються на вхід екстрактора, на виході якого відповідно до пропонованого в розділі 3.3 алгоритму формуються біометричні двійкові послідовності клавіатурного почерку користувачів довжиною 80 бітів та 200 бітів.

На третьому кроці шляхом підсумовування за модулем 2 закодовані кодом Ріда-Соломона секретні ключі та біометричні двійкові послідовності об’єднуються у відкриті ключі.

На четвертому кроці відбувається відновлення секретних ключів та їх порівняння з первинними. Помилкою першого роду вважається ситуація, коли система відновлює невірний для даного користувача ключа. Чим нижче FRR, тим вище стабільність алгоритму. Появи такої помилки на практиці означає, що користувач послуги не зможе розшифрувати дані або правильно підписати документ за допомогою ЕП. Помилкою другого роду вважається ситуація, коли ключі, отримані з біометричних даних двох різних користувачів, збігаються. У випадку такої помилки може бути здійснено несанкціонований доступ до зашифрованих даних або підроблено ЕП.

Як можна бачити з табл. 4.2, генерування ключа за достатньої надійності можна здійснити лише з урахуванням введення довгих парольних фраз. У випадку довжини ключа 120 бітів значення помилок 1-го роду та 2-го роду становлять 0.054 та 0.018 відповідно. У випадку довжини ключа 48 бітів значення помилок 1-го роду та 2-го роду становлять 0.086 та 0.052 відповідно.

Таблиця 4.2 – Генерування паролів на основі клавіатурного почерку

Позначення	Парольна фраза «thug-173»	Парольна фраза «the queue shiver light false»
Інформативних ознак	8 – час утримання клавіші; 7 – час паузи	16 – час утримання клавіші; 15 – час паузи
Довжина біометричної двійкової послідовності	80 бітів (33 % ознак виключено з аналізу, як нестабільні)	200 бітів (19 % ознак виключено з аналізу, як нестабільні)
Довжина секретного ключа	48 бітів	120 бітів
Кількість інформаційних / коректуючих символів в кодовій комбінації	48 / 32	120 / 80
Помилка 1-го роду **1-й спосіб квантування** **2-й спосіб квантування** 3-й спосіб квантування	 **0.106** **0.086** 0.128	 **0.032** **0.058** 0.025
Помилка 2-го роду **1-й спосіб квантування** **2-й спосіб квантування** 3-й спосіб квантування	 **0.131** **0.052** 0.941	 **0.085** **0.018** 0.047
Помилка 1-го роду **навчальна база – 10 записів** навчальна база – 30 записів **навчальна база – 50 записів** **навчальна база – 200 записів**	 **2.236** 0.688 **0.091** **0.086**	 **1.914** 0.348 **0.060** **0.058**
Помилка 2-го роду **навчальна база – 10 записів** навчальна база – 30 записів **навчальна база – 50 записів** **навчальна база – 200 записів**	 **1.924** 0.26 **0.055** **0.052**	 **0.414** 0.126 **0.023** **0.018**

Також можна відмітити, що навчальної бази з 50 спроб вводу парольної фрази достатньо для формування стабільного еталону клавіатурного почерку. Ситуація з кількістю рівнів квантування потребує додаткових досліджень. Попередні висновки: використання 8 рівнів квантування (1-й спосіб) сильно загрублює значення часових параметрів клавіатурного почерку, а використання 256 рівнів квантування, навпаки, сильно зашумлює дослідні характеристики.

4.5. Можливі шляхи підвищення точності перетворювачів клавіатурний почерк-код на основі нечіткого екстрактору

Отримані якісні показники генерування та відновлення секретного паролю на основі параметрів клавіатурного почерку та нечіткого екстрактору нижчі відповідних показників для НПБК (див. табл. 4.1). Розглянемо можливі шляхи підвищення ефективності дослідного алгоритму.

4.5.1 Способи подання еталонних та поточних значень ознак клавіатурного почерку

У роботі [40] показано зв'язок ефективності корекції помилок з методами групування бітів з різною ймовірністю одиничної помилки. Для підвищення якісних показників дослідного алгоритму можна застосувати процедуру індивідуальної оцінки інформативності ознак з урахуванням відносної частоти появи одиничних (або нульових) біт у перетвореному значенні ознаки. Під інформативністю мається на увазі інтегральний показник стабільності біт у перетвореному значенні ознаки. Запропоновану процедуру можна використовувати спільно з будь-яким способом відображення (перетворення) первинних значень ознак у бітову послідовність. До кожної ознаки по всіх відібраних до створення зразка перетвореним реалізаціям обчислюється відносна частота появи одиничних (чи нульових) біт. Наприклад, нехай введено 10 реалізацій, необхідно визначити показник інформативності для певної ознаки за її перетвореними значеннями:

$$00011111, 00111111, 00011111, 00001111, 00011111,$$
$$01111111, 00111111, 00011111, 11111110, 01111111.$$

Відносна частота появи одиничного біта в розрядах перетвореного значення становить:

$$0{,}1;\ 0{,}3;\ 0{,}5;\ 0{,}9;\ 1;\ 1;\ 1;\ 0{,}9.$$

Далі визначається інтегральна ймовірність появи одиничного біта у всіх розрядах, при цьому відносна частота береться як ймовірність, а ймовірності рівні 0 або 1 перетворюються на деяке число, наближене за значенням

до 0 і 1, але не рівне їм (щоб загальний добуток не став рівним нулю). Для розглянутого прикладу можна взяти значення 0.01 та 0.99:

$$0.1 \cdot (1 - 0.1) \cdot 0.3 \cdot (1 - 0.3) \cdot 0.5 \cdot (1 - 0.5) \cdot 0.9 \cdot (1 - 0.9) \cdot 0.99 \cdot$$
$$\cdot (1 - 0.99) \cdot 0.99 \cdot (1 - 0.99) \cdot 0.99 \cdot (1 - 0.99) \cdot 0.9 \cdot (1 - 0.9) =$$
$$= 0.1 \cdot (0.9) \cdot 0.3 \cdot (0.7) \cdot 0.5 \cdot (0.5) \cdot 0.9 \cdot (0.1) \cdot 0.99 \cdot (0.01) \cdot$$
$$\cdot 0.99 \cdot (0.01) \cdot 0.99 \cdot (0.01) \cdot 0.9 \cdot (0.1) =$$
$$= 0.00000000003713576847 75.$$

Чим більше розрядів матиме частоти, близькі до 0 або 1, тим менше вийде підсумковий добуток і тим вищою є інтегральна оцінка стабільності (інформативності) ознаки для користувача. Далі всі ознаки ранжуються за інформативністю (змінюється їх порядок – від самого інформативного до малоінформативного) і відбирається певна кількість ознак, інші відкидаються. Оптимальна кількість ознак, при якій ймовірності помилок 1-го та 2-го роду будуть найменшими – параметр екстрактора, який для кожної задачі буде різним. Кількість інформативних ознак та їх послідовність потрібно зберігати на окремому носії або виділеному сервері.

4.5.2 Способи «об'єднання» і «віднімання» біометричної бітової послідовності та секретного паролю

Зазвичай подібні способи зводяться до операції додавання по модулю 2, проте існують модифіковані способи на основі правил нечіткої логіки [41]. Нечіткий висновок може бути здійснений як відображення функції приналежності значення ознаки даному користувачу (функція приналежності повинна визначатися на основі функції щільності розподілу ознаки або бути їй рівною) на закодовану бітову послідовність. Однак за такого підходу потрібно зберігати допоміжну інформацію про функції приналежності ознак, фактично потрібно зберігати зразок чи докладну інформацію щодо його відновлення. Такий підхід зводить нанівець основну перевагу нечітких екстракторів – відсутність необхідності зберігання еталону. Тому в цьому випадку треба проводити додаткові дослідження.

4.6 Висновки

1. Досліджено модель перетворююча біометрія-код на основі нечіткого екстрактора та параметрів клавіатурного почерку. Сформовано вибірку біометричних образів користувачів на основі датасету «Bilingual Keystroke Dynamics Dataset», яка використовувалася надалі в ряді обчислювальних експериментів.

2. Алгоритми на основі нечіткого екстрактора мають декілька недоліків: довжина ключа жорстко залежить від корегуючої здатності коду, класичні коди не можуть виправити велику кількість помилок, нечіткі екстрактори квантують біометричні дані, не враховуючи особливості простору ознак. Запропоновано модифікації цього підходу.

3. Генерування ключа достатньої надійності можна здійснити лише у випадку введення довгих парольних фраз. У випадку довжини ключа 120 бітів (довжина паролю 16 символів) значення помилок 1-го роду та 2-го роду становлять 0.054 та 0.018 відповідно. У випадку довжини ключа 48 бітів (довжина паролю 8 символів) значення помилок 1-го роду та 2-го роду становлять 0.086 та 0.052 відповідно.

4. Також можна відмітити, що навчальної бази з 50 спроб вводу парольної фрази достатньо для формування стабільного еталону клавіатурного почерку. Ситуація з кількістю рівнів квантування потребує додаткових досліджень. Попередні висновки: використання 8 рівнів квантування (1-й спосіб) сильно загрублює значення часових параметрів клавіатурного почерку, а використання 256 рівнів квантування, навпаки, сильно зашумлює дослідні характеристики.

ВИСНОВКИ

1. Розглянуто основні стадії життєвого циклу документу в процесі змішаного документообігу, а також проведено аналіз основних загроз інформаційній безпеці на кожному із зазначених етапів. Найчастіше методами нейтралізації загроз виступають організаційно-технічні заходи, які не вирішують проблему «людського фактора» – недбалість, некомпетентність, несумлінність тощо. Використання надійних паролів та криптографічних ключів не виключає їх відчужуваності з цієї ж причини. Це призводить до фальсифікації юридично важливих документів та реалізації інших загроз (застосування сертифікованих засобів ЕП до шкідливого контенту, уникнення винними особами відповідальності). Одним з можливих рішень проблем документообігу, пов'язаних з «людським фактором», є комплексування криптографічних та біометричних методів аутентифікації.

2. Захищеність інформаційної системи визначається найслабшою ланкою в системі безпеки, тому в змішаному документообігу потрібно намагатись забезпечити приблизно рівний рівень захисту для документів на будь-яких видах носіїв за наявності одних і тих же реквізитів, що забезпечують їх автентичність. Неможливість автоматизованої перевірки цілісності та автентичності, а також застосування ЕП та інших криптографічних механізмів для «паперових» реалізацій документа призводить до більш низької захищеності документа при його розповсюдженні «на папері».

3. Розглянуто концепцію захисту гібридного документообігу, в якому:

1) наявна надійна прив'язка всіх аутентифікаторів суб'єкта (паролів, ключів шифрування та ЕП, кодів доступу тощо) до його біометричних характеристик;

2) з'являється можливість оперативно перевірити цілісність та автентичність документів незалежно від типу носія та відновити оригінал, якщо документ пошкоджений;

3) документи на всіх видах носіїв захищені від порушення конфіденційності;

4) забезпечується рівний захист документу, як в електронному, так і в паперовому вигляді (під рівним захистом мається на увазі використання однакових механізмів захисту для обох форматів документу).

4. Документ як активний елемент документообігу збагачується постійними та змінними атрибутами: мітка доступу, час внесення змін тощо. Для приховування цих метаданих можна використовувати алгоритми стеганографії. Для документу, одержуваного в електронному вигляді доцільно змінювати молодші біти в послідовності бітів, що кодують колір тесту – це не вносить надмірності в документ, не впливає на хеш-суму документу, тому повідомлення може бути вбудоване до формування ЕП; секретний ключ визначення символів, у яких приховані біти повідомлення, зашифрований відкритим ключем учасників групи, і може бути розшифрований лише особистим ключем авторизованого користувача. Для документа, отриманого у паперовому вигляді, доцільно ховати повідомлення у QR-кодах – обов'язкових реквізитах гібридного документа.

5. Досліджено модель перетворююча біометрія-код на основі нечіткого екстрактора та параметрів клавіатурного почерку. Сформовано вибірку біометричних образів користувачів на основі датасету «Bilingual Keystroke Dynamics Dataset», яка використовувалася надалі в ряді обчислювальних експериментів.

6. Алгоритми на основі нечіткого екстрактора мають декілька недоліків: довжина ключа жорстко залежить від корегуючої здатності коду, класичні коди не можуть виправити велику кількість помилок, нечіткі екстрактори квантують біометричні дані, не враховуючи особливості простору ознак. Запропоновано модифікації цього підходу.

7. Генерування ключа достатньої надійності можна здійснити лише у випадку введення довгих парольних фраз. У випадку довжини ключа 120 бітів (довжина паролю 16 символів) значення помилок 1-го роду та 2-го роду

становлять 0.054 та 0.018 відповідно. У випадку довжини ключа 48 бітів (довжина паролю 8 символів) значення помилок 1-го роду та 2-го роду становлять 0.086 та 0.052 відповідно.

8. Навчальної бази з 50 спроб вводу парольної фрази достатньо для формування стабільного еталону клавіатурного почерку. Ситуація з кількістю рівнів квантування потребує додаткових досліджень. Попередні висновки: використання 8 рівнів квантування (1-й спосіб) сильно загрублює значення часових параметрів клавіатурного почерку, а використання 256 рівнів квантування, навпаки, сильно зашумлює дослідні характеристики.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Діловодство й архівна справа. Терміни та визначення понять: ДСТУ 2732-2004 [Текст]. – Чинний від 2004-05-28. – К. : Держспоживстандарт України, 2005. – 31 с.

2. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 20.10.2023).

3. Кукарін О.Б. Електронний документообіг та захист інформації. Національна академія державного управління при презедентові України. 2019. URL: https://duikt.edu.ua/uploads/l_1504_14216152.pdf (дата звернення: 20.10.2023).

4. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 20.10.2023).

5. Башинська І.О. Глава 3.7 Основні порушники та загрози інформаційної безпеки промислових підприємств (с. 262-267) у міжнародній колективній монографії Problems of social and economic development of business: Collective monograph. – Publishing house «BREEZE», Montreal, Canada, 2014. – 408 p.

6. Hallé S. [etc.]. Decentralized enforcement of document lifecycle constraints // Information Systems. 2017.

7. ISO/IEC JTC 1/SC27 WD 24745–2006 Information technology – Security techniques – Biometric template protection.

8. Сідлецький, Є.В. Організаційні засоби захисту інформації в системах електронного документообігу / Є.В. Сідлецький; наук. керівник Т.А. Петренко // Новітні технології у науковій діяльності і навчальному процесі: зб. тез Всеукр. наук.-практ. конф. студентів, аспірантів та молодих учених (м. Чернігів, 8-9 квіт. 2020 р.): збірник тез доп. – Чернігів: НУ «Чернігівська

політехніка», 2020. – С. 144-146.

9. Коротка, Г.М. Аналіз складових інформаційної безпеки систем електронного документообігу / Г.М. Коротка; наук. керівник Т.А. Петренко // Новітні технології у науковій діяльності і навчальному процесі: зб. тез Всеукр. наук.-практ. конф. студентів, аспірантів та молодих учених (м. Чернігів, 8-9 квіт. 2020 р.): збірник тез доп. – Чернігів: НУ «Чернігівська політехніка», 2020. – С. 146-149.

10. Ali Evren Göksungur. Electronic Signature and Electronic Document Management Systems: Digital Revolution. Scholars' Press, 2018. 56

11. A. K . J ain, R . B olle, S. P ankanti. Biometrics: personal identification in networked society, 1999, Vol. 1, 434 p.

12. U. Uludag, S. Pankanti, S. Prabhakar, A. Jain. Biometric Cryptosystems: Issues and Challenges, Proceedings of the IEEE, June 2004, Vol. 92, NO. 6.

13. Anil K. Jain, Arun Ross. An Introduction to Biometric Recognition. IEEE Transactions on circuits and systems for video technology, 2004, Vol. 14, NO. 1. pp. 4–20.

14. A. Juels, M. Sudan. A fuzzy vault scheme. Des. Codes Cryptography, 2006, Vol. 38, NO. 2, pp. 237–257.

15. Juels A. fuzzy commitment scheme / A. Juels, M. Wattenberg. 6th ACM Conference on Computer Communications and Security, Singapore, 1999, pp. 28-36.

16. X. Boyen Reusable cryptographic fuzzy extractors / X. Boyen. 11th ACM Conference on Computer and Communications Security, USA, 2004, pp. 82–91.

17. Y. Dodis, R . Ostrovsky, L . R eyzin, A . Smith. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM Journal on Computing, 2008, Vol. 38, No. 1, pp. 97–139

18. G. Davida, Y. Frankel, B. Matt. On the relation of error correction and cryptography to an off-line biometric identification scheme. Proceedings of Workshop on Coding and Cryptography, Paris, France, 1999, pp. 129–138.

19 R. Sashank Singhvi, S. P. Venkatachalam, P. M. Kannan, V. Palanisamy. Cryptography key generation using biometrics. International Conference on Control, Automation, Communication and Energy Conservation (INCACEC), 2009, pp. 1–6.

20. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy// EUROCRYPT. April 13, 2004. P. 523–540.

21. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM Journal on Computing, 38(1):97–139, 2008.

22. Walport M. Distributed ledger technology: beyond block chain / UK Government Office for Science, Tech. Rep. London, UK, 2016.

23. P. Lia, X. Yanga, K. Caoa, X. Taoa, R. Wanga and J. Tian, "An alignment-free fingerprint cryptosystem based on fuzzy vault scheme", Journal of Network and Computer Applications, pp. 207-220, May 2010.

24. J. Hartloff and V. Govindaraju, "Security analysis for fingerprint fuzzy vaults", Proc. SPIE – The Int. Soc. Opt. Eng., vol. 8712, no. 4, pp. 1-12, 2013.

25. Adamovic, S., Milosavljevic, M.: ‘Information analysis of iris biometrics for the needs of cryptology key extraction’, Serb. J. Electr. Eng., 2013, 10, (1), pp. 1–12.

26. Alvarez Marino, R., Hernandez Alvarez, F., Hernandez Encinas, L.: A crypto-biometric scheme based on iris-templates with fuzzy extractors. (2012) Elsevier Inc.

27. Kanade, S., Camara, D., Krichen, E., Petrovska-Delacretaz, D., Dorizzi, B., et al.,: ‘Three factor scheme for biometric-based cryptographic key regeneration using iris,’ in The 6th Biometrics Symposium 2008 (BSYM2008).

28. Yongjin Wang, Plataniotis, K.N.: Fuzzy Vault for Face Based Cryptographic Key Generation. IEEE biometric symposium. (2007).

29. Nagar, A., Nandhakumar, K., and Jain, A. K., Multibiometric cryptosystem based on feature level fusion. IEEE Transaction on Information

Forensics and Security 7(1):255–268, 2012.

30. Takahashi, K., Matsuda, T., Murakami, T., Hanaoka, G., Nishigaki, M.: A signature scheme with a fuzzy private key. In: Malkin, T., Kolesnikov, V., Lewko, A.B., Polychronakis, M. (eds.) ACNS 2015. LNCS, vol. 9092, pp. 105–126. Springer, Cham (2015).

31. Wang, C.: A provable secure fuzzy identity based signature scheme. Sci. China Inf. Sci. 55(9), 2139–2148 (2012).

32. Li, N., Guo, F., Mu, Y., Susilo, W., Nepal, S.: Fuzzy extractors for biometric identification. In: Lee, K., Liu, L. (eds.) 37th IEEE International Conference on Distributed Computing Systems, ICDCS 2017, Atlanta, GA, USA, June 5–8, 2017, pp. 667–677. IEEE Computer Society (2017).

33. Hassan N.A., Al-Mukhtar F.S., Ali E.H. Encrypt Audio File using Speech Audio File As a key. Proceedings of the 2nd International Scientific Conference of Al-Ayen University, ISCAU-2020, 15–16 July 2020, Thi-Qar, Iraq. IOP Conference Series: Materials Science and Engineering. 2020;928 032066:79–84. DOI:10.1088/1757-899X/928/3/032066

34. Monrose, F., Reiter, M. K., and Wetzel, S. Password hardening based on keystroke dynamics. International Journal of Information Security 1, 2 (2002), 69–83.

35. Nandakumar K., Jain A.K. Multibiometric template security using fuzzy vault, in IEEE second international conference on biometrics: Theory, applications and systems, pp. 1–6. 2008.

36. Kanade S., Petrovska-Delacr ˜etaz D., Dorizzi B. Multi-biometrics based cryptographic key regeneration scheme, in BTAS09: Proceedings of the 3rd IEEE international conference on biometrics: Theory, applications and systems, pp. 1–7. 2009.

37. Brindha, V. E., and Natarajan, A. M., Multi-Modal Biometric Template Security: Fingerprint and Palmprint Based Fuzzy Vault. Journal of Biometrics & Biostatistics 3(6):1–6, 2012.

38. Vinothkanna, R., and Wahi, A., Fuzzy Vault Fusion Based Multimodal

Biometric Human Recognition System with Fingerprint and Ear. J. Theor. Appl. Inf. Technol. 59(2):304–316, 2014.

39. Bilingual Keystroke Dynamics Dataset. URL: https://github.com/ntwaijry/BKSD (дата звернення: 20.05.2023).

40. Scotti, F., Cimato, S., Gamassi, M., Piuri, V., Sassi, R. Privacy aware Biometrics: Design and Implementation of a Multimodal Verification System // 2008 Annual Computer Security Applications Conference, IEEE. – 2008. – P. 130-139.

41. Tsoukalas L. H. Fuzzy and Neural Approaches in Engineering / L. H. Tsoukalas, R. E. Uhrig. – New York: John Wiley&Sons.Inc, 1997. – 587 p.