Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи виявлення втручання в комп'ютерні системи електронного обігу документів

(тема)

Виконав:

студент II курсу, групи СПм-21-2

Сухина Ф.Ф.
(прізвище, ініціали)

Спеціальність

123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма

Системне програмування
(повна назва освітньої програми)

Керівник: проф. Можаєв О.О.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2023 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

(повна назва)

ЗАТВЕРДЖУЮ:
Зав.кафедри _____
(підпис)

“ ____ ” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Сухині Федору Федоровичу
(прізвище, ім’я, по батькові)

1. Тема роботи Методи виявлення втручання в комп'ютерні системи електронного обігу документів

затверджена наказом по університету від “ 03 ” квітня 2023 р. № 318 СТ

2. Термін подання студентом роботи до екзаменаційної комісії 10 травня 2023

3. Вхідні дані до роботи результати дослідження методів виявлення втручання в комп'ютерні системи електронного обігу документів

4. Перелік питань, що потрібно опрацювати у роботі

1. Аналіз завдання на проектування
2. Розробка та дослідження методу виявлення фальсифікованого фрагменту електронного документу шляхом перехресного хешування
3. Дослідження методу виявлення заданої кількості фальсифікованих фрагментів електронного документу на основі надлишкового хешування контрольного блоку

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 17 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз предметної області	04.04.23-07.04.23	
2	Збір і аналіз вимог для функціонування		
	електронного документу	08.04.23-13.04.23	
3	Розробка методу виявлення фальсифікованого		
	електронного документу шляхом перехресного		
	хешування	14.04.23-18.04.23	
	Тестування розробки	19.04.23-25.04.23	
	Оформлення матеріалів кваліфікаційної роботи	26.04.23-09.05.23	
	Подання кваліфікаційної роботи керівникові та	10.05.23-11.05.23	
	її попередній захист		
	Подання кваліфікаційної роботи на		
	рецензування	12.05.23-16.05.23	

Дата видачі завдання 03 квітня 2023 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Можаєв О.О.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 74 с., 23 рис., 5 табл., 1 дод., 53 джерел.

ЕЛЕКТРОННИЙ ДОКУМЕНТ, ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС, ХЕШ-ФУНКЦІЇ, ДОСТОВІРНІСТЬ, КРИПТОГРАФІЯ, ВОДЯНОЙ ЗНАК, СТЕГАНОГРАФІЯ.

Метою кваліфікаційної роботи є розробка та дослідження методу виявлення фальсифікованого фрагменту електронного документу шляхом перехресного хешування.

Об'єкт дослідження – процесс функціонування електронного обігу документів

Предмет дослідження – методи виявлення фальсифікованого фрагменту електронного документу

ABSTRACT

Master’s thesis: 74 pages, 23 figures, 5 tables, 1 appendices, 53 sources.

ELECTRONIC DOCUMENT, ELECTRONIC DIGITAL SIGNATURE, HASH FUNCTIONS, AUTHENTICITY, CRYPTOGRAPHY, WATERMARK, STEGANOGRAPHY.

The major goal of this thesis is the development and research of a method of detecting a falsified fragment of an electronic document by means of cross-hashing

The object of research is the process of functioning of the electronic circulation of documents

The subject of the study is methods of detecting a falsified fragment of an electronic document

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

XSS – Міжсайтовий скриптинг

SQL – Structured query language

OWASP – Open Web Application Security Project

XML – Extensible Markup Language

XXE – Впровадження зовнішніх сутностей

CSRF/XSRF – Межсайтова підробка запитів

ORM – Object-relational mapping

API – Application Programming Interface

HTTP – HyperText Transfer Protocol

HTTPS – HyperText Transfer Protocol Secure

SSL – Secure Sockets Layer

ОС – Операційна система

URL – Uniform Resource Locator

MD – Message Digest

SHA – Scriptores Historiae Augustae

TDE – Transparent Database Encryption

EFS – Encrypting File System

MVC – Model-View-Controller

HTML – HyperText Markup Language

IIS – Internet Information Services

UI – User interface

ПДВ – Податок на додану вартість

ДСТУ – Державні стандарти України

ПП – Програмний продукт

ВСТУП

Актуальність теми. Технічний прогрес дозволяє використання спільно зі звичайними паперовими документами використання та сучасних електронних. Такий перехід від паперового до електронного документу обігу дозволяє значно скоротити час обробки таких документів. Сьогодні все більша кількість підприємств та установ різної форми власності здійснюють перехід до використання до обміну даними в електронному вигляді, що відповідає сучасним тенденціям. Однак такий перехід неможливо провести без забезпечення надійних систем захисту інформації, що розповсюджується при електронному обігу документів. Тому виникає актуальна проблема захисту електронних документів (ЕД) при їх використанні життєдіяльності суспільства та людини. Для вирішення цієї проблеми окрім широко відомих методів та засобів захисту інформації потрібно використання ще і специфічних, які повинні враховувати особливості електронних документів Питання захисту електронних документів не можуть бути повністю вирішені лише стандартним набором засобів захисту інформації.

Таким чином, стає актуальною і сучасною задача дослідження можливостей сучасних засобів та методів захисту ЕД з використанням існуючих засобів, які базуються на криптографії та стеганографії, так і перспективних засобів. Але на жаль, жоден з існуючих механізмів захисту не здатний забезпечити вирішення цієї проблеми в повній мірі. Найбільш перспективним нині вважається компленксне використання значної кількості відомих методів захисту.

Проблему захисту інформації при електронному обігу документів можна представити, як рядок задач, комплексно рішення яких дозволить отримати бажений результат.

Серед цих задач виделимо такі. Необхідність забезпечити цілісність інформаційного обміну. Це можливо за допомогою застосування методів та

засобів криптографічного захисту. Одним з таких засобів можно вважати електронний цифровій підпис.

В той же час захист електронного обігу документів неможливо уявити без використання стеганографічних методів, які досить часто використовуються у сегоденні. Комплексне використанні переліченних методів та засобів дозволяє суттево покращати надійність та достовірність сучасного обороту документів, тому числі і електронних.

Основні теоретичні та практичні розробки сучасних методів комп'ютерної стеганографії представлені в роботах А.В. Балакіна, А.С. Єлісєва, В.Г. Грибуніна, Г.Ф. Кохановича, А.В. Аграновського та інш. Особливо виделимо праці Д.А. Сагайдака та Р.Т. Файзуліна де було розроблено та наведені результати досліджень способу формування цифрового водяного знаку для фізичних та електронних документів. На базі цьогой спосіба можна побудувати систему перевірки достовірності інформації та систему прихованої передачі даних.

1 ДОСЛІДЖЕННЯ ОСНОВНИХ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

1.1 Сучасний стан проблеми захисту електронних документів

Інформаційне середовище має визначальне значення на загальний рівень розвитку суспільства. Неможливо уявити собі будь яку складову існування значної кількості суспільних установ без сучасних інформаційних систем. Сучасні інформаційно-комунікаційних технологій привели до глобальної зміни суспільства із індустріального в інформаційне. У теперішній час значна більшість інформації отримується, обробляється зберігається та передається в вигляді електронних даних. Тоді сам розвиток інформаційного простору потребує впровадження новітніх технологій обміну даними.

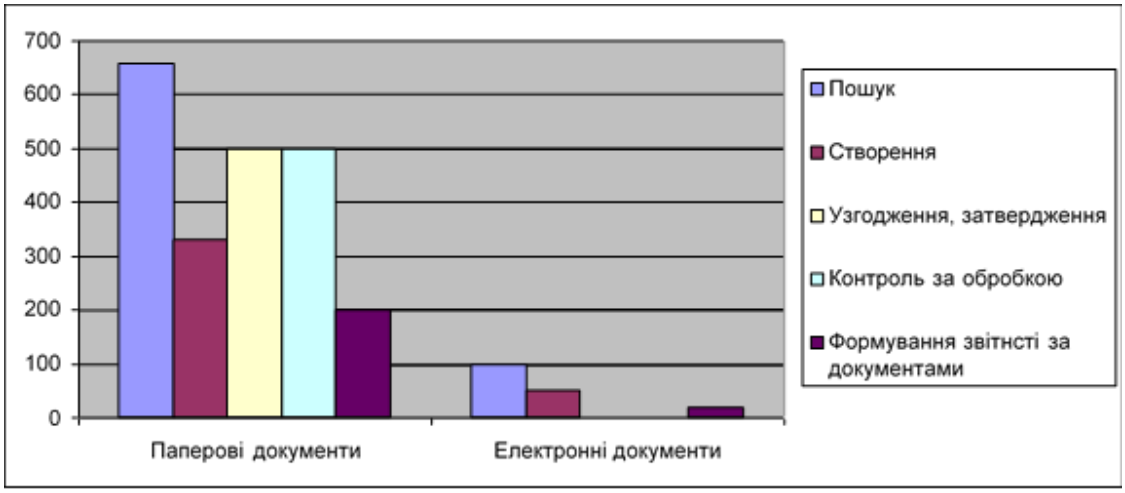


Рисунок 1.1 – Графік затрат часу на типові операції обробки паперових та електронних документів в місяць

Обіг документів в електронному поданні дозволяє спростити процес формування, збереження та відправці важливої інформації [1–5]. При

використанні технології електронного обміну інформацією можливо суттєво зменшити час на опрацювання документів, вдосконалити процес обробки документів, за рахунок формалізації базових операцій рисунок°1.1.

При аналізу часу потрібного для виконання основних операцій над документами, встановлено що існують значні переваги електронного обміну інформацією над традиційним – паперовим. Цей факт представлено на рисунку 1.1, який демонструє затрати часу на типові операції обробки паперових та електронних документів в місяць. Зміни, які мають місто у інформаційному суспільстві дозволяє провести більш значну автоматизацію людської діяльності, у тому числі використання електронних документів (ЕД), застосування електронного обігу документіво та електронного цифрового підпису (ЕЦП). Яскравим прилдадом цієї тенденції є системи автоматизації управлінської сфери життедіяльності.

Електронний документообіг – це сукупність процесів створення, опрацювання, відправлення, передавання, одержання, зберігання, використання та знищення ЕД, які виконуються із застосуванням перевірки цілісності, і в разі необхідності, – з підтвердженням факту одержання таких документів [6–11]. Сучасні тенденції розвитку інформаційних технологій в значній мірі характеризуються зростанням обсягів інформації, яка необхідна у процесі прийняття рішень. Таким чином, виникає необхідність обробки більшої кількості документів, ніж раніше. Методи обробки документів, які вважалися традиційними до теперішнього часу не дозволяють ефективну роботу з документами, тому паперові документи необхідно замінити за можливостю електронними. У європейських країнах набуто суттєвий досвід з функціонування електронного документообігу на всіх етапах життєвого циклу документу на рівні з традиційним, а інколи електронний документообіг навіть перевищує паперовий [12-16]. необхідно відмітити, що ЕД мають таку ж юридичну легальність, як і традиційні.

Найбільше використання ЕД має місця у таких сферах людської діяльності, як освіта, медицина, державне управління та інших. Але розвиток

сучасних інформаційно-технічних можливостей генерує нові ризики та загрози. Це призводить до некоректного функціонування системи електронного документообігу, зниження достовірності та надійності, а в результаті і до значних матеріальних втрат. Таким чином, при використанні електронного документообігу обов'язково потрібно виукористовувати надійні системи електронного захисту [17].

Документообіг в державі є системою, що матеріалізує процеси збирання, перетворення, зберігання інформації, а також процеси управління: підготовку та прийняття рішень, контроль за їх виконанням [18–20]. Сучасні системи електронного урядування базуються на використанні електронного документообігу, котрий забезпечує циркуляцію документів, та є одним із найважливіших складових системи, тому що він забезпечує сучасну форму взаємодії держави та суспільства. Таким приладом є звернення за допомогою документа, що забезпечує в результаті можливість надання послуги державою громадянину. Необхідність побудови систем автоматизації управління документообігом в теперішній час отримало практичний сенс. Все більша кількість установ, підприємств різної форми власності використовують різноманітні системи електронного документообігу. Це дозволяє значної кількісті організацій провести оцінку переваг новітньої технології обробки документів.

Стрімке зростання обсягів інформації, яка використовується в управлінській діяльності установ в Україні, потребує швідкого впровадження сучасних систем електронного обігу документів. Таке впровадження технологій електронного урядування потребує використання електронного обігу документів, яке має у своєму складі засоби ЕЦП. При користуванні системою електронного обігу документів виникає необхідність застосування сучасних систем захисту інформації. Тоді виникає важлива проблема, рішення якої має велічезне значення. Це проблема цілісності електронних документів процесі електронного документообігу.

Основною відміною від паперових документів, є те що ЕД зберігаються

в електронних пристроях, поширюється телекомунікаційними системами, можуть мати значну кількість копій, отже ці документи є більш вразливими до атак. Рішення цієї важливої проблеми займає вже дуже значний час. Але все ж існує багата кількість питань, яка потребує свого вирішення. Наприклад це дослідження методів забезпечення безпеки ЕД у інформаційному просторі.

Підробка цінних документів це злочин, який призводить до великого збитку всьому суспільству. Згідно з кримінальним кодексом, підробка документів – це злочин який характеризується виготовленням повністю фальсифікованих документів або його складових частин: носія інформації, фрагменту тексту, підпису [21]. Якщо засоби виявлення підробки в паперових документах давно відомі та широко застосовуються, то фальсифікація ЕД це достатньо нове явище, котре потребує нових підходів до її рішення [22–23]. Особливостями цього явища є те що, оскільки мінімальні зміни документу можуть кардинально змінити його суть. Розглянемо модель інформаційної безпеки електронного документу, що представлено на рисунку 1.2.

Відповідно даної моделі, електронний документ схильний до впливу, який спрямоваі на порушення цілісності та надійності ЕД. Для забезпечення протидії загрозам ЕД потрібно застосовувати засоби захисту інформації та надійні методи інформаційного обміну. Документ вважається фальсифікованим, якщо є деякі факти порушення цілісності інформації електронного документу. Підробку в документі можна виявити за допомогою існуючих методів визначення фрагментів ЕД, що фальсифіковані.

Електронний обіг документів є досить важливим для людства та відграє значну роль. Таку ж значну роль має і проблема його захисту. Однак, незважаючи на велику кількість існуючих методів та засобів захисту електронних документів, жоден з них не гарантує абсолютного захисту.. Така відсутність методів гарантованного захисту електронних документів є джерелом нескінченного пошуку шляхів нових рішень. Серед таких шляхів

необхідно виділити такі, як криптографія та стеганографія на основі використання сучасних комп'ютерних технологій. Велике значення багато дослідників приділяє розробці та вдосконаленню алгоритмів побудови електронного цифрового підпису за різними принципами. Проведене дослідження встановило, що рішення таких питань є актуальними і у теперішній час.

Рисунок 1.2 – Модель інформаційної безпеки електронного документу

Основна відмінність від криптографії, методів стеганографії полягає в тому що приховують не лише самий зміст документу, що передається, а і факт передачі документу. Одним з основних характерних засобів стеганографії є використання цифрового водяного знаку. Це використовується в інформації електронного документу для захисту прав автора документу. У сьогоденні ми маємо значну кількість засобів використання цифрового водяного знаку в дані. Мало досліджувалося

питання захисту ЕД шляхом накладання цифрового водяного знаку. В деяких працях було запропоновано методи побудови цифрового водяного знаку для документів різної фізизної природи, якій можуть використовуватися для перевірки надійності, достовірності та прихованості інформації, що передана у системі [24].

Комплексне використання електронного цифрового підпису та цифрового водяного знаку має у перспективи велике значення, однак ця ідея не має суттєвих реалізацій. Все це обумовлює подальші дослідження методів захисту інформації на базі комплексного використання відповідних елементів.

В декількох працях неведено метод виявлення фальсифікованого інформаційного блоку шляхом введення надлишковості інформації. Однак такий метод обмежен лише пошуком тільки у одному блоці. Таким чином виникає актуальна задача вдосконалення цього методу для отримання можливості аналізувати та виявити фальсифікації у декілких блоках інформації.

Таким чином, встановлено, що в теперішній час має місця розрив між бажаними потребами в захисті системи електронного обсягу документів і можливостями, які можуть надати методи та засоби, що існують. Тому задача дослідження та побудови нових методів виявлення фальсифікації електронних документів є актуальною.

1.2 Інформаційна безпека електронних документів

Для вирішення основної проблеми –забезпечення гарантованого захисту інформації, яка функціонує у інформаційних системах обробки електронних даних, спочатку сформулюємо основну мету захисту інформації. Це можна виришити за рахунок аналізу та классифікації всіх можливих загроз, які можуть навести до фальсифікації вихідної інформації.

Інформаційна безпека це одна з основних складових частин

електронного документообігу, що набуває розвитку за стандартами, що відповідають існеючим законам. Без безпеки та захисту електронних документів не можливо уявити собі сучасну інформаційну систему, у томі числі і електронного обігу документів.

Якість формування відповідних електронних документів стає основним фактором, який визначає ефективність управління організаційною структурою у целому. Докуметообіг повинен бути побудован таким чином, щоб була присутня можливість якісного контроль за формуванням, виконанням, пошуком, використанням, а також надійним зберіганням та захисту інформації, яка є основою системи. Системи електронного документообігу – організаційно-технічні системи, що забезпечують процес створення, керування доступом та розповсюдження електронних документів по комп'ютерною мережею.

Якщо ми вивчаємо електронно середовище, то бажано розумити, що процеси обробки документованої інформації є складний організаційно-технічний процес, який може супроводжуватися загрозами у цільності та якості інформації, о стає причиною втрати документом своєї юридичної значущості [27].

Під безпекою електронного документообігу розуміють захищеність інформації від перетворення і знищення, неможливість отримання суб'єктами непередбачених прав доступу [28]. Захищеність інформаційних ресурсів від впливу, направленого на порушення їх конфіденційності, цілісності та достовірності.

При розробці системи захисту необхідно провести аналіз ймовірних загроз, які виникають у електронних документів. Сучасні системи захищеного документообігу зобов'язані забезпечити захищений обмін юридично значимими електронними документами. Такий процес потрібно забезпечувати як програмними, так і технічними засобами.

Сучасні методи обробки, передачі і збереження інформації спричинили виникненню загроз, пов’язаних з можливістю втрати, спотворення та несанкціонованого отримання даних.

Загрози інформаційної безпеки – сукупність умов та факторів, які можуть спричинити потенційну небезпеку, що може призвести до різних непередбачуваних подій, таких як витік інформації, модифікація та знищення інформації [29–31]. Всі ймовірні впливи, які здатні завдати шкоди системі, є загрозами безпеці системи електронного обігу документів.

В теперішній час відомо великий перелік загроз інформаційній безпеці. До нього входить майже сто найменувань. Аналіз всіх цих загроз проводиться з метою визначення набору вимог до системи захисту електронного обігу документів. Крім цього бажано провести аналіз, на основі класифікації загроз у відповідності з їх ознаками. Як відомо, кожна ознака класифікації, яку ми виділили повинна відповідати одній спільній вимогі до системи захисту інформації у системі ЕД і дозволяти диференцувати вимоги щодо захисту інформації. Класифікацію загроз безпеки ЕД потрібно провести через те що інформація піддається впливу великій кількісті факторів. Це наводить до того, що формалізація завдання стає неможливою завдяки опису повної множини загроз. (дивитись рисунку 1.3 [22, 32].)

Загроза конфіденційності може виникнути, як результат таких злочинних дій, як крадіжки, зміни маршрутів руху електронного документу, перехоплення інформації.

Загрози порушення конфіденційності спрямовані на розголошення конфіденційної або секретної інформації. При реалізації цих загроз інформація може бути відомою для суб’єктів, які не мають до неї доступу. Порушення конфіденційності є причиною отримання суб’єктами несанкціонованого доступу до електронних документів [33].

Загрози цілісності – це загрози, які характеризуються тем, що інформація втрачає значимість, юридичну силу при їх реалізації. Загрози цілісності інформації, яка зберігається в мережі електронного обігу

документів, які спрямовані на її редагування чи перетворення, модифікацію та знищення. Порушення цілісності інформації може мати випадковий і навмисний характер. Доступність характеризує можливість несанкціонованого доступу до документів, що зберігаються в системі електронного документообігу в будь-який момент часу [34–36].

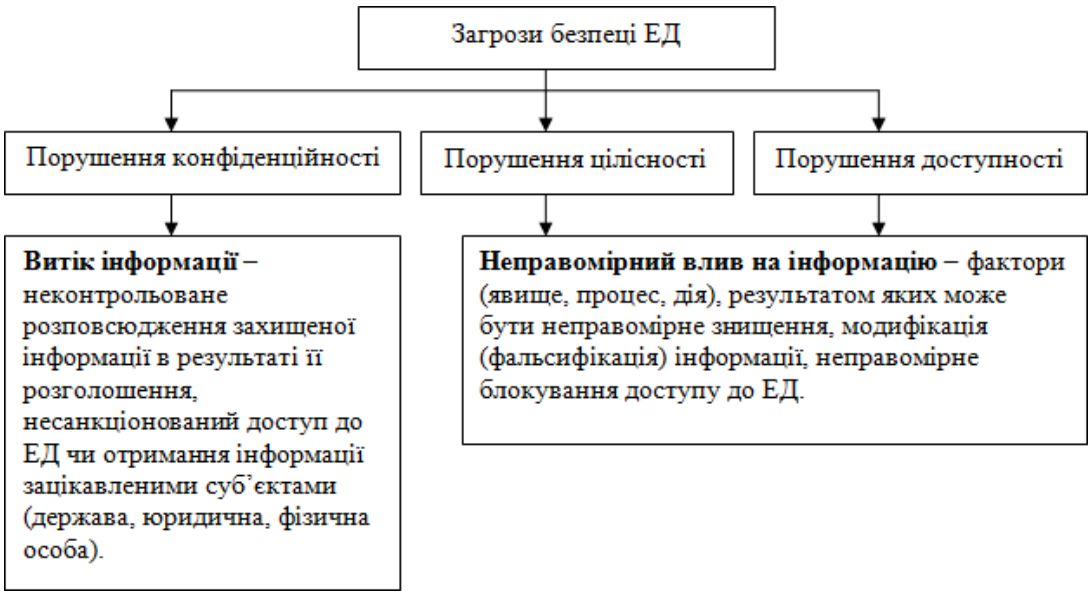


Рисунок 1.3 – Класифікація загроз безпеці електронного документу

Проаналізував все вищесказане, можно встановити що система електронного документообігу, яка відповідає вимогам захищенності, потрібна мати таку реалізацію механізмів захисту: забезпечення цілісності документів, безпечного доступу, конфіденційності та достовірності документів.

Захист інформації від несанкціонованого доступу – заходи, що унеможливлюють доступу до інформації зацікавленими суб'єктами з порушенням встановлених правових норм. Захист інформації від витоку – діяльність спрямована запобіганню неконтрольованому розповсюдженню інформації від її розголошення, несанкціонованому доступу до інформації і отриманню її зловмисниками [37–39].

1.3 Основні властивості та реквізити електронного документу

Електронний документ представляє собою електронний аналог паперового документу, який було створено на захищенному цифровому носії. Електронний документ – документ, який створюють та використовують тільки в межах комп'ютерної системи.

В Законі України «Про електронні документи та електронний документообіг» зазначено, що електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [40]. Юридична сила електронного документу не може бути заперечена виключно через те, що він має електронну форму. Оригіналом ЕД вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з ЕЦП його автора, накладанням якого й завершується створення документа. Склад та порядок розміщення обов'язкових реквізитів ЕД визначається законодавством [41].

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання ЕД є відображення інформації, яку він містить, технічними засобами (комп'ютерне оснащення, програмне забезпечення тощо) або на папері (у спосіб переведення його в друковану форму за допомогою сучасних технічних пристроїв) у формі, придатній для сприймання його змісту людиною [42–45].

Юридична чинність і доказовість ЕД надається за допомогою електронного підпису. Згідно з ст. 6 Закону України «Про електронні документи та електронний документообіг» [40], ЕЦП є обов'язковим реквізитом електронного документу, що використовується для ідентифікації автора чи особи, яка підписала документ. ЕЦП – це атрибут, який дозволяє, на основі криптографічних методів, встановити авторство і цілісність електронного документу [41, 42]. Законодавець визначив, що електронний

документ набуває юридичної сили з моменту накладання електронного цифрового підпису.

Важливе місце в ЕД має задача ідентифікації користувачів, виришити яку забовязан такий атрибут ЕД, як електронний цифровий підпис. ЕЦП зручний та надійний інструмент ідентифікації особи, який знайшов своє застосування при для здійснення угоди у розосередженому режимі та обміну юридично значимою документацією міє суб'єктами правової діяльності. ЕЦП дає гарантію на достовірність інформації, що обробляється, забезпечує її цілісність та дозволяє побудовати корпоративну систему обміну електронними документами [43]. Правовий статус електронного документу визначається використанням ЕЦП, який забещзпечує ідентифікацію автора документа, що підписан [40]. Електронний документ складається з таких елементів, як його зміст, реквізити і носій.

Зміст електронного документу – це документована інформація (відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх подачі).

Реквізити електронного документу повинні розміщуватись відповідно до чинних нормативних документів та стандартів. Зокрема, згідно з ДСТУ 41632003, таких обов'язкових реквізитів п'ять [44]:

1) найменування установі, що створила цей документ;

2) геолокація установи що створила цей документ (або його 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) інформативна складова документа (зображення, звук, текст) повинна бути незалежною від конкретного матеріального носія;

2) існує універсальна система кодування (бінарний код), яка однакова

для фіксації документів будь-якої знакової системи;

4) відсутність індивідуального носія для кожного з документів, розміщених на окремому комп'ютері або сервері;

5) «інтерактивність» документа.

Остання специфічна властивость електронного документа порождає питання про його цілісность. Однак, як відомо, при передачі документа каналами зв'язку відбувається його поділ на множину дрібних складових. Після прийому вони з'єднуються в цілісний об'єкт на робочій станції особи-одержувача. Але при цьому не можна виключати деякі технічні збої у процесі передачі інформації, у результаті яких документ може бути пошкоджений .

Усі електронні документи містять досить різноманітне програмне забезпечення, однак це не є критичним фактором впливу на передану інформацію. Різні дані можуть бути по різному оброблені. Так одні незалежно від комп'ютера-прийомника можуть бути адекватно сприйняті, в той же час для інших необхідно використання спеціальних додатків, без яких документ не функціонує.

Носій електронного документу – це матеріальний об'єкт, на якому інформація може бути записана і відтворена в електронно-цифровому вигляді. Існує велика кількість різноманітних носіїв ЕД, якості кожного з них повинні залежати від особистостей той інформації, яка повинна оброблятися.

Всі електронні документи мають специфічні ознаки та функції. Можна виделити таки характерни ознаки електронних документів:

1) Електронні документи є програмно-технічно залежними продуктами;

2) мають широкий спектр інформаційного відображення;

3) форма електронних документів може бути відокремлена від змісту, а зміст документів може бути фрагментований, тобто фізично документ може зберігатись в кількох різних файлах;

4) електронні документи можуть містити посилання, які не підлягають контролю з боку авторів;

5) електронні документи зберігають на фізичних носіях інформації

(магнітні, оптичні пристрої), що не можуть гарантувати довготривале збереження інформації (процес розмагнічування, механічне ушкодження, фізичне та моральне старіння програмно-технічних засобів) [45].

Висновки до розділу 1

Дослідження принципів впровадження електронного документообігу показало, що є очевидною необхідність захисту документованої інформації представленої в електронному форматі. Попри низку переваг використання електронного документообігу, залишається ряд невирішених або малодосліджених питань, пов’язаних з забезпеченням інформаційної безпеки електронних документів. Виходячи з аналізу основних властивостей електронних документів, можна виділити основні напрямки – забезпечення цілісності, достовірності та конфіденційності, на які слід акцентувати особливу увагу при виборі засобів захисту.

2 КРИПТОГРАФІЧНИЙ ТА СТЕГАНОГРАФІЧНИЙ ЗАХИСТ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Криптографія – це наука, яка вивчає способи перетворення інформації з метою захисту її від незаконних користувачів [46]. Основне завдання криптографії, з часу її витворення, це розробка методів шифрування інформації. Таке відбувалося до недавнього часу, однак, у сучасності сфера використання криптографії значно збільшилась. Це є результатом значного використання різноманітних інформаційних у богатьох областях людської діяльності. Однак всі ці нові задачі, які виришують за допомогою криптографічних моделей, методов та методик так або інакше пов'язане проблемами захисту інформації.

Особливістю застосування вище перелічених методів виникає в зв'язку з теми умовами, при яких відбувається процес обробки та передачі інформації. Важливо відмітити, що у сучасності при значної кількості різноманітних операцій, наприклад, при прийнятті колективних рішень при розподіленої управляючій системи, при проведення фінансових операцій за допомогою сучасних систем транзакцій виникає необхідність підписання документів. В цих випадках необхідно використовувати таки засоби, які забезпечували те, що інформація в процесі її обробки буде непошкоджена та допуск до неї буде обмеженим. Це доступно лише при використанні и лише методів криптографічного захисту.

Криптографія, як галузь людської діяльності має мету: забезпечити конфіденційності, цілісність, автентичність даних [47]. Основу гарантування інформаційної безпеки в інформаційно-телекомунікаційних системах становлять криптографічні методи та засоби захисту інформації. [48]. Застосування цих методик, методів та моделей є гарантією того, що не можливо порушити конфіденційність ЕД.

Можливості криптографії вже відомі, вона давно пройшла шлях свого

становлення і існуючі методи можуть бути легко адаптовані до задач захисту електронних документів.

Використання криптографічних методів має значну кількість практичних застосувань. Однак найбільш поширеними серед них єтаки, як передача інформації, з обмеженим доступом, в сучасних інформаційних мережах, забезпечення дійсності файлов, які були передані, збереження даних на різноманітних носіях у вигляді шифрів. Криптографія дає можливість скрити інформацію, яка цього потребує, таким чином, що будь-яка операція по її обробці можлива тільки при наявності відповідного ключа. Для класифікації методів, що використовуються у криптографії, у теперешній час відомо велике різноманіття підходів [49]. В якості приклада можна привести класифікацію криптографічних методів за способом дії на дані (рисунок 2.1.)

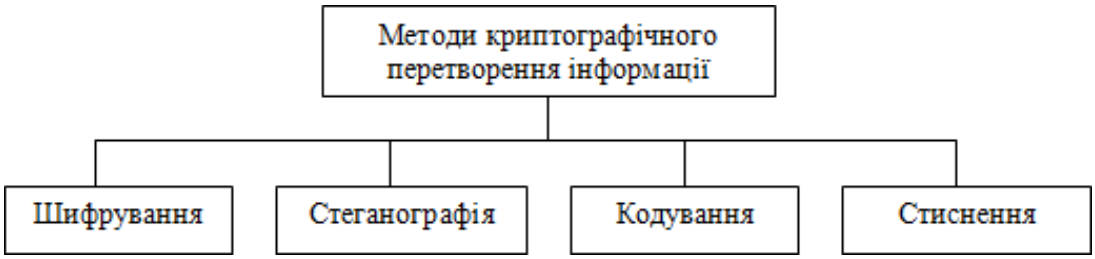


Рисунок 2.1 – Класифікація методів криптографічного перетворення інформації

Криптографічні перетворення даних здатні вирішити головні проблеми захисту інформації: проблему конфіденційності і проблему цілісності [50].

Безумовно шифрування можна визначити, як найважливіший способом криптографії, що використовується для приховування інформації в сучасних інформаційних системах. Сучасну криптографію можна поділити на таки складові: симетричні системи шифрування, асиметричні системи, системи ЕЦП та управління ключами [50]. Захист ЕД у сучасності проводиться з використанням різноманітних симетричних системи, які можна визначити як:

підстановки, перестановки, гамування та блочні шифри.

Основою більшості методик забезпечення кібернитичного захисту ЕД безумовно є використання набору різноманітних криптографічних шифрів і процедур шифрування. Забезпечення захисту електронних документів організується таким чином, шо при цьому використовуються криптографічні методи, які дозволяють обробити дані таким чином, що до їх змісту можна отримати доступ лише особам, які володіють відповідний ключ шифрування. Шифрування – це процес перетворення відкритих даних в закриті за визначеними криптографічними правилами [51]. Шифрування забезпечує функціонування основних властивостей ЕД, таких як: конфіденційність, цілісність та достовірність. Криптографічне перетворення в математичній формі можна представити у вигляді алгоритмів шифрування (2.1) та дешифрування (2.2) інформації.

$$F(T) = Z \tag{2.1}$$

$$R(Z) = T' \tag{2.2}$$

де T – відкритий текст документа;

Z – зашифрований текст;

F – функція шифрування, яка виконує криптографічні перетворення;

T' – розшифрований текст,

R – функція розшифрування, що виконує обернені криптографічні перетворення.

Для будь-якого шифру можна визначити найбільш важливу характеристику – криптографічну стійкість. Крипостійкість безумовно є головною характеристикою алгоритму шифрування, що свідчіть про складність для зловмисник можливости отримання вихідного тексту ЕД, якщо він не володіє ключем шифрування [52].

В загальному вигляді схема шифрування-дешифрування електронних документів представлена на рисунку 2.2.

Засоби криптографії є одними з надійних способів захисту інформації,

оскільки захищається безпосередньо сама інформація, а не доступ до неї. Особливосттю використання криптосистем є те, що потрібно у деякій час проводити її вдосконалення у відповідності до розвітку сучасних методів криптографічного аналізу, що відповідно призводить до ускладнення роботи криптоаналітика. Модифікація КС відбувається різноманітними способами, які включають і: метод збільшення довжини ключа; метод, який враховує багатократно шифрування та інш.. Багато криптографічних систем захисту даних у своїх методах використовують Хеш-функції. Найбільше застосування хеш-функцій в криптографії отримали у схемах електронного цифрового підпису. Засоби криптографії є одними з надійних способів захисту інформації, оскільки захищається безпосередньо сама інформація, а не доступ до неї.

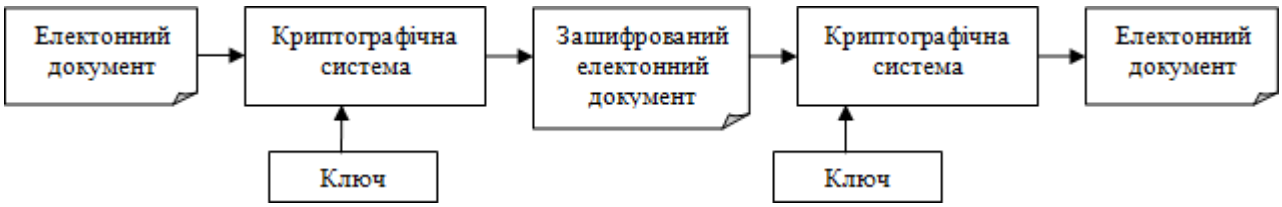


Рисунок 2.2 – Схема шифрування-дешифрування електронного документу

Хеш-функції є необхідним елементом багатьох криптографічних систем. Основною сферою застосування хеш-функцій в криптографії є схеми електронного цифрового підпису.

У процесі обміну електронними документами через телекоммунікаційну мережу ЕЦП знижують часови та системні витрати на обробку данихв, для пошуку потрібних даних використовується менша кількость часу. Однак в той же час виникає складна проблема ідентифікації як автора, так його самого документу. Таким чином потрібно виришити дві задачі: хто автор, та яка достовірность отриманої інформації. В традиційних, паперових документах є тісний зв'язок між інформацією, що наведена у документі та власноруч поставленим підписом, який пов’язан з папером. В

електронних документах на різноманітних цифрових носіях такого зв'язку немає.

Таким чином, традиційні способи встановлення достовірності документів при обороті їх в електронній формі є не легітимними. Вирішити цю задачу для електронних документів можна з використанням електронного цифрового підпису [40].

Електронний цифровий підпис – це реквізит електронного документу, отриманий в результаті криптографічного перетворення набору інформації з використанням закритого ключа електронного цифрового підпису, який додається до цього набору або логічно поєднується з ним. ЕЦП дає можливість в цілісність документу та ідентифікувати його автора. Ше важливою функцією ЕЦП є гарантія відсутноісті порушення даних в електронному документі [50].

Використання ЕЦП дозволяє отримати [51]:

1) контроль цілісності ЕД за умови будь-якого випадкового чи навмисного спотворення документа;

2) захист від фальсифікації електронного документу;

3) гарантування авторства і неможливість відмови від нього.

Технологія використання ЕЦП передбачає електронний обмін інформацією між учасниками телекоммунікаційної мережі системи електронного обігу документів. Це забезпечується тим, що і відправник, і отримувач мають пару ключів: відкритий і закритий, які генеруються спеціально для кожного документу. Закритий ключ повинен зберігатися у відправника в таємниці та використовується ним при генерації ЕЦП. Відкритий ключ відомий отримувачеві, знаходиться у нього та використовується для перевірки електронного цифрового підпису ЕД. Система ЕЦП складається з процедуиу формування підпису та процедури його перевірки. Особливостью системи ЕЦП є принципова неможливість підробки цифрового підпису користувача, якщо немає володіння секретним ключем підпису. Це призводить до необхідності тримати ключ в таємниці та

забезпечити його надійний захист [39]. На рисунку 2.3 представлена найбільш поширшена схема формування ЕЦП.

При побудові ЕЦП потрібно використовувати закритий ключ автора документу, а для процесу перевірки підпису – відкритий ключ. Спочатку відправник генерує пару ключів і повідомляє відкритий ключ отримувачеві для подальшої перевірки підпису. Наступна дія відправника є обчислення значення хеш-функції електронного документу [46].

У зв'язку з тим, що електронний документ може бути достатньо великим, то тоді ЕЦП можна накладати не на сам документ, а на його хеш. За правилами обчислення Хешу, це виконується з використанням криптографічних хеш-функцій. Цей крок надає гарантії щодо виявлення змін в документі в процесі перевірці підпису. Таким чином основна властивість Хеш-функції у тому, що вона виконує операції обчислення хешу електронного документа. Бажано розуміти, що Хеш (*H*), за визначенням, – це фіксована кількість бітів, яка є повною характеристикою всього документу. В цьому випадку автор робить шифрування хешу з використанням свого таємного ключа, а пара чисел, що отримана в результаті, є ЕЦП даного ЕД. Потім підписаний ЕД надходить до отримувача. Використання хеш-функцій дозволяє формувати криптостійкі контрольні суми ЕД [42].

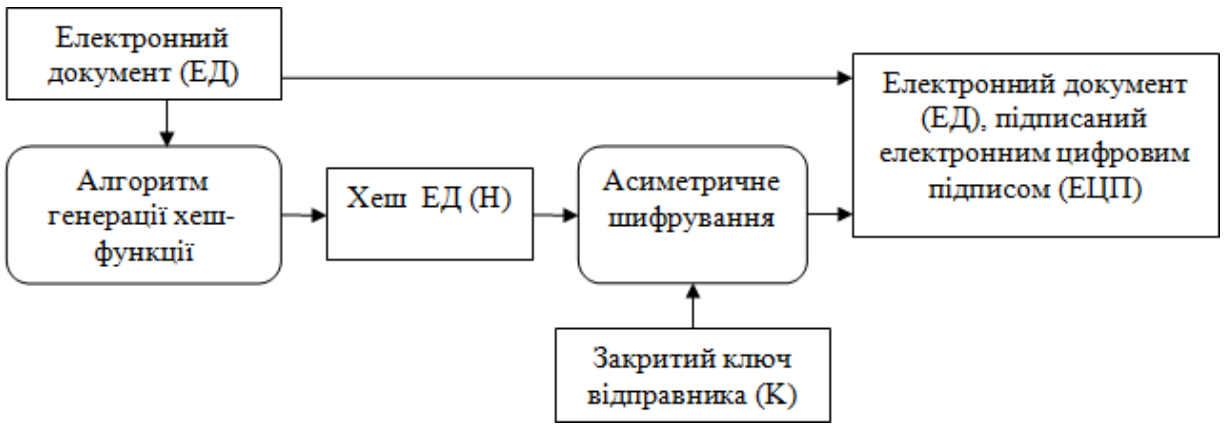


Рисунок 2.3 – Схема формування електронного цифрового підпису

В випадку перевірці ЕЦП отримувач ЕД проводит операцію дешифрування прийнятого хешу (Н) відкритим ключем автора. В той же час, отримувач повинен самостійно за допомогою хеш-функції (*H*) провести обчислення хешу (*h*) отриманого ЕД і порівняти його з дешифрованим. Якщо *(H) і (h)* співпадають, то ЕЦП – вірний. В іншому випадку – ЕЦП фальсифікований, або змінено вміст ЕД. Співпадання *(H) і (h)* є критерієм цілісності ЕД і підтвердженням його авторства.

Запропонована технологія асиметричного шифрування надає гарантію достовірності авторства ЕД. Зловмисник не має можливості поставити підпис від чужого імені, оскільки не має доступу до його секретного ключа. Достовірність ЕД визначається особливостями функцій хешування.

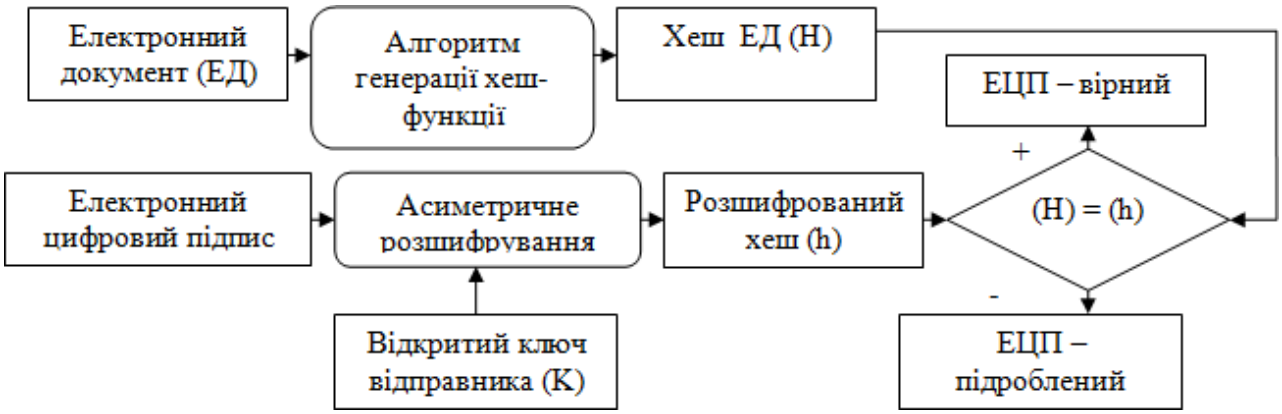


Рисунок 2.4 – Схема перевірки електронного цифрового підпису

При використанні хеш-функцій в процесі шифрування повідомлень можна виділити такі переваги [32]:

1) хеш-функцію можна використовувати для перетворення будь-якого вхідного тексу в потрібний формат;

2) хеш ЕД має меншу довжину, ніж самий ЕД і алгоритми обчислення хеш функції швидші ніж алгоритми ЕЦП;

3) для підпису ЕД великого об’єму його потрібно ділити на блоки, лише потім ставити ЕЦП, використання хеш-функцій цього не потребує.

Разглянемо приклади деяких алгорітмів цифрового підпису. як перший зразок розглянемо алгоритм ЕЦП Ель-Гамаля (EGSA).

В цьому алгорітмі цифровий підпис виконує роль поїску було зміни інформації електронного документу та встановити авторство цих дій. Для режиму підпису необхідна наявність фіксованого значення – хеш-функції h (M), причому значення цієї функції повинни знаходится в проміжку (1, p-1). Таким чином процедура електронного підпису повинна складатися з множини таких операцій:

1) обчислюється хеш-функція ЕД M:m= h(M)

2) обирається випадкове число $1< k < p-1$ взаємно просте з $p-1$ та обчислюється $r= g^k \bmod p$;

3) обчислюється число $S=(m-xr)^k (\mathrm{mod} p-1)$

4) підписом повідомлення M є пара (r,s).

Перевірка достовірності підпису документу здійснюється таким чином:

1) виконується перевірка умов $0 < r < p$ і $0<s<p-1$, при тому що хоча б одна з умов виконується, підпис вважається невірним

2) виконується обчислення хеш-функції ЕД M:m= h(M)

3) підпис вважається вірним, при виконанні рівності $(y^r r^s) \bmod p \equiv g^m (\mathrm{mod}\ p)$

Наступним буде розглянуто алгоритм цифрового підпису RSA. Ця система отримала свою назву в честь її розробників R.Rivest, A.Shampir, L.Adleman. Ця схема стала першою практичною реаліщзацією підпису електронного документу з використанням криптографічних систем з відкритим ключем. Відомо, що при використанні алгорітму RSA суб'єкт, котрий підписує документ зобов'язаний сформувати два ключі: закритий та відкритий.

При цьому значення (K_o , r) , які відповідають відкритому ключу підпису, відправник надсилає всім ймовірним користувачам його ЕД. Ці значення потрибно використовувати при перевірки достовірності та забезпечення гарантій авторства ЕД. Друга пара значень (K_c , r) повинна

зберігатися у таємниці і виконує роль секретного ключа автора. Таким чином загальна процедура формування підпису документу M повинна складатися з наступних кроків:

- обчислення хеш-функція ЕД M:m= h(M);
- на базі хеш-функції, що отримана, та закритого ключа проводяться обчислення підпису $S = m^{K_c} \mod r$, пара M , та потім отримаємо підписаний ЕД, який передається отримувачу.

При чому можливість сформувати підпис S є лише у власника закритого ключа K_c .

Для перевірки достовірності підпису необхідно провести наступну процедуру:

- отримувач повинен провести обчислення значення хеш-функції M:m= h(M);
- отримувач повинен розшифрувати хеш-функції відкритим ключем відправніка Ko перетворюючи значення підпису S за алгоритмом RSA: $S = m^{K_O} \ mod \ r$;

Наступним алгоритмом цифрового підпису DSA є криптографічний алгоритм, який використовується при створенні ЕЦП, але не використовується для шифрування, як попередні алгоритми. В цьому випадку підпис потрібно створювати таємно, щоб тільки один суб'єкт мав можливість створити підпис, в той же час провесті перевірку підпису на коректність може довільний користувач. Цей алгоритм був побудований на принципу складності обчислення логарифмів в кінцевих полях. Як і попередних схемах, DSA має дві складові: алгоритм створення підпису та алгоритм його перевірки. При своєму функціонуванні ці алгоритми по перше обчислюють хеш, за допомогою криптографічноїу хеш-функції. Алгоритм створення підпису повинен використовувати хеш та таємний ключ, алгоритм перевірки підпису – хеш і відкритий ключ [33]. Схема побудови ЕЦП за схемою DSA представлено на рисунку 2.5.

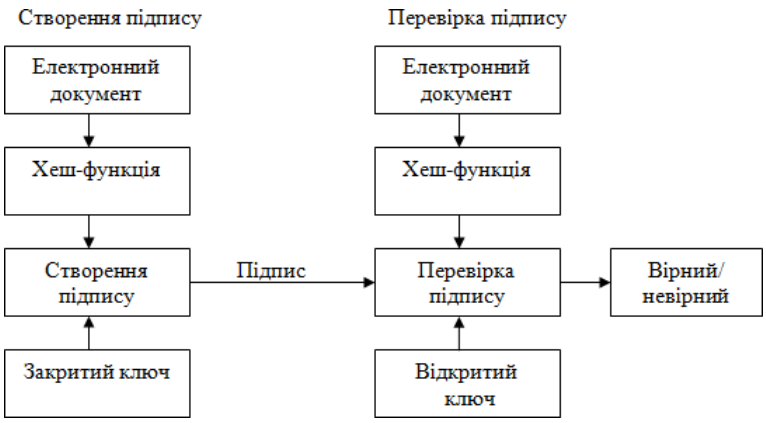


Рисунок 2.5 – Схема побудови електронного цифрового підпису за схемою DSA

2.2 Стеганографічний захист електронних документів

Наступним апаратом, який досить часто використовується для захисту електронних документів, в процесі обробки, зберігання, та передачі інформації про документ є цифрова стеганографія. Стеганографія – метод організації зв'язку, який приховує факт його існування [75–79]. Засоби стеганографії характеризуються тим, повідомлення, яке необхідно приховати вбудовується в деякий об'єкт. Цей об'єкт можна відкрито переслати існуючій мережею. Основна різниця стеганографії від криптографії, в тому, що криптогафія пов'язана приховувати зміст ЕД, а стеганографія закриває сам факт його існування. Найбільш ефективним є комплексне використання стеганографії з методами криптографії.

На відміну від криптографії, в теперішній час, використання стеганографії в інформаційних системах ЕД, недостатньо розвинута, а її методи недостатньо пристосовані до завдань захисту ЕД. Це слід з такими недоліками, що властиві їй, як недостатньо надійність і стійкість. Однак, разом з цим, використання систем, які базуються на стеганографії, в галузі електронного обігу документів дає можливість вирішити ряд важливих проблем. Серед яких варто відмітити забезпечення прихованого збереження і

передачі ЕД, забезпечення непомітності комунікації між відправником та отримувачем повідомлень, виявлення каналів витоку ЕД, а також внесення прихованого ЕЦП [47].

Стеганографічні системи можуть виконувати ряд завданнь, щодо захисту авторських прав на електронний документ за умов різного роду спроб порушення та атак. Для цього досить часто використовують системи цифрового водяного знаку, які дозволяют забезпечити ідентифікацію автора ЕД. Важливої рисою цих систем є те, що стеганографічна система дозволяє вбудувати цифрові дані одного об'єкту в інший і вилучати приховану інформацію.

Ще одним з механізмів захисту електронних документів є використання цифрових водяних знаків (ЦВЗ), з метою захисту авторських прав творця ЕД. Під ЦВЗ розуміють такі цифрові мітки, що впроваджуються в ЕД з використанням стеганографічних перетворень спеціального призначення [49]. Практичне застосування характеризується такими аспектами, як захист авторських прав, захист від копіювання, отримання цифрового відбитку, приховування факту обміну інформацією. У теперешній час є багато різноманітних систем впровадження ЦВЗ в різні види інформаційного продукту. В той же час, захист ЕД при наявності вбудовоної ЦВЗ є не дсить вивченим. Е кілька можливих способів використання ЦВЗ, як в електронні, так фізичні документи [25, 49].

Представимои структуру стеганосистеми за допомогою таких позначення: нехай С – цифрове зображення, ЦВЗ, І – цифровий документ, зображення, в яке вбудовується ЦВЗ має назву контейнерм, тоді К – контейнер, що повний. Процеси Е, Т, D – відповідно процес вбудовування ЦВЗ в документ, перетворення заповненого контейнера і вилучення ЦВЗ. Стандартну схему стеганографічної системи можна показати наступним чином, як на рисунку 2.6 [17].

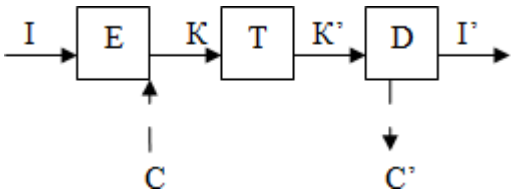


Рисунок 2.6 – Схема стеганографічної системи

В перетворення Т повного контейнера К’ можна включати таки процеси, як передача даних по мережі, атаки на ЕД, різної природи та інші. Головною характеристико. стеганосистеми є приблизна рівність між значеннямі порожнього і заповненого контейнера $I \approx K$.

Ця умова повинна бути виконаною для того, м Математичну модель стеганографічної системи у вигляді (2.3, 2.4). Спочатку виконується генерація ЦВЗ (2.3).

$$Z = F(R, K, I), \tag{2.3}$$

де Z – множина можливих ЦВЗ,

R – ключі,

K – контейнери,

I – приховані дані, ЕД.

Процес вбудовування ЦВЗ $Z\ (m,\ n)$ в вихідний цифровий документ $I°(m, n)$ можна показати формулою (2.4)

$$I^{'} = I(m,\ n) \otimes L\left(m,\ n\right)Z\left(m,\ n\right)p(m,\ n), \tag{2.4}$$

де $L\,(m, n)$ маска вбудовування ЦВЗ, ,

$p\ (m,\ n)$ проектуюча функція яка залежить від ключа і відповідає за розподіл ЦВЗ по площині цифрового документу.

У наш час розроблені різні методи накладання цифрового водяного знаку,класифікація яких показана на рисунку 2.7 [43].

За допомогою просторові методи побудови ЦВЗ можливо провести формування ЦВЗ для фізичних та електронних документів. До таких методів можна віднести:

Метод LSB (Last Significant Bit). Суть даного методу полягає в заміні молодших бітів в контейнері на біти прихованого повідомлення. Різниця між порожнім та заповненим контейнером має бути не відчутною для органів сприйняття людини. Основними перевагами даного методу є простота реалізації, можливість приховувати в відносно невеликих зображеннях достатньо великі об’єми інформації, а також те, що людський зір в більшості випадків не здатний помітити зміни в молодших бітах.

Метод випадкового інтервалу. На відміну від методу LSB, в якому кожний біт прихованого повідомлення записується послідовно в молодші біти, метод випадкового інтервалу дозволяє здійснювати випадковий розподіл бітів цього повідомлення по контейнеру, в результаті чого, відстань між двома вбудованими бітами прихованого повідомлення визначається випадково. Недоліком даного методу є те, що біти розміщуються в тій самій послідовності, що і в самому прихованому повідомленні.

Варто відмітити, що всі вищеописані методи є вдосконаленими версіями методу LSB.

Безпека інформації при її передачі відкритими каналами зв’язку може забезпечуватися методами, як криптографії, так і стеганографії. Проте, враховуючи, що жоден з цих напрямків на даному етапі свого розвитку не може самостійно розв’язати всі питання, пов’язані з захистом ЕД, забезпечення інформаційної безпеки електронного документообігу можливе лише в умовах комплексного використання криптографічних і стеганографічних засобів захисту.

Рисунок 2.7– Класифікація методів накладання цифрового водяного знаку

Дослідження, результати яких було представлено у другому розділі були присвячені захисту електронних документів з використанням аппарату стеганографії та криптографії. В розділі представлені основні схеми алгоритмів, що використовуються при побудовви електронного цифрового підпису та цифрового водяного знаку.

Наведено результати порівняльного аналізу запропанованих методів захисту інформації, яка належить електронному документу.

3 МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ ФАЛЬСИФІКАЦІЙ В ЕЛЕКТРОННИХ ДОКУМЕНТАХ НА ОСНОВІ ВИКОРИСТАННЯ ХЕШ-ФУНКЦІЙ

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

Хеш-функція є найпростішим варіантом електронного цифрового підпису, який є гарантом цілісності, достовірності електронного документу та підтвердження авторства електронного документу. В попередньому розділі були запропоновані алгоритми обчислення хеш-функції електронного документу, на основі яких можна побудувати механізми виявлення фальсифікованих фрагментів інформації. Узагальнена схема використання хеш-функцій показана на рисунку 3.1.

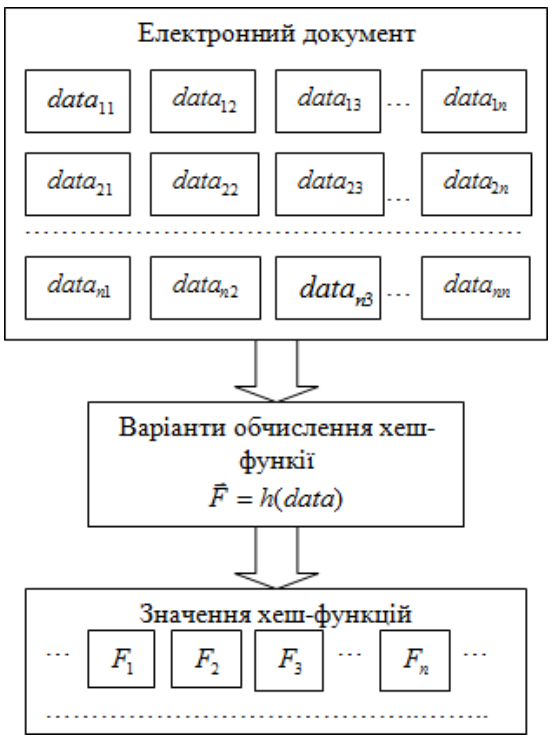


Рисунок 3.1 – Узагальнена схема використання хеш-функцій

Використання алгоритмі хешування для забезпечення цілісності інформації має ряд переваг, серед яких:

- відносно невисока надлишковість;
- невелика кількість криптографічних перетворень;
- можливість контролювати довжину хеш-коду.

Варіантів побудови хеш-функцій існує дуже багато, наприклад, на основі використання матричних криптографічних перетворень, які описані в попередньому розділі.

Найбільш типовими способами отримання хеш-функції електронного документу є:

1) обчислення хеш-фунції всього документу, результат – одна контрольнасума, яка характеризує повністю весь електронний документ;

2) обчислення хеш-функції для кожного запису в блоці інформації, результат – множина значень хеш-функцій, яка відповідає кількості записів в ЕД;

3) обчислення хеш-функції для блоку даних, результат – множина значень хеш-функції, яка дорівнює кількості блоків інформації електронного документу.

Кожен із способів має певні особливості, переваги та недоліки, розглянемоїх детальніше.

Отримана в результаті виконання алгоритму хешування контрольна сума, яка характеризує повністю весь документ, може бути найпростішим варіантом електронного цифрового підпису. Така схема, згідно властивостей ЕЦП, дозволяє забезпечити гарантію авторства електронного документу, але не дає можливості виявити в яких фрагментах інформації відбулися порушення цілісності.

Обчислення хеш-функції повністю всього електронного документу, дивись рисунку 3.2.

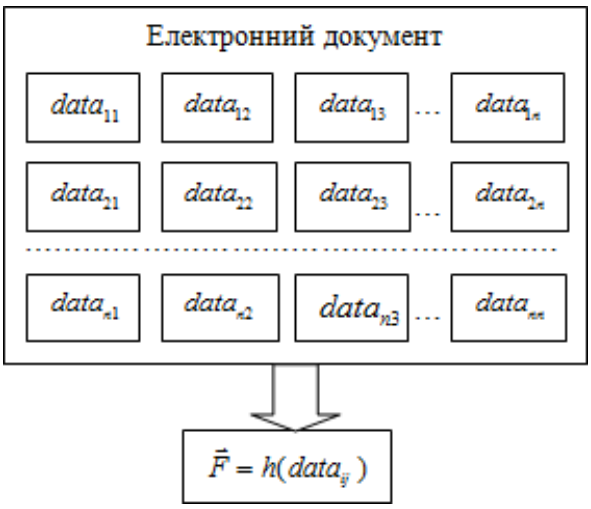


Рисунок 3.2 – Схема отримання хеш-функції електронного документу

Для наступних двох схем введемо позначення, нехай інформація представлена у вигляді записів довільного розміру, позначимо їх через множину:

$A = \{\vec{a}, \vec{a}, \ldots . \vec{a}\}$ – множина двійкових векторів;

$F = \{f_m, f_{m-1}, \ldots, f_{m-k}\}$ – множина двійкових векторів, хеш-кодів фіксованого розміру.

Обчислення хеш-функції для кожного запису в блоці інформації, як на рисунку 3.3.

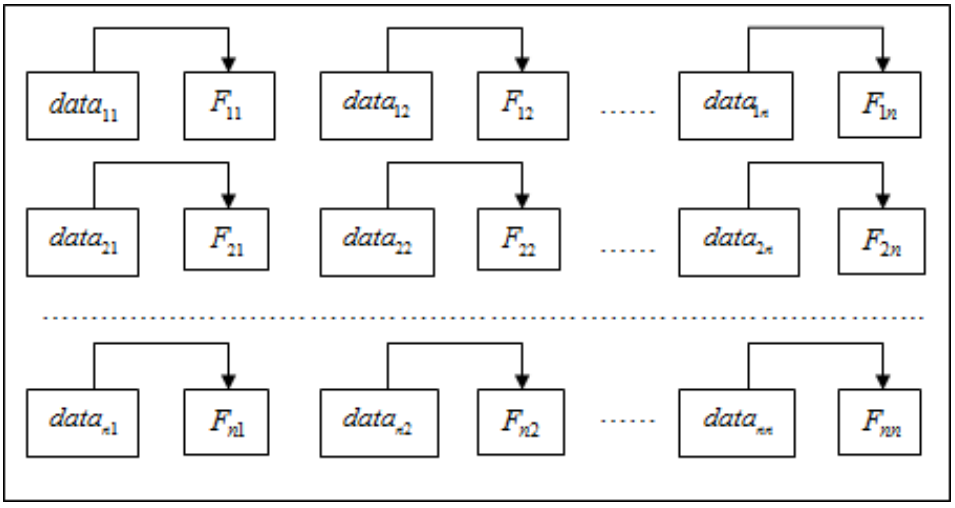


Рисунок 3.3 – Схема отримання хеш-функції для кожного запису в блоці електронного документу

Перевагою описаного способу обчислення хеш-функцій є можливість визначення запису, в якому відбулися зміни. Недолік – висока надлишковість при контролі цілісності послідовності записів невеликого розміру.

Обчислення хеш-функції для блоку даних, дивись рисунок 3.4.

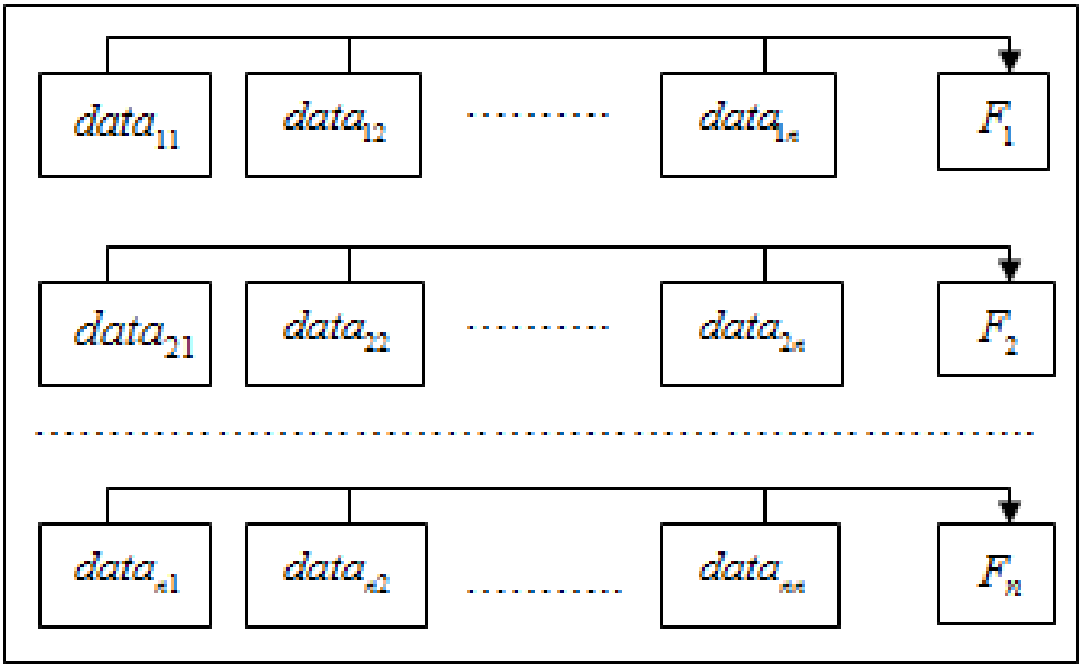


Рисунок 3.4 – Схема отримання хеш-функції для блоку даних електронного документу

Для описаної схеми характерна невисока надлишковість, проте, суттєвим недоліком є відсутність можливості виявлення фальсифікацій в окремому записі вкожному з блоків.

3.2 Метод виявлення фальсифікованого фрагменту електронного документу шляхом перехресного хешування

Захист електронних документів має на увазі не лише факт непошкодження інформації. У значній кількості випадків життєво важливим є знання про місце в електронному документі, де ця інформація зазнала змін. Тому, актуальним стає задача розробки методів визначення підробок в

створенному електронному документі. Вирішення цієї задачі, може бути побудовано на методі, використовує алгоритмв хешування, розглятуті раніше.

Цей методу базується на обчисленні хеш-функції електронного документу для блоку даних, згідно схеми показаної на рисунку 3.4. Але на рисунку 3.4 представлено операцію обчислення значення хеш-функції лише в горизонтальних блоках даних. Якщо за запропонованою схемою обчислити значення хеш-функції також і в вертикальних блоках даних це дасть змогу, при перевірці значень хеш-функції за формулою (2.4) виявити порушення цілісності в горизонтальному та вертикальному блоці, як показано на рисунку 3.5 [30].

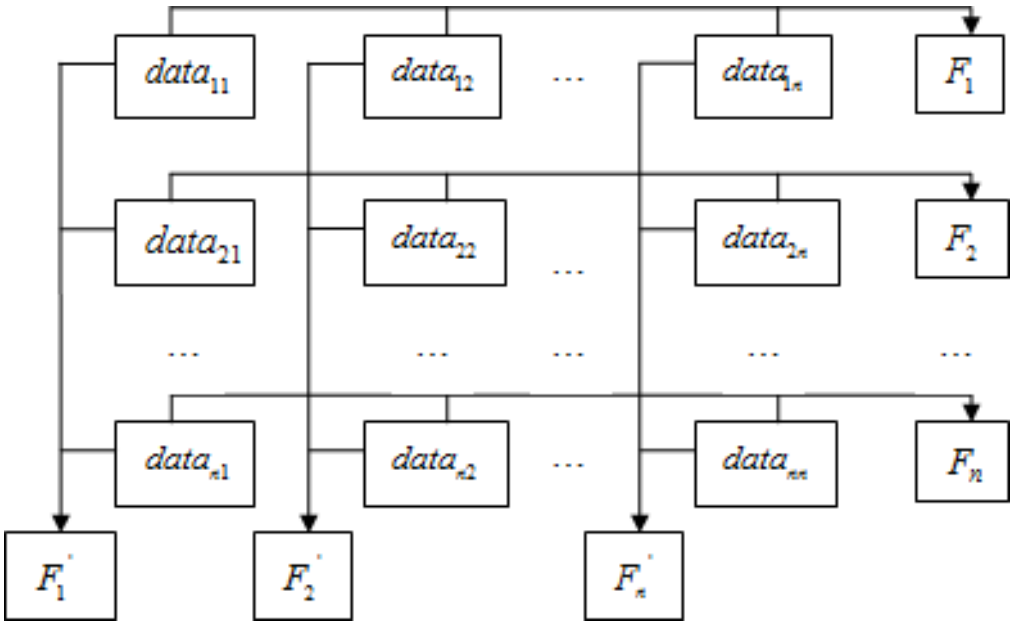


Рисунок 3.5 – Схема обчислення хеш-функції в горизонтальних/вертикальних блоках даних

Очевидно, якщо проводити обчислення хеш-функції у вертикальних або горизонтальних блоках, це призведе до того, що стає неможливим виявити факт модифікації документа в довільному блоці. Але якщо ми знаємо, рядок та стовпець, де відбулися модифііікація, тоді їх перетин можна

бажати, як фальсифікований фрагмент електронного документу. Запропонований метод отримав назву перехресного хешування.

Розглянемо детальніше процес виявлення фальсифікацій в електронному документі запропонованим методом. Для цього спочатку електронний документ потрібно розбити на інформаційні блоки, як показано на рисунку 3.6.

A_{11}	A_{12}	A_{13}	A_{14}	....	A_{1n}
A_{21}	A_{22}	A_{23}	A_{24}	....	A_{2n}
A_{31}	A_{32}	A_{33}	A_{34}	...	A_{3n}
A_{41}	A_{42}	A_{43}	A_{44}	...	A_{4n}
...	...	...	...	...	...
A_{n1}	A_{n2}	A_{n3}	A_{n4}	...	A_{nn}

Рисунок 3.6 – Поділ електронного документу на фрагменти інформації

Табличне представлення процесу отримання міні хеш-функцій електронного документу можна показати наступним чином, дивись рисунок 3.7.

Рисунок 3.7 – Табличне представлення процесу отримання міні хеш-функцій

A_{11}	A_{12}	A_{13}	A_{14}	...	A_{1n}	Обчислення міні хеш-функцій $F(A_{in})$	F_{11}
A_{21}	A_{22}	A_{23}	A_{24}	...	A_{2n}		F_{12}
A_{31}	A_{32}	A_{33}	A_{34}	...	A_{3n}		F_{13}
A_{41}	A_{42}	A_{43}	A_{44}	...	A_{4n}		F_{14}
...	...	...	...	...	...		...
A_{n1}	A_{n2}	A_{n3}	A_{n4}	...	A_{nn}		F_{1n}
Обчислення міні хеш-функцій $F(A_{nj})$							
F_{21}	F_{22}	F_{23}	F_{24}	...	F_{2n}		

Далі необхідно перевірити достовірність значень хеш-функції кожного блоку, який відповідає предікату

На рисунку 3.8 представлено блок-схема алгоритму виявлення фальсифікованого фрагменту електронного документу методом перехресного хешування.

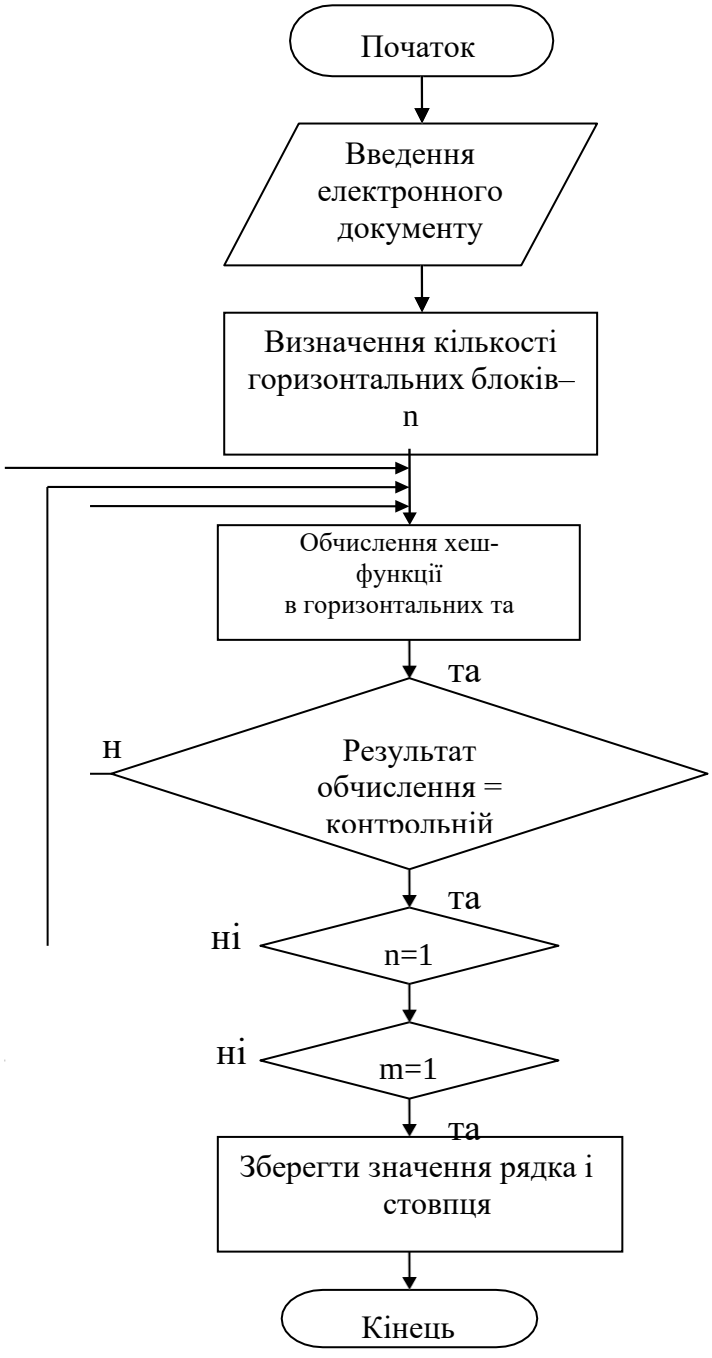


Рисунок 3.8 – Алгоритм виявлення фальсифікованого фрагменту електронногодокументу методом перехресного хешування

призведе до коригування міні хеш-функції. Спираючись на аналіз зміни своєго значення міні-хеш функціями можна зробити висновок об інформаційному блоці ЕД, де і відбулося порушення документу. Відповідно, горизонтальна міні хеш-функція забезпечить знання рядка, тоді як вертикальна буде вказувати на стовпець. Місце перетину буде визнавати блок зі зміненою інформації, дивись рисунок 3.9.

A_{11}	A_{12}	A_{13}	A_{14}	...	A_{1n}	F_{11}
A_{21}	A_{22}	A_{23}	A_{24}	...	A_{2n}	F_{12}
A_{31}	A_{32}	A_{33}	A_{34}	...	A_{3n}	F_{13}
A_{41}	A_{42}	A_{43}	A_{44}	...	A_{4n}	F_{14}
...	...	...	...	...	...	...
A_{n1}	A_{n2}	A_{n3}	A_{n4}	...	A_{nn}	F_{1n}
F_{21}	F_{22}	F_{23}	F_{24}	...	F_{2n}	

Рисунок 3.9 – Табличне представлення процесу виявлення фальсифікованого фрагменту інформації

З рисунку 3.9 видно, що при перевірці міні хеш-функції, F_{24} і F_{13} змінили своє значення, це означає, що в інформаційному блоці A_{34} відбулися зміни, тобто даний фрагмент електронного документу був фальсифікований

3.3 Метод виявлення заданої кількості фальсифікованих фрагментів електронного документу на основі надлишкового хешування контрольного блоку інформації

Достовірність передачі, обробки та зберігання електронних документів в наш час є вкрай важливим завданням. Ефективним способом вирішення даної проблеми є використання надлишкового хешування інформації. Введення надлишкової інформації в інформацію, яка передається мережею забезпечує можливість виявлення і виправлення помилок на стороні отримувача інформаційного повідомлення. Математична теорія побудови надлишкових (завадостійких) кодів зараз має великі досягнення. Проте, існує великий розрив між рівнем теоретичних досягнень теорії завадостійкого кодування і рівнем результатів практичного використання даної теорії [13–18].

Введення надлишковості дає можливість виявлення і виправлення помилок в інформації, яка передається і може бути змінена під час передачі. Однак, до цього відомі корегуючі, циклічні коди, коди Хеммінга, Ріда-Соломона, описані в дослідженнях [37-39], не придатні для вирішення проблеми виявлення фальсифікованих фрагментів інформації. Розрізняють коди, які виявляють помилки, і корегуючі коди, які ще додатково, крім виявлення помилки, виправляють її.

Оскільки в документах зазвичай можуть фальсифікуватися цілі фрагменти інформації, тому, перелічіни методики не завжди мають можливість виришити задачу фальсифікації ЕД.

Історія виникнення і розвитку теорії та практики завадостійкого кодування з метою виправлення помилок і тим самим забезпечення достовірності переданих даних починається робіт американського вченого Шеннона [3]. Проте, Шеннон не вказав, як побудувати завадостійкі коди, а лише довів їх існування. Вже незабаром Хеммінгом була розроблена теорія лінійних блокових кодів. Хеммінг ввів і дав визначення основним

параметрам блокових кодів, а також розробив кодуючий і декодуючий пристрої для своїх кодів. Для оцінки корегуючої можливості кодів Хеммінг ввів параметри кодова d і мінімальна кодова d_0 відстані і показав їх залежність від довжини коду і введеної надлишковості [5].

Мінімальна кодова відстань по Хеммінгу – відповідає (дорівнює) кількості позицій, якими відрізняються дві порівнювані між собою кодові послідовності. Порівнюються кодові послідовності побітно шляхом сумування за модулем два.

Хеммінг довів, що мінімальна кодова відстань характеризує корегуючі властивості завадостійкого коду. В роботах Хеммінгу встановлено, що у тому випадку коли різниця між двомя кодовимі послідовностями представлена в t $(t \geq 1)$ позиціях, а всі інши кодови послідовності цієї кодової множини відрізняються більш ніж в t позиціях, то виправлення t помилок можливо, якщо було забезпечено мінімальна кодовау відстань $d_0 \geq 2 * t + 1$.

Оскільки розглядається проблема підробки ЕД, при розробці методу виявлення підроблених часток ЕД можна взяти за основу принципи алгоритму кодування за Хеммінгом. Традиційно алгоритми кодування-декодування за Хеммінгом виявляють символьні помилки в кодових послідовностях. На відміну від традиційного алгоритму кодування за Хеммінгом, який працює з бітами, доречною є побудова алгоритму, який оперує блоками інформації, тобто фрагментами електронного документу.

Зупинимося детальніше на тому, що будь-який (Gn,k) код Хеммінга в загальному вигляді може бути представлено такий матрицею (3.1).

$$G_{(n,k)} = \begin{bmatrix} 1\,0 \cdots 0 & \cdots & b_{11}, b_{12} \cdots b_{1n} \\ \vdots & \ddots & \vdots \\ 000 \cdots 1 & \cdots & b_{k1}, b_{k2} \cdots b_{kn} \end{bmatrix} \qquad (3.1)$$

Для визначення значень перевірочних елементів правої частини

матриці необхідно виходити з основних властивостей систематичних кодів.

З огляду на те що кожен рядок одиничної матриці k×k має лише одну одиницю, то вага кожного рядка цієї матриці не повинна бути меншою за d°–°1, а таким чином за модулю два будь-яких двох рядків не повинна бути меншою за d –2, для виправлення однократної помилки. Крім того комбінації правої частини матриці повинні бути лінійно незалежними.

Аналогічно принципам кодування за Хеммінгом, введемо надлишковість, але замість символів–додамо блоки інформації. Для цього введемо позначення, нехай $\vec{A} = (\vec{a}_1,\ \vec{a}_2, \vec{a}_3, \dots \vec{a}_n)$ –електронний документ, де $\vec{a}_1,\ \vec{a}_2, \vec{a}_3, \dots \vec{a}_n$ відповідно множина двійкових векторів, блоків інформації довільного розміру. Через множину $\vec{F} = (\vec{f}_1,\ \vec{f}_2, \vec{f}_3, \dots \vec{f}_n)$ позначимо значення хеш-функцій фіксованого розміру, обчислені за $f_i = a(h_i)$, де. Обчислити значення хеш-функцій кожного з інформаційних блоків можна за допомогою одного з алгоритмів,запропонованих в статті [12].

Аналогічно принципам кодування за Хеммінгом, введемо надлишковість, але замість символів – додамо блоки інформації.

Множину можливих схем хешування блоків $a_1, a_2, a_3, \dots, a_n$ представити у вигляді двійкової матриці (3.2), де кожний рядок відповідає визначеній схемі хешування.

$$F = \begin{pmatrix} f_{11}, f_{12}, & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{m1}, f_{m2} & \cdots & f_{mn} \end{pmatrix}, \qquad (3.2)$$

де кожний рядок відповідає визначеній схемі хешування.

При цьому виконуються наступні умови для рядків матриці:

1) відсутні нульові рядки матриці;
2) всі рядки матриці є лінійно-незалежними;
3) існує мінімальна кодові відстань між рядками матриці.

В теорії кодування для породжуючої матриці також є характерними перелічені властивості, що дає змогу використовувати правила побудови лінійнихкодів для побудови систем хеш-кодів.

Система хеш-кодів – множина хеш-кодів, які отримані шляхом реалізації будь-якого алгоритму обчислення хеш-функції в порядку, визначеному спеціальною процедурою вибору записів (блоків інформації), на основі математичного апарату лінійної алгебри.

Алгоритм побудови хеш-кодів для забезпечення цілісності ЕД.

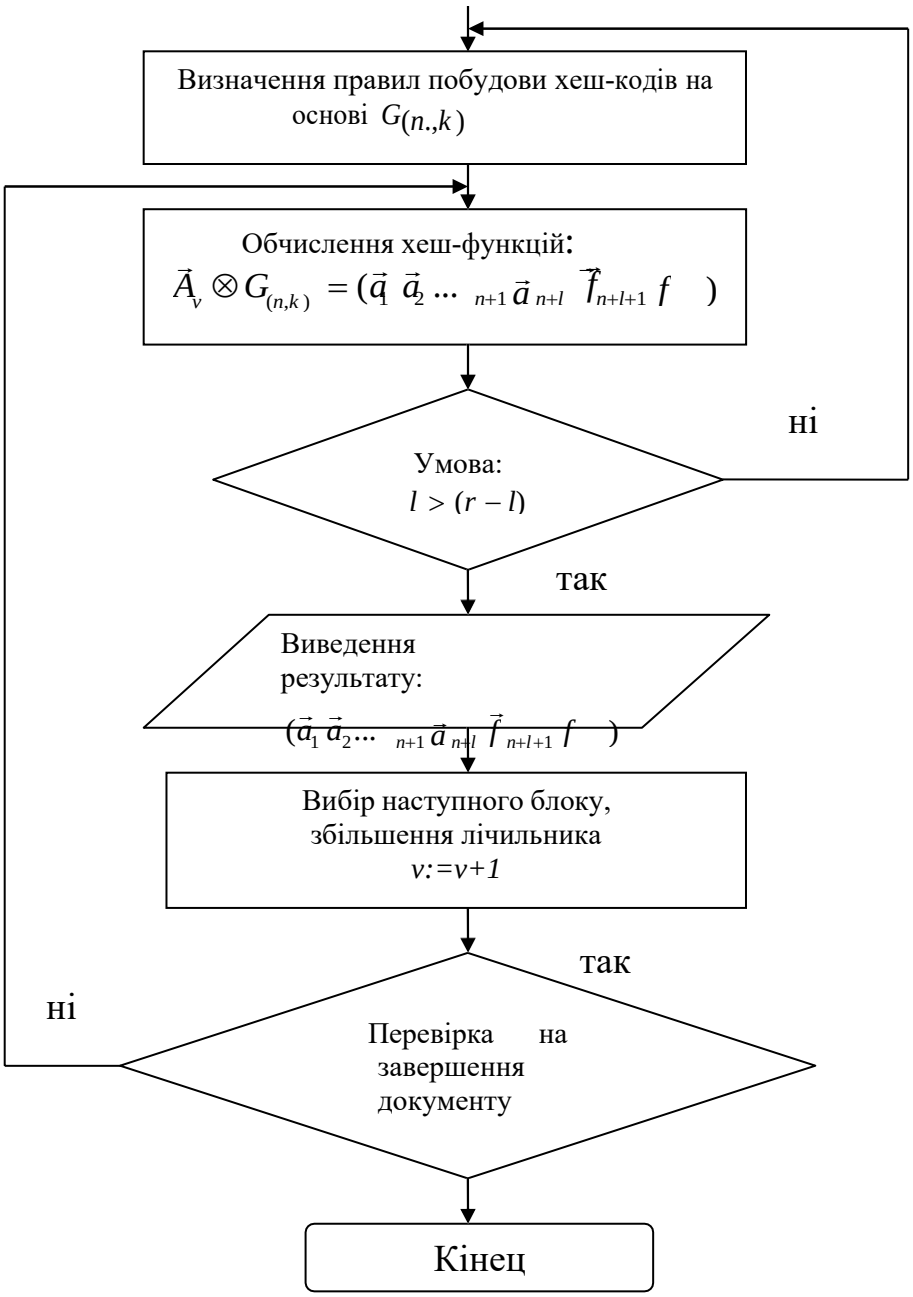
Хешування вихідного блоку інформації можна представити у вигляді виразу (3.3), який є спеціальною багатовимірною не комутативною операцією хешування.

$$(\overrightarrow{a_1}\ \overrightarrow{a_2}\ \dots \overrightarrow{a_{n+1}} \dots \overrightarrow{a_{n+l}}) \rightarrow (\overrightarrow{a_1}\ \overrightarrow{a_2}\ \dots \overrightarrow{a_{n+1}}.\overrightarrow{a_{n+l}}\ \overrightarrow{f_{n+l+1}}\ \overrightarrow{f_{n+l+r}}) \qquad (3.3)$$

Тоді, отриманий, в результаті хешування, захищений блок виглядатиме, як спеціальна багатовимірна не комутативна операція хешування інформаційних блоків електронного документу. Схематично суть алгоритму обчислення хеш-функцій для забезпечення цілісності ЕД можна показати наступним чином (рисунок 3.10)

Для контролю цілісності інформації в теорії лінійних кодів використовується поняття синдром. Синдром в теорії кодування означає сукупність ознак, характерних для певного явища. Синдром вектора, який може мати помилки дає можливість розпізнати найбільш ймовірний характер цих помилок.

Для пошуку всіх можливих варіантів кодів (матриць), з мінімальною кодовою відстанню $d_0 \geq 3$ між послідовностями рядків матриці, було розроблено програмне забезпечення, результати роботи якого показані в таблиці 3.1.



-

Рисунок 3.10 – Алгоритм обчислення хеш-функцій для забезпечення цілісності ЕД

Таблиця 3.1– Варіанти породжуючих матриць

№	Матриця	№	Матриця	№	Матриця	№	Матриця

1	0 0 0 0 1 0 0 1 1 0 1 0 0 0 1 1 1 1 1 0	2	0 0 0 0 1 0 0 1 0 1 1 1 0 1 0 1 1 1 0 1	3	0 0 0 0 1 0 1 1 1 1 1 1 0 1 1 1 1 1 0 0	4	0 1 1 1 1 0 0 1 0 1 1 1 0 1 0 1 1 1 0 1
5	0 0 0 1 0 0 0 1 1 1 1 1 0 1 0 1 1 1 0 1	6	0 0 1 1 1 0 0 1 0 1 1 1 0 0 1 1 1 1 1 0	7	0 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 1 1	8	0 0 0 1 1 0 1 1 1 0 1 1 0 1 0 1 1 1 0 1
9	0 0 0 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 0 0	10	0 0 0 1 1 0 0 1 1 0 1 1 0 1 1 1 1 1 1 1	11	0 0 0 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 0 0	12	0 0 0 1 0 0 0 1 1 1 1 1 0 1 1 1 1 1 1 0
13	0 0 0 1 1 0 1 1 0 1 1 1 0 0 0 1 1 1 1 1	14	1 0 0 1 0 0 0 0 1 1 1 1 0 0 1 1 1 1 1 0	15	0 1 0 1 0 0 0 1 1 1 1 1 0 1 1 1 1 1 0 0	16	0 0 1 1 0 0 1 1 0 1 1 1 0 0 0 1 1 1 1 1
17	0 0 0 1 1 0 1 1 1 0 1 1 1 1 1 1 0 1 1 0	18	0 0 1 0 1 0 1 1 1 0 1 1 0 1 1 1 1 0 0 1	19	0 1 0 0 1 0 0 1 1 1 1 1 0 1 0 0 1 1 1 1	20	0 1 0 1 1 0 0 1 1 0 1 1 0 1 1 1 0 1 0 0

Продовження таблиці 3.1

21	0 0 1 1 1 1 0 1 0 1 1 1 1 1 0 1 1 1 0 1	22	1 0 0 1 1 0 1 1 0 0 1 1 0 1 0 1 1 1 1 1	23	0 0 1 0 0 0 1 1 1 1 1 1 0 1 0 1 1 1 0 0	24	0 1 1 1 1 0 0 0 0 1 1 1 0 1 0 1 1 1 0 0
25	1 0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 1 1 1	26	0 1 1 0 0 0 0 1 0 1 1 1 0 1 1 0 1 1 1 0	27	0 0 1 1 0 1 1 0 0 0 1 1 0 1 1 0 1 1 0 1	28	0 0 0 1 1 1 0 0 1 0 1 1 0 1 0 1 1 0 1 1
29	1 0 1 0 1 1 0 0 1 0 1 1 0 1 1 1 1 0 1 1	30	0 1 1 0 1 0 1 0 1 0 1 1 0 0 1 1 1 1 0 1	31	0 0 1 1 1 0 0 0 1 1 1 1 1 0 0 1 1 1 1 0	32	0 0 1 0 0 1 0 0 0 0 1 1 0 1 1 1 1 1 1 1
33	0 0 1 0 0 1 0 0 0 1 1 1 0 1 1 1 1 1 1 0	34	0 0 0 1 1 0 0 0 0 1 1 1 0 1 0 1 1 1 0	35	0 0 0 1 1 0 0 0 1 0 1 1 0 1 1 1 1 0 0 1		

Відповідно до представлених в таблиці 3.1 варіантів породжуючих матриць, будуть виконуватися матричні перетворення задані формулами, які показані в додатку А.

Розглянемо декілька прикладів виявлення фальсифікованих фрагментів інформації на основі запропонованого методу

Як показують обчислення, між всіма кодовими послідовностями (рядками матриці) зберігається мінімальна кодова відстань $d\ 0 \square 5$, це дає можливість стверджувати, що даний код сприятиме гарантованому виправленню двохкратної помилки в блоках інформації.

Схематично принцип отримання хеш-функцій можна показати наступним чином, рисунок 3. 11

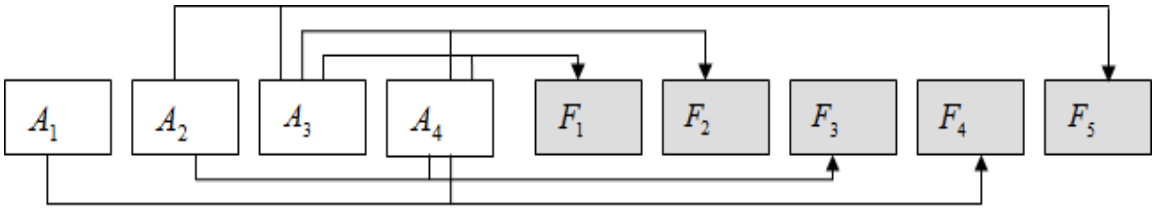


Рисунок 3.11 – Схема отримання хеш-функцій

Таблиця 3.2 – Виправлення помилок в блоках електронного документу (*– фальсифікований блок інформації)

Локалізація помилки										
	Двохкратна 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

В таблиці 3.2 показано значення синдрому при різних комбінаціях помилок. Перевіримо правильність методу на прикладі, нехай маємо інформаційні блоки «0101», обчислимо контрольні блоки.

Всі комбінації помилок в інформаційних блоках показані в таблиці 3.3.

Таблиця 3.3 –Виправлення помилок в блоках електронного документу (*– фальсифікований блок інформації)

0101 11011 ⊕ * * 1001 11100 1100 00111	0101 11011 ⊕ * * 1111 00000 1010 11011	0101 11011 ⊕ * * 1100 00111 100111100	0101 11011 ⊕ * * 0011 00111 0110 11100	0101 11011 ⊕ * * 0000 00000 0101 11011
0101 11011 ⊕ * * 0110 11100 0011 00111	0101 11011 ⊕ * 1101 11001 1000 00010	0101 11011 ⊕ * 0001 11110 0100 00101	0101 11011 ⊕ * 0111 00010 0010 11001	0101 11011 ⊕ * 0100 00101 0001 11110

Схематично принцип отримання хеш-функцій можна показати наступним чином, рисунок 3.12.

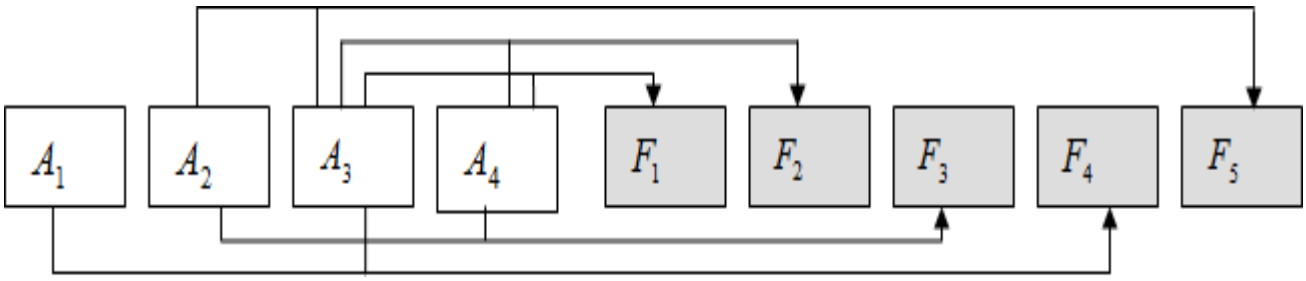


Рисунок 3.12 – Схема отримання хеш-функцій

Розглянемо результати виявлення і виправлення помилок приведеними кодами Хеммінга в залежності від кратності помилки. Дані результати наведені в таблиці 3.4

Таблиця 3.4 – Виправлення помилок в блоках електронного документу(*– фальсифікований блок інформації)

Локалізація помилки										
	Двохкратна 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	0	1	1	0	1	1	0	1	0
$f_5(x_2 + x_3)$	1	1	0	0	1	1	0	1	1	0

Розглянемо результати виявлення і виправлення помилок приведеними кодами Хеммінга в залежності від кратності помилки. Дані результати наведені в таблиці 3.5.

Таблиця 3.5 – Виправлення помилок в блоках електронного документу (*– фальсифікований блок інформації)

Локалізація помилки										
	Двохкратна 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	1	0	0	1	1	1	0	0	1
$f_4(x_1 + x_4)$	1	0	1	1	0	1	1	0	1	0
$f_5(x_2 + x_3)$	1	0	1	1	0	1	0	1	0	1

Були побудовані моделі розроблених методів виявлення підробок ЕД , які базуються на обчисленні значення хеш-функції. Ці моделі могут бути були реалізовані як програмному так і апаратному рівнях.

При розробці апаратних засобів реалізації методів контролю цілісності та виявлення фальсифікацій в електронних документах можливо використовувати функціональні схеми розробленних у роботі методів:

1) схема впровадження методу обчислення хеш-функції, що базується на використанні послідовного виконання операцій, без використання ключа;

2) схема впровадження методу обчислення хеш-функції, що базується на використанні паралельного виконання операцій, без використання ключа;

3) схема впровадження модіфікованого методу обчислення хеш-функції електронного документу, що базується на послідовної реалізації обчислень;

4) схема впровадження методу обчислення хеш-функції електронного документу, що базується на використання операцій матричного криптографічного перетворення;

5) схема впровадження методу обчислення хеш-функції електронного документу, що базується на паралельної реалізації обчисленьпри використанні операцій матричного криптографічного перетворення;

Функціональні схеми методів виявлення фальсифікованих фрагментів електронного документу:

1) функціональна схема реалізації методу виявлення фальсифікованого фрагменту електронного документу шляхом перехресного хешування;

2) функціональна схема реалізації методу виявлення заданої кількості фальсифікованих фрагментів електронного документу на основі надлишкового хешування контрольного блоку інформації.

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 .

Зовнішній вигляд інструментального модуля Xilinx Spartan-3E Srarter Kit показаний на рисунку 3.13. Всі компоненти модуля змонтовані на друкованій платіз двостороннім розміщенням компонентів.

До комплекту проектування дискретних пристроїв Xilinx Spartan-3E Srarter Kit (рисунок 3.13 входять: плата відладки на базі ПЛІС; універсальне джерело живлення на 100-240В, 50/60Гц; мережевий адаптер; програмне забезпечення зі скороченим терміном ліцензії: CD-диски зі САПР ISE и EDK Xilinx; USB-кабель.

Основні характеристики комплекту: мікросхеми Xilinx: XC3S500E-4FG320C Spartan-3E, XC2C64A-5VQ44C CoolRunner-II и ППЗУ Platform Flash XCF04S-VO20C; синхронізація: 50МГц кварцевий генератор синхроімпульсів; пам'ять SPI, 64Мб DDR SDRAM; конектори і інтерфейси: порт Ethernet 10/100 Phy, JTAG USB-порт, два послідовних порти RS-232 на 9 контактів, порттипу PS/2; дисплей РКІ з двома рядками по 16 символів.

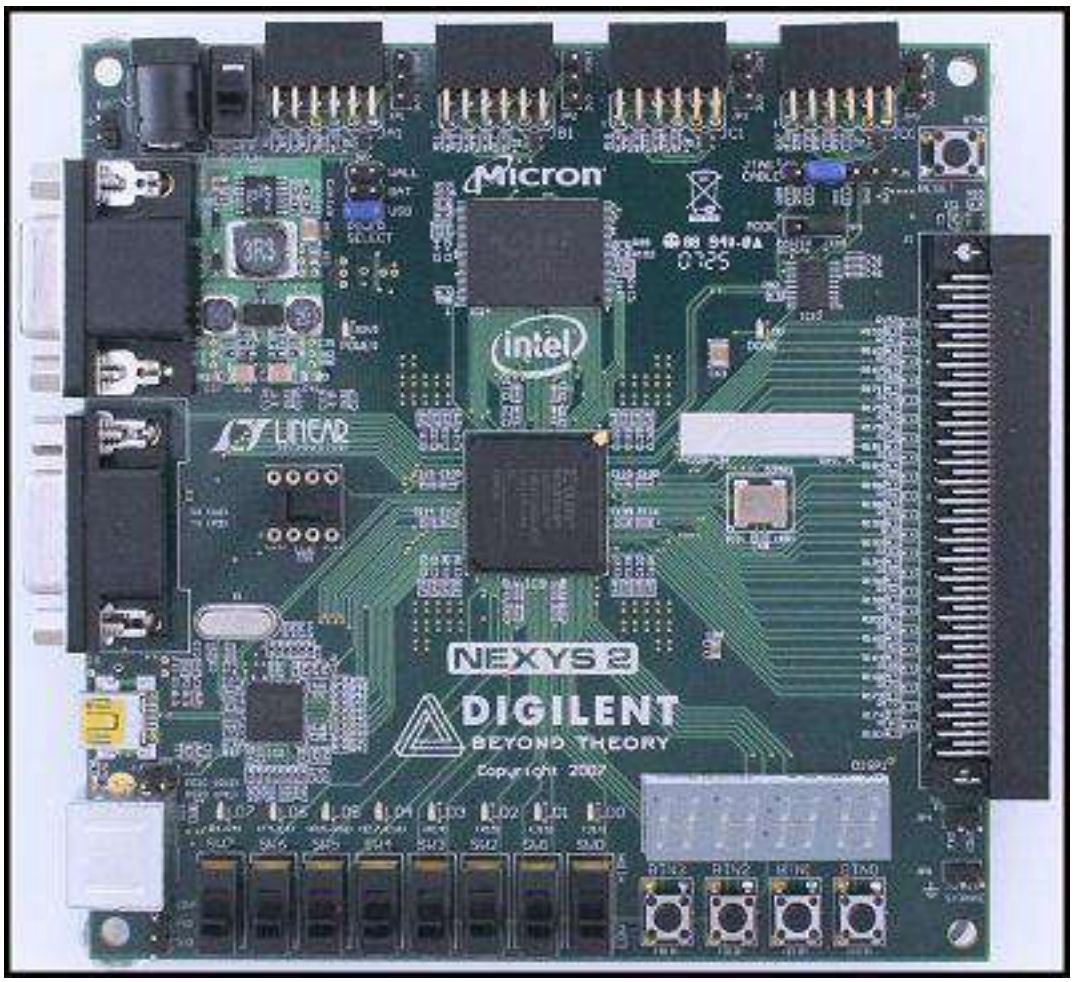


Рисунок 3.13 – Зовнішній вигляд інструментального модуля Xilinx Spartan-3E Srarter Kit

У розділі наведані результати досліджень щодо 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.

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 помилкив 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.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. 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.

2. Hu Fei. Opportunities in 5G Networks: A Research and Development Perspective / F. Hu. – CRC Press, 2016. – 561 p.

3. Lavrovska T. Physical model of pseudorandom codes in multidimensional Euclidean space [Электронный ресурс] / T. Lavrovska, S. Rassomahin // Problems of Infocommunications Science and Technology (PIC S&T 2016): materials of III International Science-Practical Conference, 4–6 October 2016 / Kharkiv National University of Radio Electronics. – Text (250 Mb). – Kharkiv, 2016. – Electron-optical disk (CD-ROM).

4. Lavrovska T. The method of pseudorandom codes decoding on the basis of the modified method of branches and boundaries/ T. Lavrovska // Computer Science and Cybersecurity. – 2017, № 5. – P. 4 – 16.

5. Mignone V. OFDM: A Novel Demodulation Scheme for Fixed and Mobile Receivers / V. Mignone, A. Morello // IEEE Transactions on Communications. – 1996, №44. – P. 1144 – 1150.

6. Nikolic J. Lloyd–Max's Algorithm Implementation in Speech Coding Algorithm Based on Forward Adaptive Technique / J. Nikolic, Z. Peric // Informatica. – 2008. – Vol. 19, №. 2. – P. 255 – 270.

7. Sesia S. LTE – The UMTS Long Term Evolution: From Theory to Practice / S. Sesia, I. Toufik, M. Baker. – 2nd edition. – Wiley, 2011. – 792 p.

8. Shannon C. E. A Mathematical Theory of Communication / C. E. Shannon. – Bell Syst. Tech. J., 1948. – Vol. 27. – P. 379–423, 623–656.

9. Shulman N. Random Coding Techniques for Nonrandom Codes / N. Shulman // IEEE Trans. Inf. Theory. – 1999. – Vol. 45, № 6. – P. 2101 – 2104.

10. Shulze H. Theory and Applications of OFDM and CDMA / H. Shulze, C. Luders. – Germany: John Wiley & Sons, Ltd , 2005.− 408 p.

11. Ungerboeck G. Channel coding with multilevel/phase signal / G. Ungerboeck // IEEE Trans., 1981. – Vol. IT-28, № 1. – P. 55 – 66.

12. Verd´u S. Fifty Years of Shannon Theory / S. Verd´u // IEEE Transactions on information theory. – 1998. – Vol. 44, №6. – P. 2057 – 2078.

13. Xiang W. 5G Mobile Communications / Xiang W., Zheng K., Xuemin Sh.; Springer International Publishing, 2016. – 690 p.

14. Report: Cenzic Application Vulnerability Trends Report: 2014 [Електронний ресурс] // Cenzic. – 2014. – Режим доступу до ресурсу: https://info.cenzic.com/2013- Application-Security-Trends-Report.html.

15. OWASP Secure Coding Practices Quick Reference Guide. // OWASP. – 2010. 4 OWASP Top 10 – 2017 The Ten Most Critical Web Application Security Risks, 2017.

16. The Bobby Tables Guide to SQL Injection. Archived from the original on November 7, 2017. Retrieved October 30, 2017

17. Martin Anderson. Cross-site scripting enabled on 1000 major sites – including financial sites. The Stack. 24 лютого 2016., 205с.

18. CERT Vulnerability Notes Database. Software Engineering Institute. Original Release Date: 2008. – 21с.;

19. NIST Comments on Cryptanalytic Attacks on SHA-1 – NIST Information Technology Laboratory / 2006.

20. MySQL / Режим доступа до ресурсу: https://uk.wikipedia.org/wiki/MySQL.

21. Encyclopedia of Cryptography and Security / Ed. By Henk C. A. Van Tilborg and Sushil Jajodia. — Springer, 2011. — P. 307—312.

22. Kosenko, V. (2017), “Principles and structure of the methodology of risk-adaptive management of parameters of information and telecommunication networks of critical application systems”, *Innovative technologies and scientific solutions for industries*, No 1 (1), P. 75-81. Doi:https://doi.org/10.30837/2522-

9818.2017.1.046

23. Kosenko, V. (2017), «Mathematical model of optimal distribution of applied problems of safety-critical systems over the nodes of the information and telecommunication network», *Advanced Information Systems*, Vol. 1, No. 2, P. 4–9.DOI: https://doi.org/10.20998/2522-9052.2017.2.01.

24. Karen Bailey, Kevin Curran. Steganography. – BookSurge Publishing, 2005 г. – 118 с.

25. Johnson N., Duric Z., Jajodia S. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures, New York. – NY.: Kluwer Academic Pub, 2000 p.

26. Elad Barkan. Instant Ciphertext-Only Cryptanalysis of GSM. Encrypted Communication. / Elad Barkan, Eli Biham, Nathan Keller.// Journal of Cryptology, Volume 21, Number 3, July 2008 , pp. 392-429(38)

27. J. Golic. Cryptanalysis of Alleged A5 Stream Cipher. – Proceedings of EUROCRYPT'97, LNCS 1233, pp. 239 – 255, Springer-Verlag 1997.

28. Alex Biryukov. Real Time Cryptanalysis of A5/1 on a PC. / Alex Biryukov, Adi Shamir, David Wagner.– Springer Berlin / Heidelberg, 2001. ¬ ISBN: 978-3-540-41728-6

29. Mozhaiev O. Development of a method for determining the general criteria of abnormal behavior of a computer system based on the improved criterion of uniformity of input data samples../ Mozhaiev O., Semenov, S., Kuchuk, N., Mozhaiev, M., Tiulieniev, S., Gnusov, Y., Yevstrat, D., Chyrva, Y., Kuchuk, H.// Eastern-European Journal of Enterprise Technologies, 6 (4 (120)), PP40-49. Doi: https://doi.org/10.15587/1729-4061.2022.269128

30. Mozhaiev O. Crypto-resistant methods and random number generators in internet of things (iot) devices/ Mozhaiev O., Klimushyn P., Solianyk T., Gnusov Y., Manzhai O., Svitlychnyi V.// *Innovative technologies and scientific solutions for industries*, 2022 № 2 (20), P. 22—34 https://doi.org/10.30837/ITSSI.2022.20.022

31. Mozhaiev O. Potential application of hardware protected symmetric

authentication microcircuits to ensure the security of internet of things/ Mozhaiev O, Klimushyn P., Solianyk T., Kolisnyk T. // *Advanced Information Systems*, 2021. Vol. 5, No3 P. 103-111 DOI:https://doi.org/10.20998/2522-9052.2021.3.14

32. Klimushyn, P., (2021), «Hardware support procedures for asymmetric authentication of the internet of things»,/ Klimushyn, P., Solianyk, T., Mozhaev, O., Nosov, V., Kolisnyk, T., Yanov V// Innovative Technologies and Scientific Solutions for Industries, No. 4 (18), P. 31–39. DOI: 10.30837/ITSSI.2021.18.031

33. J. Friedrich, G. Miroslav, R. Du. Reliable Detection of LSB Steganography in Color and Grayscale Images. Binghampton, New York: SUNY, 2001.

34. J. Fridrich, R. Du, and L. Meng, "Steganalysis of LSB Encoding in Color Images", ICME 2000, New York City.

35. W. Brock. W. Dechert and J. Scheinkman. «A test for independence based on the correlation dimension», Working Paper, University of Wisconsin, 1987.

36. Wu H.C., Wu N.I., Tsai C.S., Hwang M.S. Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods // IEEE Transactions on Image and Signal Processing, 2005. – № 5. – P. 611-615.

37. Svyrydov, A., Kuchuk, H., Tsiapa, O. (2018). Improving efficienty of image recognition process: Approach and case study. Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018, 593-597, doi: https://doi.org/10.1109/DESSERT.2018.8409201·

38. O. Mozhaev Potential application of hardware protected symmetric authentication microcircuits to ensure the security of internet of things/P. Klimushin, T.Solianyk, T. Kolisnyk, O. Mozhaev// Advanced Information Systems. 2021. Vol. 5, No. 3, P 103-111, doi: https://doi.org/10.20998/2522-9052.2021.3.14

39. Mozhaiev M. Sustainability of Open Educational Resources in Forensic Sciences: International Experience/ Karina Palkova, Olena Agapova, Aelita Zīle, Anton Polianskyi, Khosha Vadym, Serafyma Hasparian, Mozhaiev

Mykhailo// European Journal of Sustainable Development(2022), 11, 3, 71-80 ISSN: 2239-5938 Doi:10.14207/ejsd.2022.v11n3p71

40. Закон України «Про електронні документи та електронний документообіг»/ Відомості Верховної Ради України (ВВР), 2003, № 36, ст.275

41. Mozhaiev, M., (2022). Devising a procedure for defining the general criteria of abnormal behavior of a computer system based on the improved criterion of uniformity of input data samples./ Semenov, S., Mozhaiev, O., Kuchuk, N., Mozhaiev, M., Tiulieniev, S., Gnusov, Y., Yevstrat, D., Chyrva, Y., Kuchuk, H. EasternEuropean Journal of Enterprise Technologies, 6 (4 (120)), 40–49. Doi: https://doi.org/10.15587/17294061.2022..

42. Гнусов Ю.В., Клімушин П.С., Колісник Т.П., Можаєв М.О. Аналіз систем моделювання мікроконтролерів з додатковими модулями криптографічного захисту інформації. Вісник Національного технічного університету «ХПІ». Серія: Системний аналіз, управління та інформаційні технології №1(3) 2020 С. 79-84

43. Mykhailo Mozhaiev, Viacheslav Davydov, Zhang Liqiang Analysis and comparative researches of methods or improving the software Advanced Information Systems, 2020 Vol. 4, No. 3, pp. 8-11, DOI: https://doi.org/doi: 10.20998/2522-9052.2020.3.18

44. Коваленко А. А., Кучук Г. А. Методи синтезу інформаційної та технічної структур системи управління об’єктом критичного застосування. Сучасні інформаційні системи. 2018. Т. 2, № 1. С. 22–27. DOI: https://doi.org/10.20998/2522-9052.2018.1.04

45. Вимоги до оформлювання документів/ Національний стандарт України ДСТУ 4163-2003// наказ Держспоживстандарту України від 7 квітня 2003 р. №55

46. Kuchuk G., Kharchenko V., Kovalenko A., Ruchkov E. Approaches to selection of combinatorial algorithm for optimization in network traffic control of safety-critical systems. *East-West Design & Test Symposium (EWDTS)*. 2016. Pp. 1-6. Doi:https://doi.org/10.1109/EWDTS.2016.7807655.

47. Kuchuk G.A. An Approach To Development Of Complex Metric For Multiservice Network Security Assessment / G.A. Kuchuk, A.A. Kovalenko, A.A. Mozhaev // Statistical Methods Of Signal and Data Processing (SMSDP – 2010): Proc. Int. Conf., October 13-14, 2010.– Kiev: NAU, RED, IEEE Ukraine section joint SP, 2010. – P. 158 – 160.

48. Mozhaiev M Method of Forensic Research on Image for Finding Touch up on the Basis of Noise Entropy/O. Kliuiev ; M. Mozhaiev ; M. Mozhaiev , O.Uhrovetskyi ,E. Simakova-Yefremian 3rd International Conference on Advanced Information and Communications Technologies (AICT) Publisher: IEEE, 2019 Lviv, Ukraine P. 76 – 79. DOI: 10.1109/AIACT.2019.8847760 (Scopus)

49. Mozhaiev M., (2017). Multiservice network security metric/ Mozhaev, O., Kuchuk, H., Kuchuk, N., Mozhaiev M., Lohvynenko, M..// 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017 – Proceedings, 133-136. Doi: https://doi.org/10.1109/AIACT.2017.8020083.

50. OWASP Secure Coding Practices Quick Reference Guide. // OWASP. – 2010. 4 OWASP Top 10 – 2017 The Ten Most Critical Web Application Security Risks, 2017.

51. The Bobby Tables Guide to SQL Injection. Archived from the original on November 7, 2017. Retrieved October 30, 2017

- Martin Anderson. Cross-site scripting enabled on 1000 major sites – including financial sites. The Stack. 24 лютого 2016., 205с.

52. CERT Vulnerability Notes Dat abase. Software Engineering Institute. Original Release Date: 2008. – 21с.

53. NIST Comments on Cryptanalytic Attacks on SHA-1 – NIST Information Technology Laboratory / 2006.