Додаток А.

Комплект графічних матеріалів

Методи захисту інформації в системах електронного документообігу

Актуальність роботи. Дослідження, що проводяться щороку провідними гравцями на ринку інформаційної безпеки показують, що, з одного боку, кількість інцидентів, пов'язаних з фінансовими збитками, спричиненими фальсифікацією юридично значущих документів, щороку знижується, але, з іншого боку, сукупний збиток залишається приблизно незмінним. Тобто, з кожним роком значно зростають фінансові втрати від одного інциденту.

Таким чином, слід визнати, що засоби захисту документів недостатньо ефективні або вони неефективно застосовуються. Відомо, що захищеність системи визначається найслабшою ланкою у системі безпеки. Виходячи з цієї тези можна зробити висновок: потрібно прагнути до забезпечення рівного рівня захисту для документів на будь-яких видах носіїв.

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.

Труднощі виконання вимог «рівного захисту» документів на електронних та паперових носіях

1. Електронний підпис неможливо застосувати до документа на паперовому носії.

2. Електронний підпис є відчужуваним від власника, тобто за електроннимі підписом неможливо точно ідентифікувати підписувача.

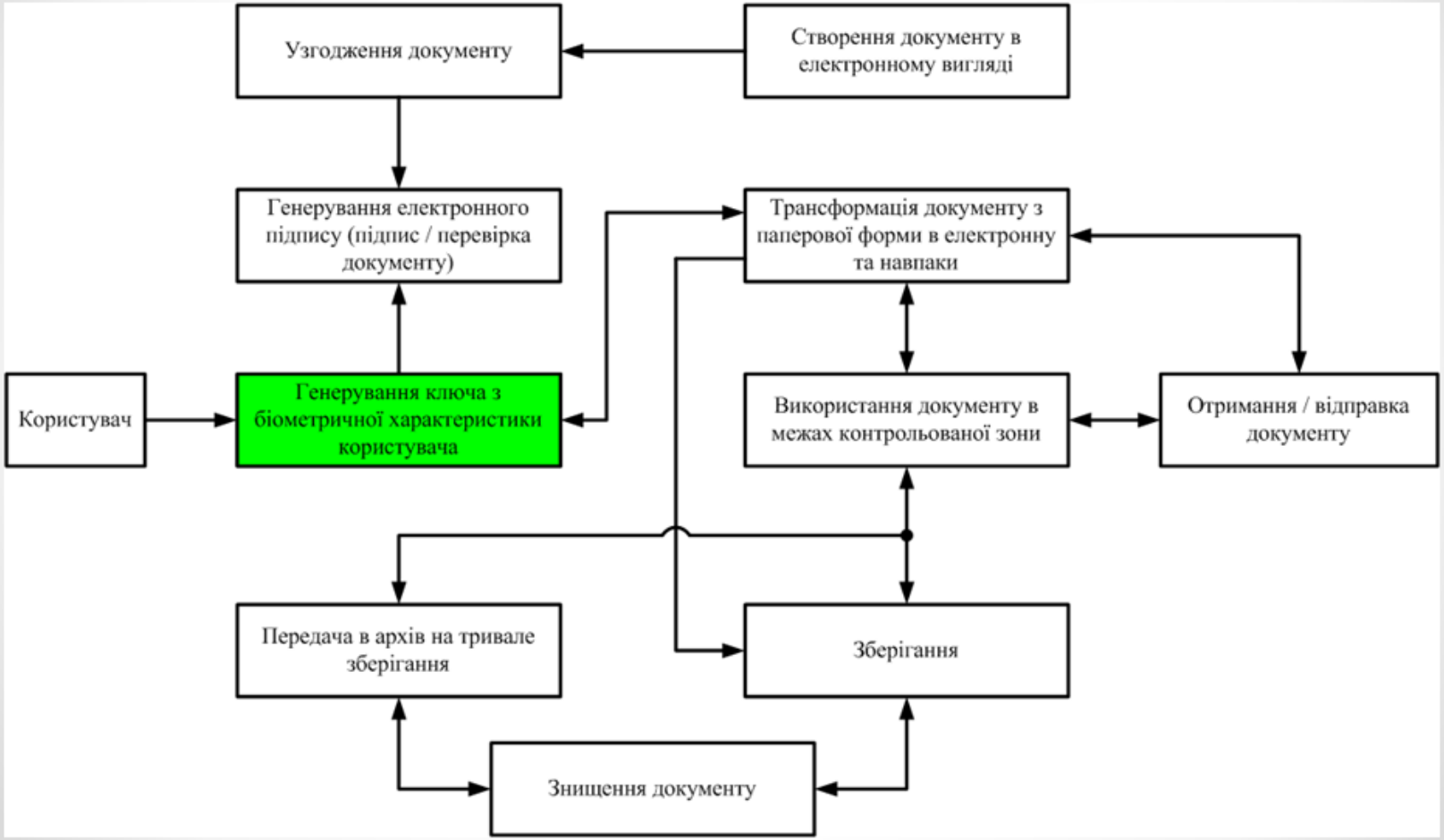
3 Зображення автографа, який застосовується у паперовому документі для збереження та підтвердження юридичної значущості може бути скопійоване з метою подальшої фальсифікації інших документів (як електронних, так і паперових).

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.

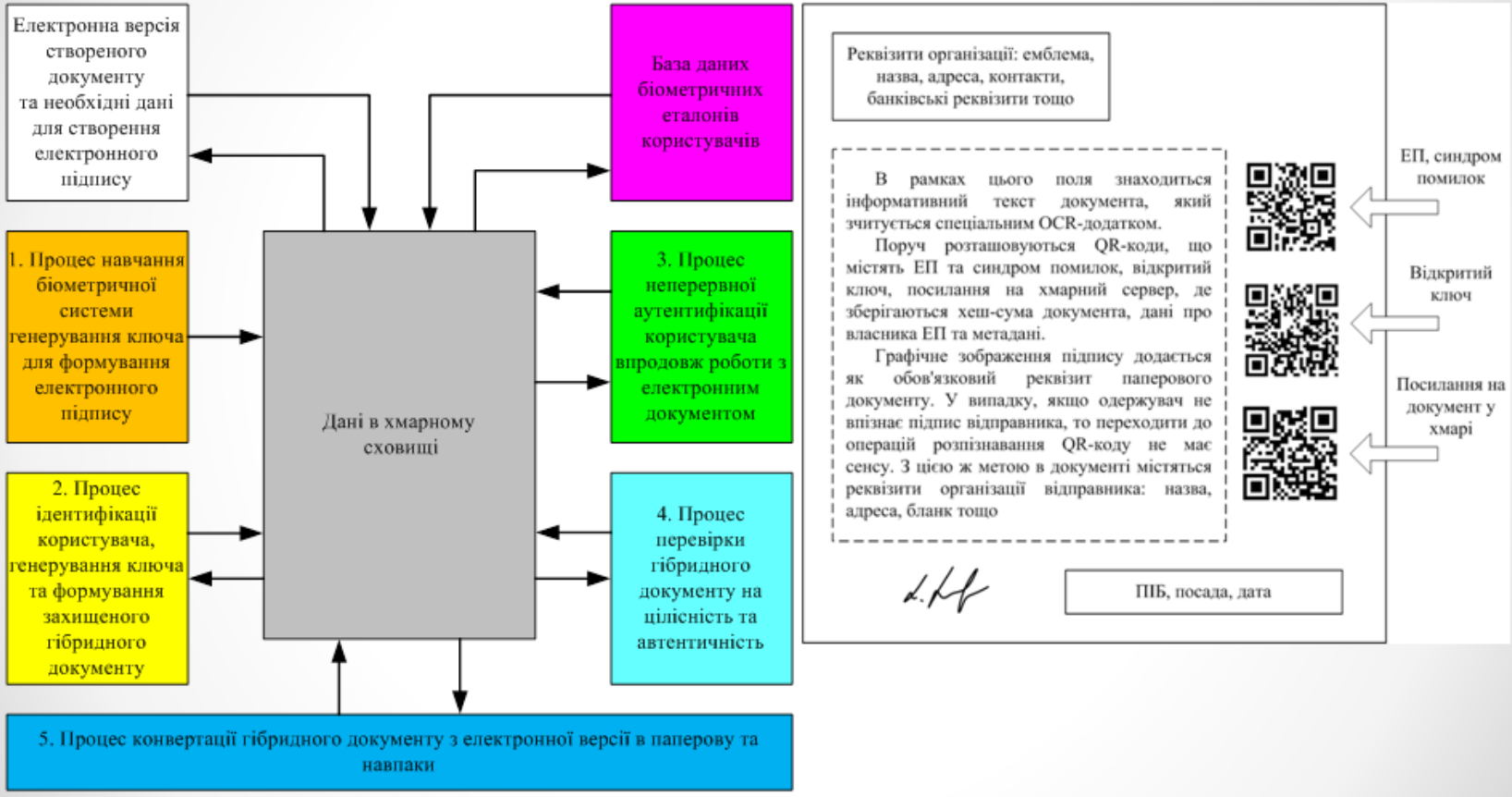
5. Міграцію документів на паперовому носії за межі контрольованої зони складно відстежити чи запобігти – «людський фактор» завжди впливатиме на безпеку систем.

6. Дії щодо створення паперових документів повинні 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.

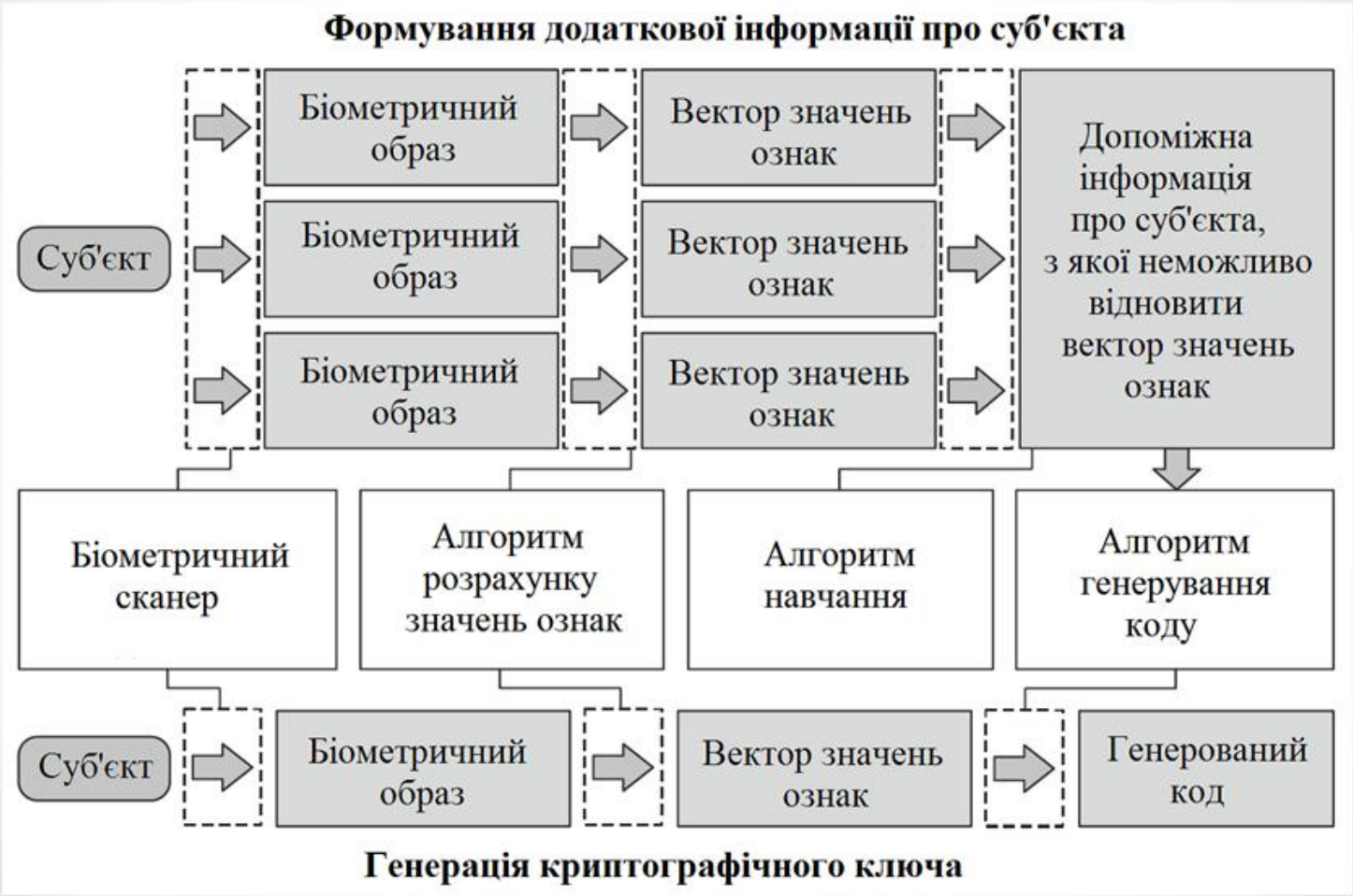
Схема маршруту документу в гібридному документообігу



Структурна схема системи захищеного гібридного документообігу



Перетворювачі біометрія-код



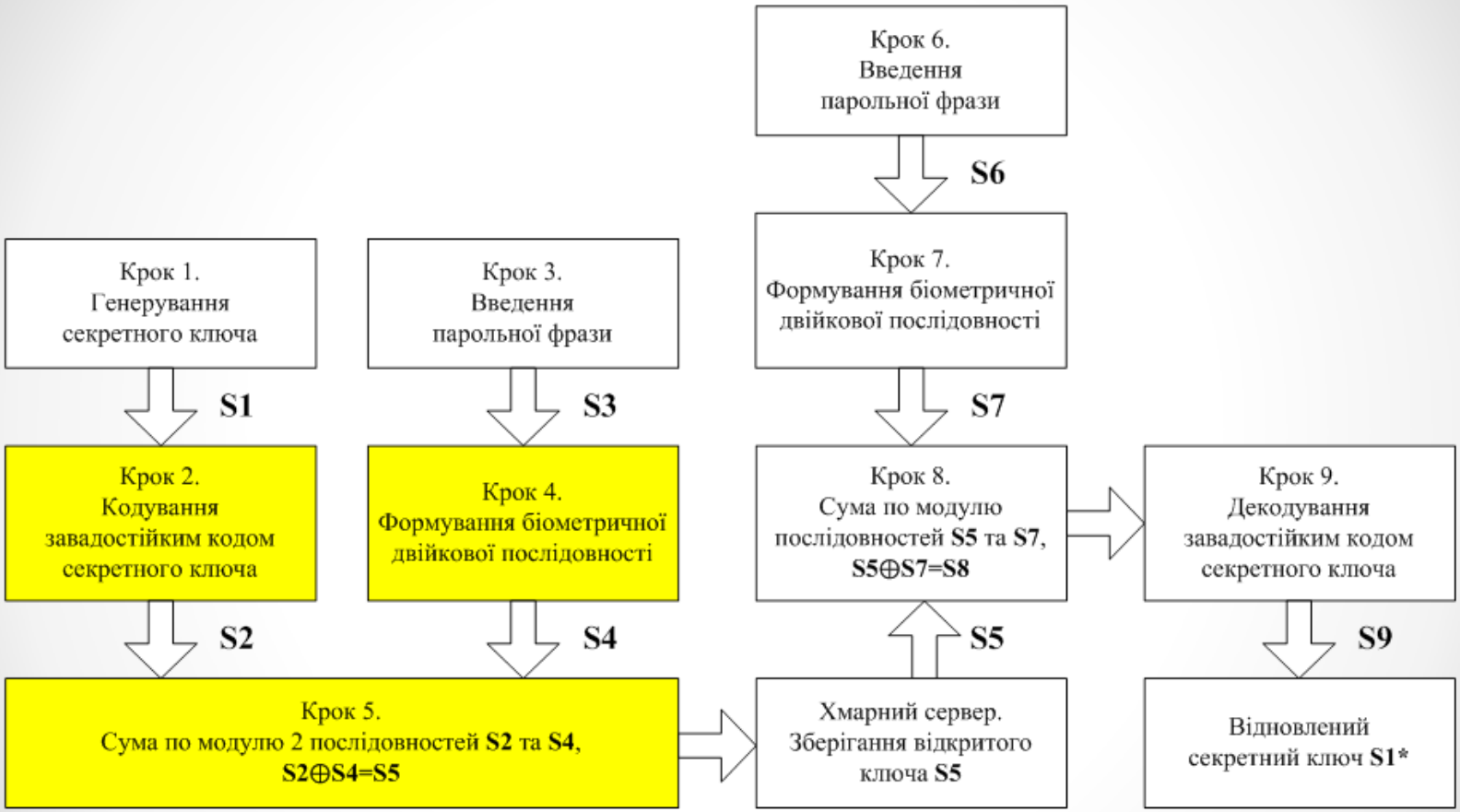
Перетворювачі біометрія-код

Переваги нечітких екстракторів	Недоліки нечітких екстракторів	Переваги нейромережевих перетворювачів біометрія-код	Недоліки нейромережевих перетворювачів біометрія-код
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		

Перетворювачі біометрія-код

Тип задачі	Тип біометричного параметру	Вихідні дані експериментів	Тип перетворювача біометрія-код	Середня оцінка якості роботи перетворювачів
Формування ключа	Голосовий відбиток	10 користувачів; всього 100 дослідів	НПБК	FRR+FAR=0.16
		60 користувачів 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)
	Динамічний рукописний підпис	-		FRR = 0,089 FAR=0,096
		65 користувачів 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 користувачів, 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)
Аутентифікація	Динамічний рукописний підпис	280 оригінальних підписів одного користувача, 1281 фальсифікацій підпису семи користувачів	Нечіткі класифікатори	FRR=0.0057-0.038 FAR=0.0016-0.005
Верифікація	Динамічний рукописний підпис, голосовий відбиток	90 користувачів, загальна кількість реалізацій 10000	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)

Типова схема нечіткого екстрактору



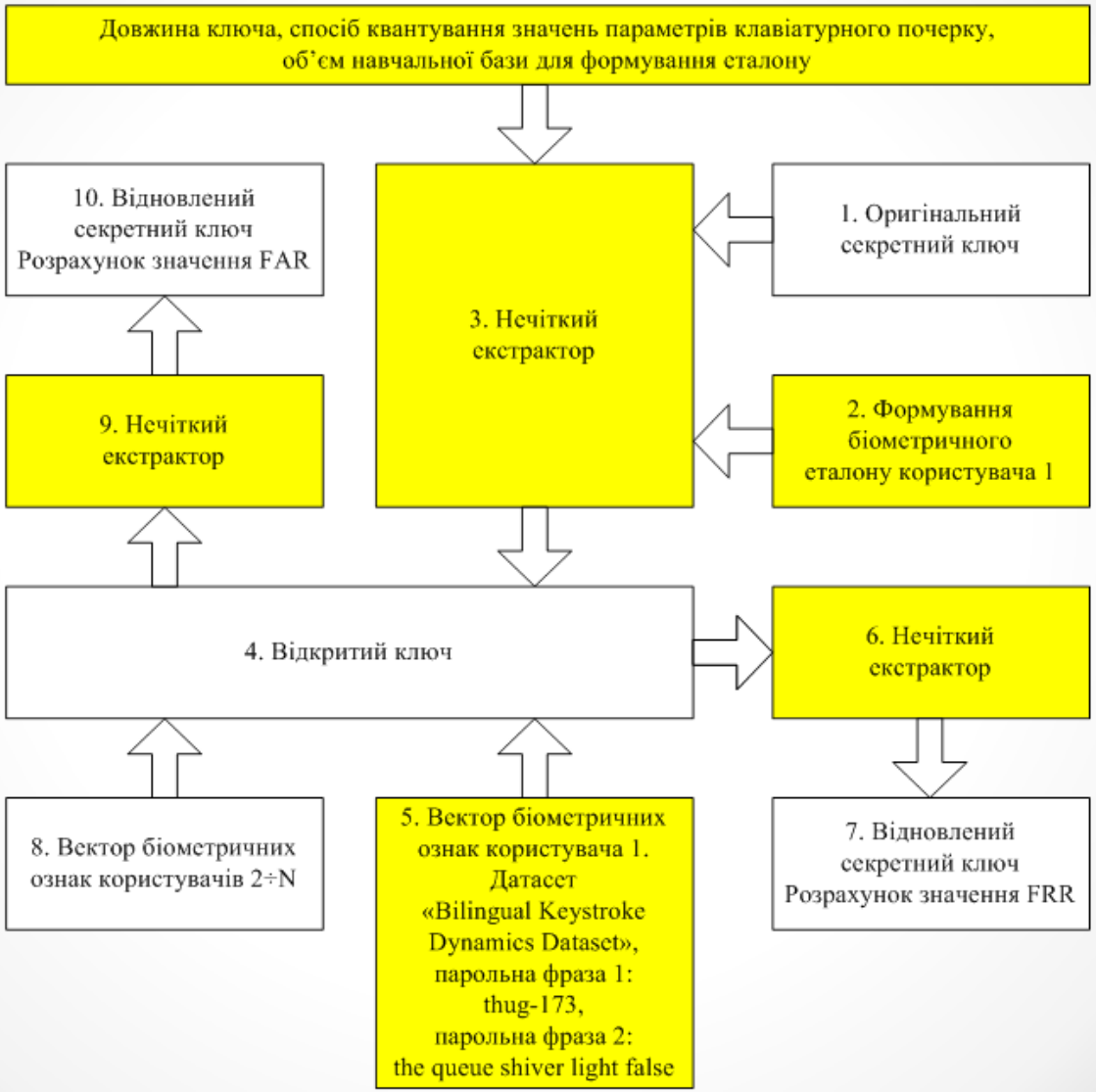
Пропонована схема нечіткого екстрактору

В пропонованому алгоритмі в якості вектору біометричного еталону користувача використовується вектор середніх значень натискання на кожну клавішу t та часів паузи між натисканнями p. Якщо довжина паролю складає N символів (тобто N значень параметру t та N-1 значень параметру p), то довжина вектору становить $0.75 \cdot (2N-1)$. З аналізу виключаються 25 % середніх значень параметру t та параметру p, які відповідають максимальним значенням їх СКВ, тобто відповідають найнестабільнішим ознакам клавіатурного почерку користувача.

В пропонованому алгоритмі використовується три способи квантування $Y=f(x)$ вектору біометричного еталону x, тобто трансформування його складових в двійкові числа. 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.

В пропонованому алгоритмі використовується завадостійкий 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 корегуюча здатність коду Ріда-Соломона становить не більше H/3 (H – довжина інформаційної послідовності), надмірність коду складає (2/3)H, тобто довжина кодової послідовності H* на 2/3 перевищить довжину H.

Схема експерименту



Результати проведених досліджень

Позначення	Парольна фраза «thug-173»	Парольна фраза «the queue shiver light false»
Інформативних ознак	15	31
Довжина біометричної двійкової послідовності	80 бітів (33 % ознак виключено з аналізу, як нестабільні – 5 з 15)	200 бітів (19 % ознак виключено з аналізу, як нестабільні – 6 з 31)
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	**0.106**	**0.032**
2-й спосіб квантування	**0.086**	**0.058**
3-й спосіб квантування	0.128	0.025
Помилка 2-го роду		
1-й спосіб квантування	**0.131**	**0.085**
2-й спосіб квантування	**0.052**	**0.018**
3-й спосіб квантування	0.941	0.047
Помилка 1-го роду		
навчальна база – 10 записів	**2.236**	**1.914**
навчальна база – 30 записів	0.688	0.348
навчальна база – 50 записів	**0.091**	**0.060**
навчальна база – 200 записів	**0.086**	**0.058**
Помилка 2-го роду		
навчальна база – 10 записів	**1.924**	**0.414**
навчальна база – 30 записів	0.26	0.126
навчальна база – 50 записів	**0.055**	**0.023**
навчальна база – 200 записів	**0.052**	**0.018**

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 електронного підпису 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 електронного підпису та інших криптографічних механізмів для «паперових» реалізацій документа призводить до більш низької захищеності документа при його розповсюдженні «на папері».

Висновки

3. Розглянуто концепцію захисту гібридного документообігу, в якому:

1) наявна надійна прив'язка всіх аутентифікаторів суб'єкта (паролів, ключів шифрування та електронного підпису, 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 електронного підпису; 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.

Висновки

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.

Номер документу	Позначення	Найменування	Прим.
		Текстові документи	
1		Пояснювальна записка	102 с.
		Графічний матеріал	
2		Методи захисту інформації в системах	А4 ел.ф.
		електронного документообігу	
3		Труднощі виконання вимог «рівного	А4 ел.ф.
		захисту» документів на електронних	
		та паперових носіях	
4		Схема маршруту документу	А4 ел.ф.
		в гібридному документообігу	
5		Структурна схема системи захищеного	А4 ел.ф.
		гібридного документообігу	
6-8		Перетворювачі біометрія-код	3х А4 ел.ф.
9		Типова схема нечіткого екстрактору	А4 ел.ф.
10		Пропонована схема	А4 ел.ф.
		нечіткого екстрактору	
11		Схема експерименту	А4 ел.ф.
12		Результати проведених досліджень	А4 ел.ф.
13-15		Висновки	3х А4 ел.ф.

Из	Лист	№ докум.	Підпис	Дата
Розроб.		Федотов		
Перев.		Горелов		
Н.контр.		Милютченко		
Затв.		Антіпов		

Методи захисту інформації в системах електронного документообігу

Відомість кваліфікаційної роботи магістра

Літера	Лист	Листів
Д		

ХНУРЕ
Кафедра КРіСТЗІ