ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Комплексний аналіз методів виявлення фальсифікацій в електронних документах

Виконав здобувач групи СПм-21-2
Федір СУХИНА
Керівник роботи доктор технічних наук, професор
Олександр МОЖАЄВ

Харків – 2023

Характеристика наукового дослідження

- Об’єктом дослідження є процесс функціонування електронного обігу документів.
- Предметом дослідження – методи виявлення фальсифікованого фрагменту електронного документу
- Метою кваліфікаційної роботи є розробка та дослідження методу виявлення фальсифікованого фрагменту електронного документу шляхом перехресного хешування..

Завдання дослідження:

- 1) аналіз сучасного стану проблеми захисту електронних документів;
- 2) аналіз методів криптографічного захисту електронних документів;
- 3) аналіз та розроблення моделей побудови хеш-функцій для визначення фальсифікованих фрагментів електронного документу;
- 4)Розроблення засобів виявлення фальсифікацій в електронних документах;

- Технічний прогрес, обумовлений розвитком інформаційного суспільства передбачає використання технологій електронного обміну даними. Перехід до електронного документообігу, насамперед, пов'язаний з низкою переваг його використання. Електронний документообіг дозволяє суттєво спростити роботу по формуванню, збереженні та відправці важливої інформації.
- На рис. 1. показаний графік, який демонструє час необхідний для виконання основних операцій над документами, що свідчить про переваги електронного документообігу над традиційним – паперовим.

5

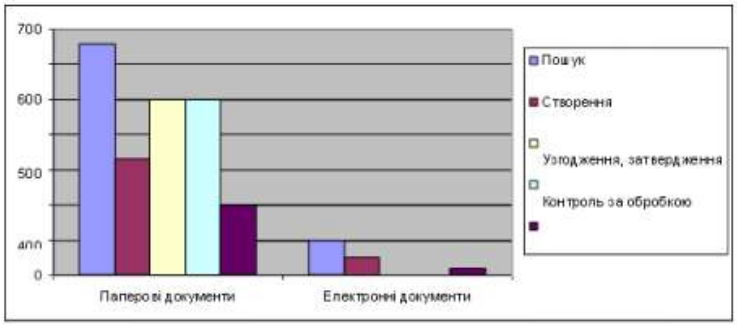

Рис 1 Графік затрат часу на типові операції обробки паперових та електронних документів в місяць

6

Фальсифікація електронних документів може стати непоправним явищем, оскільки найменші зміни в документі можуть докорінно змінити його суть. На рис.2. показана модель інформаційної безпеки електронного документу.

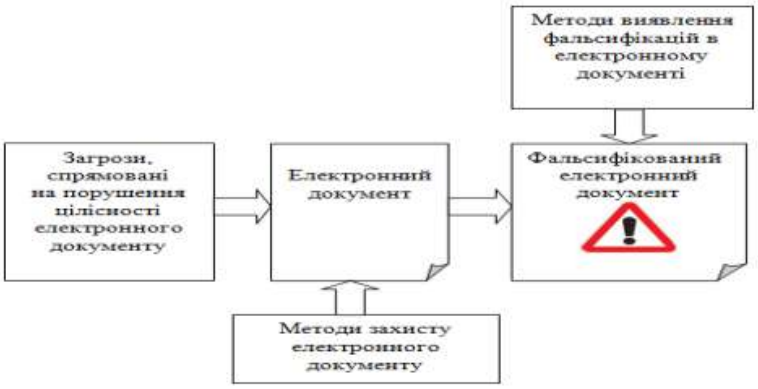

Рис. 1.2. Модель інформаційної безпеки електронного документу

Загрози порушення конфіденційності спрямовані на розголошення конфіденційної чи секретної інформації. У разі реалізації цих загроз інформація стає відомою для суб'єктів, які не мають до неї доступу. Порушення конфіденційності є причиною отримання суб'єктами несанкціонованого доступу до електронних документів 7

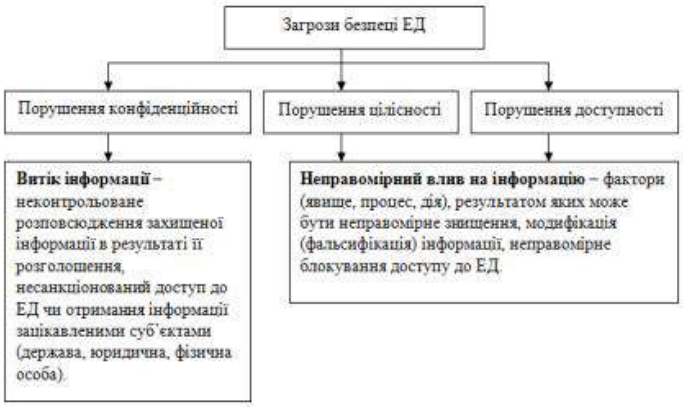

Рис. 3. Класифікація загроз безпеці електронного документу

Електронний документ представляє собою аналог паперового документу, створеного на цифровому носії, включаючи обов'язкові реквізити. 8

Реквізити електронного документу повинні розміщуватись відповідно до чинних нормативних документів та стандартів. Зокрема, згідно з ДСТУ 41632003, таких обов'язкових реквізитів п'ять:
1) найменування організації-творця документа;
2) місцезнаходження організації-творця документа (або поштова адреса);
3) найменування документа;
4) дата виготовлення документа;
5) код особи, що виготовила або затвердила документ.

До специфічних властивостей електронних документів можна віднести такі:
1) незалежність інформативної складової (зображення, звуку, тексту) від конкретного матеріального носія;
2) наявність загальної системи кодування (бінарний код), однакової для фіксації документів будь-якої знакової системи (тексту, звуку, зображення, графіки);
3) практична неможливість вичленовування деяких електронних документів із програмної оболонки й загальних масивів (наприклад, у базах даних);
4) відсутність індивідуального носія для кожного з документів, розміщених на окремому комп'ютері або сервері;
5) «інтерактивність» документа (можливість втручання користувача в його текст і структуру, робити за своїм розсудом перекомпонування матеріалу або його додавання).

Криптографічний захист електронних документів

Криптографія – це наука, яка вивчає способи перетворення інформації з метою захисту її від незаконних користувачів .

Основні напрямки використання криптографічних методів – передача конфіденційної інформації в каналах зв'язку, встановлення дійсності переданих повідомлень, збереження інформації на носіях у зашифрованому вигляді. За способом дії на дані криптографічні методи розділяють на групи рис. 4.

Рис. 4. Класифікація методів криптографічного перетворення інформації

9

Технологія використання ЕЦП передбачає електронний обмін даними між абонентами мережі. Для відправника і отримувача генерується пара ключів: відкритий і закритий. Закритий ключ зберігається у відправника в таємниці і використовується ним з метою формування ЕЦП.

Рис. 5. Схема формування електронного цифрового підпису

11

При перевірці ЕЦП отримувач ЕД розшифровує прийнятий хеш (H) відкритим ключем відправника. Крім того, отримувач самостійно за допомогою хеш-функції (*H*) обчислює хеш (*h*) отриманого ЕД і порівнює його з розшифрованим. Якщо *(H) і (h)* співпадають, то ЕЦП – вірний.

Рис. 6. Схема перевірки електронного цифрового підпису

12

Моделі цифрового водяного знаку

Рис. 7. Класифікація методів накладання цифрового водяного знаку

Моделі побудови хеш-функцій для визначення фальсифікованих фрагментів електронного документу 13

Хеш-функція є найпростішим варіантом електронного цифрового підпису, який є гарантом цілісності, достовірності електронного документу та підтвердження авторства електронного документу.

Рис. 8. Узагальнена схема використання хеш-функцій

Виправлення помилок в блоках електронного документу (*– фальсифікований блок інформації)

Блок-схема алгоритму виявлення фальсифікованого фрагменту електронного документу методом перехресного хешування 14

Схематично принцип отримання хеш-функцій можна показати наступним чином, рис. 9

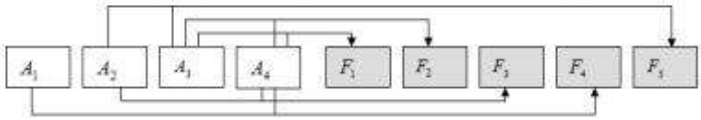

Рис. 9 Схема отримання хеш-функцій

Таблиця Виправлення помилок в блоках електронного документу

Локалізація помилки											
	Двократна помилка							Однократна помилка			
x_1	1 *	1 *	1 *	0	0	0		1 *	0	0	0
x_2	1 *	0	0	1 *	1 *	0		0	1 *	0	0
x_3	0	1 *	0	1 *	0	1 *		0	0	1 *	0
x_4	0	0	1 *	0	1 *	1 *		0	0	0	1 *
$f_1(x_3 + x_4)$	0	1	1	1	1	0		0	0	1	1
$f_2(x_3 + x_4)$	0	1	1	1	1	0		0	0	1	1
$f_3(x_2 + x_4)$	1	0	1	1	0	1		0	1	0	1
$f_4(x_1 + x_4)$	1	1	0	0	1	1		1	0	0	1
$f_5(x_2 + x_3)$	1	1	0	0	1	1		0	1	1	0

Технічна реалізація виконується на основі ПЛІС Xilinx Spartan-3E Srarter Kit. Архітектура інструментального модуля Xilinx Spartan-3E Srarter Kit Board дозволяє використовувати його для реалізації автономних систем управління, збору і обробки інформації, цифрової обробки сигналів, вбудованих цифрових пристроїв з комп'ютерними інтерфейсами, зокрема пристрої, що виконують криптографічні операції .

15

Рис. 10 Зовнішній вигляд інструментального модуля Xilinx Spartan-3E Srarter Kit

Публікації за тематикою дослідження

Ф.Ф. Сухина Метод виявлення втручання в комп'ютерні системи електронного обігу документів/Можаєв О.О., Сухина Ф.Ф., Башилов В.С// Системи управління, навігації та зв'язку. Полтава : НУ «Полтавська політехніка», 2023. Вип. 1(71). С. 122-126.

16

ВИСНОВКИ

- Було розглянуто використання хеш-функцій в процесі забезпечення цілісності інформації. На основі розроблених в другому розділі алгоритмів обчислення хеш-функції електронного документу було запропоновано два методи виявлення фальсифікацій в електронному документі:
- Метод виявлення порушень цілісності шляхом перехресного хешування. Суть запропонованого методу полягає в обчисленні хеш-функції в блоках даних: горизонтальних та вертикальних. В разі виникнення помилки, при перевірці значень хеш-функції, перетин блоків вкаже на фальсифікований фрагмент інформації.
- Виявлення порушень цілісності електронного документу на основі введення надлишковості. Розробка методу ґрунтується на принципах алгоритму кодування за Хеммінгом. До інформаційних блоків додаються контрольні блоки інформації, обчислені за формулою згідно породжуючої матриці. В результаті побудовано коди, які гарантують виправлення двохкратної помилки в блоках інформації.
- Таким чином, застосування запропонованих методів дозволить забезпечити належний рівень захищеності електронного документу, зокрема цілісність даних. Крім цього, на основі реалізації методів виявлення фальсифікацій в електронному документі, можна робити припущення про мету підробки та можливих зловмисників.