МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В. Н. Каразіна

Факультет: **ННІ Каразінський банківський інститут**
Кафедра: **Інформаційних технологій та математичного моделювання**
Спеціальність: **122 Комп'ютерні науки**
Освітня програма: **Комп'ютерні науки**

Група: АК-21М **денна форма навчання**

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

«ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СИСТЕМИ ЗАХИЩЕНОГО ЗБЕРІГАННЯ Й ПЕРЕДАВАННЯ ІНФОРМАЦІЇ»

ЗА НАКАЗОМ № 4601-5/3262 ВІД 15 ВЕРЕСНЯ 2025 РОКУ

здобувача вищої освіти **Кравченко Владислава Віталійовича**

Робота допущена до захисту в ЕК
протокол кафедри ІТММ № 5 від 02.12.2025 р.

В.о. завідувача кафедри ІТММ
PhD
_____**Ковальчук Д. М.**

Науковий керівник
к.ф.-м.н., доцент
_____**Філатова Л. Д.**

м. Харків 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В. Н. Каразіна

Факультет навчально-науковий інститут “Каразінський банківський інститут”
Кафедра інформаційних технологій та математичного моделювання
Рівень вищої освіти другий (магістерський)
Спеціальність 122 Комп’ютерні науки
Освітня програма Комп’ютерні науки

ЗАТВЕРДЖУЮ

Завідувач кафедри

Н. І. Стяглик

“15” вересня 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЕКТ)

Кравченко Владислава Віталійовича
(прізвище, ім’я, по батькові студента)

1. Тема роботи «Дослідження та розробка програмного забезпечення для системи захищеного зберігання й передавання інформації»

Керівник роботи к.ф.-м.н., доцент Філатова Л. Д.

затверджені наказом по університету від “15” вересня 2025 року №4601-5/3262

2. Строк подання студентом роботи 24 листовада 2025 р.

3. Перелік питань, які потрібно розробити:
У розділі 1: Проаналізувати сучасні технології електронного документообігу, принципи їх функціонування та проблеми інформаційної безпеки.
У розділі 2: Дослідити методи інформаційного захисту, алгоритми шифрування (DES, Triple DES, AES, Blowfish, Twofish, RSA) для захищеного зберігання та передавання даних.
У розділі 3: Розробити програмне забезпечення з паралельними алгоритмами шифрування та провести оцінку продуктивності і ефективності системи.

4. План роботи

№ з/п	Назви етапів роботи
1	Вибір здобувачем теми кваліфікаційної магістерської роботи
2	Затвердження плану і завдання кваліфікаційної магістерської роботи
3	Здача кваліфікаційної магістерської роботи керівнику
4	Підпис кваліфікаційної магістерської роботи у керівника
5	Підпис кваліфікаційної магістерської роботи у нормо контролера
6	Допуск завідувачем кафедри до захисту кваліфікаційної магістерської роботи
7	Захист кваліфікаційної магістерської роботи

5. Дата видачі завдання 15 вересня 2025 року

Студент _____ В. В. Кравченко
Підпис інніціали, прізвище

Керівник роботи _____ Л. Д. Філатова
підпис інніціали, прізвище

РЕФЕРАТ
НА КВАЛІФІКАЦІЙНУ МАГІСТЕРСЬКУ РОБОТУ
«ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СИСТЕМИ ЗАХИЩЕНОГО ЗБЕРІГАННЯ Й ПЕРЕДАВАННЯ ІНФОРМАЦІЇ»
Кравченко Владислав Віталійович

Кваліфікаційна магістерська робота містить 80 сторінок, 3 таблиці, 30 рисунків, список літератури з 21 найменування.

Об'єктом дослідження є процеси захищеного зберігання та передавання інформації в електронних системах документообігу.

Предметом дослідження є методи та алгоритми криптографічного захисту інформації, а також засоби підвищення ефективності їх виконання за допомогою паралельного програмування.

Мета кваліфікаційної магістерської роботи полягає у дослідженні та розробці програмного забезпечення для системи захищеного зберігання й передавання інформації з високим рівнем безпеки та ефективності обробки даних.

Завданнями кваліфікаційної магістерської роботи є:

- провести аналіз сучасних технологій електронного документообігу та методів інформаційного захисту;
- дослідити та обрати ефективні алгоритми шифрування для захищеного зберігання та передавання даних;
- розробити програмне забезпечення з реалізацією паралельних алгоритмів шифрування;
- оцінити продуктивність та ефективність розроблених алгоритмів.

Актуальність дослідження: сучасний розвиток інформаційних технологій створює нові загрози конфіденційності, цілісності та доступності даних в електронних системах документообігу. Розробка ефективних методів та програмних засобів захисту інформації є важливою для забезпечення безпечного обміну даними в корпоративних та державних системах.

За результатами дослідження сформовано основні теоретичні аспекти використання криптографічних алгоритмів (DES, Triple DES, AES, Blowfish, Twofish, RSA) для захищеного зберігання та передавання інформації.

Практична новизна: розроблено програмне забезпечення з реалізацією паралельних алгоритмів шифрування, що дозволяє підвищити ефективність обробки даних та забезпечити високий рівень безпеки інформації. Проведено експериментальне порівняння продуктивності алгоритмів при різних розмірах файлів та різній кількості процесорних ядер.

Одержані результати можуть бути використані для впровадження у корпоративних і державних інформаційних системах, забезпечення безпечного документообігу, розробки навчальних та дослідницьких проєктів у сфері криптографії та інформаційної безпеки.

КЛЮЧОВІ СЛОВА: ЗАХИЩЕНЕ ЗБЕРІГАННЯ ІНФОРМАЦІЇ, ПАРАЛЕЛЬНЕ ШИФРУВАННЯ, AES, DES, 3DES, BLOWFISH, TWOFISH, RSA, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.

ABSTRACT
AT QUALIFICATION MASTER'S WORK
«RESEARCH AND DEVELOPMENT OF SOFTWARE FOR A SECURE INFORMATION STORAGE AND TRANSMISSION SYSTEM»
Vladyslav Kravchenko

The master’s qualification thesis contains 80 pages, 3 tables, 30 figures, and a list of 21 references.

The object of research is the processes of secure storage and transmission of information in electronic document management systems.

The subject of research is the methods and algorithms of cryptographic information protection, as well as means of increasing their execution efficiency using parallel programming.

The aim of the master’s qualification thesis is to research and develop software for a secure information storage and transmission system, ensuring a high level of data security and processing efficiency.

The tasks of the thesis are:

- to analyze modern technologies of electronic document management and information protection methods;
- to research and select effective encryption algorithms for secure data storage and transmission;
- to develop software implementing parallel encryption algorithms;
- to evaluate the performance and efficiency of the developed algorithms.

Relevance of the research: The modern development of information technologies creates new threats to confidentiality, integrity, and availability of data in electronic document management systems. The development of effective methods and software tools for information protection is essential to ensure secure data exchange in corporate and governmental systems.

Results of the research: The main theoretical aspects of using cryptographic algorithms (DES, Triple DES, AES, Blowfish, Twofish, RSA) for secure information storage and transmission have been established.

Practical novelty: Software implementing parallel encryption algorithms has been developed, which improves data processing efficiency and ensures a high level of information security. An experimental comparison of algorithm performance with different file sizes and varying numbers of processor cores has been conducted.

The obtained results can be used for implementation in corporate and governmental information systems, ensuring secure document management, and for the development of educational and research projects in the field of cryptography and information security.

KEYWORDS: SECURE INFORMATION STORAGE, PARALLEL ENCRYPTION, AES, DES, 3DES, BLOWFISH, TWOFISH, RSA, SOFTWARE.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧОК, СИМВОЛІВ І ТЕРМІНІВ 8
ВСТУП 9
РОЗДІЛ 1. АНАЛІТИЧНИЙ ОГЛЯД ТЕХНОЛОГІЙ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ. 11
1.1. Загальні положення і принципи функціонування систем електронного документообігу 11
1.2. Принципи побудови та захисту інформації в системах електронного документообігу 17
1.3. Проблеми забезпечення інформаційної безпеки в системах електронного документообігу та захисту електронних документів 25
1.4. Висновки до розділу 1 30
РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ ІНФОРМАЦІЙНОГО ЗАХИСТУ В СИСТЕМАХ ЗАХИЩЕНОГО ЗБЕРІГАННЯ Й ПЕРЕДАВАННЯ ІНФОРМАЦІЇ 31
2.1. Способи забезпечення захисту інформації в системах електронного документообігу 31
2.2. Способи захищеного передавання та зберігання інформації в системах електронного документообігу 35
2.3. Алгоритм шифрування DES 43
2.4. Алгоритм шифрування Triple DES 45
2.5. Алгоритм шифрування AES 47
2.6. Алгоритм шифрування Blowfish 49
2.7. Алгоритм шифрування Twofish 51
2.8. Алгоритм шифрування RSA 54
2.9. Висновки до розділу 2 55

РОЗДІЛ 3. РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СИСТЕМИ ЗАХИЩЕНОГО ЗБЕРІГАННЯ Й ПЕРЕДАВАННЯ ІНФОРМАЦІЇ 57
3.1. Вибір мови програмування та засобів паралельного програмування 57
3.2. Розробка паралельних алгоритмів шифрування 59
3.3. Оцінювання продуктивності та ефективності паралельної криптографічної системи 62
3.4. Аналіз продуктивності та обговорення результатів експериментального дослідження 64
3.5. Висновки до розділу 3 75
ВИСНОВКИ 77
ПЕРЕЛІК ПОСИЛАНЬ 79

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧОК, СИМВОЛІВ І ТЕРМІНІВ

AES – Advanced Encryption Standard (стандарт розширеного шифрування)

DES – Data Encryption Standard (стандарт шифрування даних)

3DES – Triple Data Encryption Standard

RSA – Rivest–Shamir–Adleman (асиметричний криптографічний алгоритм)

PKI – Public Key Infrastructure (інфраструктура відкритих ключів)

SDK – Software Development Kit (набір засобів для розробки програмного забезпечення)

API – Application Programming Interface (інтерфейс програмування додатків)

LAN – Local Area Network (локальна мережа)

VPN – Virtual Private Network (віртуальна приватна мережа)

ЕЦП – електронний цифровий підпис

КЕП – кваліфікований електронний підпис

ЕД – електронний документ

ЕДО – електронний документообіг

СЕДО – система електронного документообігу

СЗІ – система захисту інформації

ПЗ – програмне забезпечення

ПП – паралельне програмування

ВСТУП

Сучасний розвиток інформаційних технологій зумовлює зростаючу потребу у забезпеченні безпеки електронної інформації, що передається та зберігається в різних системах документообігу. В умовах активного використання електронних сервісів виникають нові загрози конфіденційності, цілісності та доступності даних, що робить актуальним створення ефективних та надійних засобів захисту інформації.

Актуальність теми дослідження полягає у необхідності розробки програмного забезпечення, яке забезпечує захищене зберігання та передавання інформації, використовуючи сучасні криптографічні алгоритми та паралельні обчислення для підвищення продуктивності систем.

Мета роботи полягає у дослідженні та розробці програмного забезпечення для системи захищеного зберігання й передавання інформації, здатного забезпечувати високий рівень безпеки та ефективності обробки даних.

Завдання дослідження включають:

– аналіз сучасних технологій електронного документообігу та методів інформаційного захисту;

– дослідження та вибір ефективних алгоритмів шифрування для захищеного зберігання та передавання даних;

– розробку програмного забезпечення з реалізацією паралельних алгоритмів шифрування;

– оцінювання ефективності розроблених паралельних алгоритмів шифрування.

Об’єкт дослідження – процеси захищеного зберігання та передавання інформації в електронних системах документообігу.

Предмет дослідження – методи та алгоритми криптографічного захисту інформації, а також засоби підвищення ефективності їх виконання за допомогою паралельного програмування.

У вступі представлено актуальність роботи, сформульовано мету та відповідні завдання, об’єкт та предмет дослідження, наведено загальну структуру роботи.

У першому розділі «Аналітичний огляд технологій електронного документообігу та методів захисту інформації» проведено аналіз сучасного стану розвитку систем електронного документообігу, розглянуто принципи їх функціонування та основні проблеми інформаційної безпеки.

У другому розділі «Методи та засоби інформаційного захисту в системах захищеного зберігання й передавання інформації» досліджено алгоритми шифрування (DES, Triple DES, AES, Blowfish, Twofish, RSA) та методи забезпечення конфіденційності, цілісності та доступності даних у системах документообігу.

У третьому розділі «Розробка програмного забезпечення для системи захищеного зберігання й передавання інформації» спроектовано та реалізовано програмне забезпечення з паралельними алгоритмами шифрування, оцінено продуктивність та ефективність системи.

Висновок висвітлює підсумки дослідження, наукову та практичну значущість роботи, а також можливі напрями подальшого розвитку систем захищеного зберігання й передавання інформації.

Практична новизна роботи полягає у розробці програмного забезпечення для паралельного шифрування даних, що дозволяє значно підвищити ефективність систем захищеного зберігання та передавання інформації.

Одержані результати можуть бути використані для впровадження у корпоративних та державних інформаційних системах, забезпечення безпечного документообігу, розробки навчальних та дослідницьких проєктів у сфері криптографії та інформаційної безпеки, а також для подальшого вдосконалення програмних продуктів із захищеного обміну даними.

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД ТЕХНОЛОГІЙ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

1.1. Загальні положення і принципи функціонування систем електронного документообігу

Сучасний розвиток цифрових технологій, розширення телекомунікаційних можливостей та впровадження електронних сервісів на всіх рівнях управління створили сприятливі умови для переходу від традиційного паперового документообігу до повністю електронних систем. Електронний документообіг (ЕДО) став невід’ємною складовою інфраструктури управління інформаційними потоками в державних, комерційних та громадських організаціях. Його основна мета полягає у забезпеченні ефективного, безпечного та юридично значущого обміну інформацією між суб’єктами господарської діяльності. Перехід до ЕДО дає змогу оптимізувати процеси створення, передачі, зберігання й оброблення документів, скоротити витрати часу та ресурсів, а також забезпечити високий рівень контролю за діловими процесами [1].

Електронний документообіг являє собою сукупність технологічних, програмних і організаційних рішень, спрямованих на автоматизацію руху документів у цифровому форматі (рис. 1.1). Основними учасниками цього процесу є автор документа, адресат, система передачі та зберігання, а також засоби перевірки автентичності. Усі документи, які циркулюють у такій системі, мають статус електронних документів, що відповідно до Закону України «Про електронні документи та електронний документообіг» мають юридичну силу, еквівалентну паперовим аналогам за умови використання кваліфікованого електронного підпису (КЕП) [1, 2].

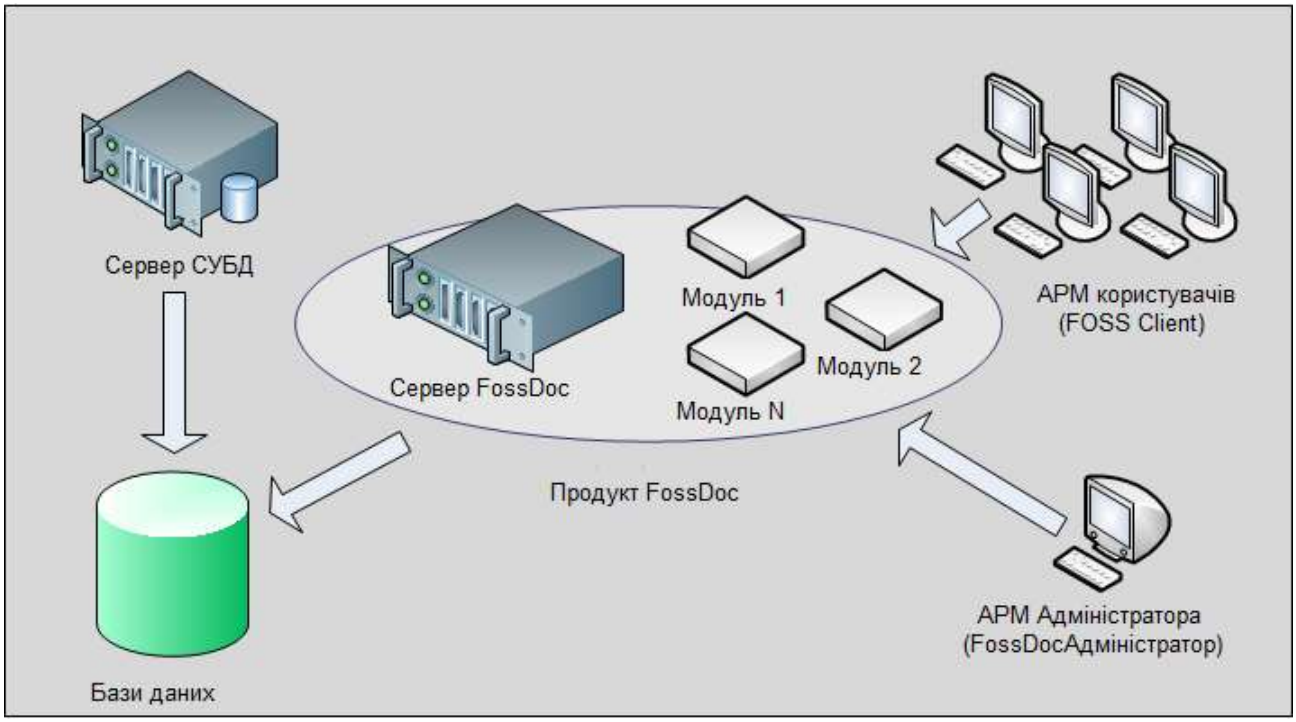

Рис. 1.1. Схема функціонування інформаційної мережі електронного документообігу

Основу будь-якої системи ЕДО становить електронний документ (ЕД) – структурований набір даних, що зберігається у цифровому вигляді та містить обов’язкові реквізити: автора, дату створення, підпис, відомості про адресата та інші метадані, які забезпечують його юридичну значущість і можливість перевірки достовірності. Важливою характеристикою електронного документа є можливість його візуалізації у зрозумілій людині формі, а також підтримка машинного зчитування для автоматизованої обробки в інформаційних системах [2, 3].

Принципи функціонування електронного документообігу базуються на кількох ключових положеннях. Насамперед, це принцип автентичності, що гарантує ідентифікацію автора документа та достовірність його підпису за допомогою криптографічних методів. Другим важливим принципом є цілісність, яка забезпечується неможливістю несанкціонованого внесення змін у вміст документа після його підписання. Третій принцип – доступність, який передбачає можливість швидкого та зручного доступу до документів

усіх уповноважених користувачів у будь-який момент часу. Додатково враховується принцип захищеності інформації, що полягає у використанні засобів шифрування, контрольованого доступу, журналювання дій користувачів і резервного копіювання даних. Реалізація цих принципів забезпечує надійне функціонування системи ЕДО навіть у розподіленому середовищі, де документи передаються між різними організаціями або віддаленими філіями.

Функціонування системи електронного документообігу відбувається в межах визначених етапів життєвого циклу документа. Спочатку створюється електронний документ, який формується у відповідному програмному середовищі або автоматично генерується на основі шаблону. Після створення здійснюється його погодження між відповідальними особами, що може включати кілька рівнів перевірки та підписання. Коли документ набуває остаточного вигляду, він підписується електронним підписом, який виконує функцію юридичного підтвердження автентичності. Далі документ передається адресату через захищений канал зв’язку або внутрішню мережу організації. Після отримання від адресата може вимагатися накладання додаткового підпису або підтвердження отримання. Заключним етапом є архівація документа у системі зберігання, де він зберігається у захищеному вигляді протягом визначеного терміну відповідно до нормативних вимог [4].

Однією з ключових технологічних особливостей ЕДО є застосування КЕП, який базується на принципах асиметричної криптографії. Автор документа використовує закритий ключ для створення підпису, який потім перевіряється відкритим ключем, доступним усім сторонам обміну. Додатковим елементом безпеки є мітка часу, що забезпечує фіксацію точного моменту підписання документа. Цей реквізит видається акредитованим центром сертифікації ключів і гарантує неможливість підроблення або зміщення дати підписання. Таким чином, у разі виникнення спору можна достеменно встановити момент створення й підписання документа, що має важливе значення у юридичній практиці [3].

Ще одним принципом функціонування ЕДО є трасованість або відстежуваність. Усі дії користувачів – створення, перегляд, редагування, передавання чи видалення документа – фіксуються в журналі подій. Це дозволяє забезпечити прозорість процесу документообігу, виявляти несанкціоновані дії та проводити аудит інформаційної безпеки. У сучасних системах ЕДО використовується централізована база даних або розподілена система зберігання, яка гарантує збереження документів навіть у разі технічних збоїв. Для цього застосовуються технології резервного копіювання, реплікації даних і хмарного зберігання з багаторівневим шифруванням [3-5].

Переваги впровадження електронного документообігу є численними та відчутними на всіх рівнях управління. Насамперед, це значне скорочення часу на підготовку, узгодження й доставку документів. Процеси, які раніше займали кілька днів, тепер можуть виконуватись за лічені хвилини. Також істотно зменшуються витрати на папір, друк, зберігання, кур’єрську доставку й архівне обслуговування. Електронні документи не потребують фізичного місця для зберігання, що звільняє ресурси організації. Крім того, ЕДО забезпечує високий рівень контрольованості бізнес-процесів: керівництво має змогу у будь-який момент відстежити, на якому етапі перебуває певний документ, хто його погодив чи затримав. Це сприяє підвищенню дисципліни виконання завдань і прозорості роботи установи.

Ще однією вагомою перевагою є юридична значущість електронних документів, підписаних КЕП, що надає можливість повноцінно використовувати ЕДО у правовому полі без дублювання паперових носіїв. Водночас підвищується інформаційна безпека завдяки використанню криптографічного захисту, розмежуванню прав доступу та багаторівневій автентифікації користувачів. Усі ці механізми зменшують ризики втрати, несанкціонованого доступу або підроблення документів. У контексті захищеного зберігання й передавання інформації це є одним із найважливіших аспектів, що визначають надійність і довіру до системи [4].

Однак, поряд із перевагами, електронний документообіг має певні недоліки та обмеження, що необхідно враховувати під час його впровадження. Найпоширенішою проблемою є залежність від технічної інфраструктури. У разі збою серверів, втрати електроживлення або порушення мережевого з'єднання процес документообігу може бути призупинений. Тому критично важливо передбачати резервні копії, дублювання вузлів і безперервність обслуговування. Іншим суттєвим недоліком є необхідність стандартизації форматів документів. У різних організаціях використовуються різні системи ЕДО, що іноді призводить до проблем сумісності та потребує інтеграційних рішень. Ще одним обмеженням є ризики кібербезпеки: хакерські атаки, фішинг, підроблення сертифікатів чи викрадення ключів підпису можуть поставити під загрозу цілісність даних. Тому важливо дотримуватись політики інформаційної безпеки, проводити регулярний аудит і використовувати сучасні криптографічні алгоритми [3, 5].

Деякі труднощі виникають і на організаційному рівні. Не всі співробітники готові до повного переходу на цифрові технології. Потрібно проводити навчання персоналу, пояснювати особливості користування електронними підписами, правила архівації документів, етичні норми роботи з конфіденційною інформацією. Крім того, виникає потреба у змінах внутрішніх регламентів підприємств, адаптації існуючих процедур до нової форми документообігу. У державному секторі такі зміни часто потребують додаткових нормативних рішень, що може сповільнити процес впровадження.

Попри вказані складнощі, тенденція до цифровізації управління документами є незворотною. Сучасні системи ЕДО інтегруються з іншими інформаційними платформами – системами управління підприємством (ERP), фінансовими модулями, CRM-системами, сервісами обміну даними та хмарними сховищами. Завдяки такій інтеграції формується єдиний інформаційний простір, у якому документи не лише передаються між

підрозділами, а й автоматично генеруються на основі бізнес-процесів. Це забезпечує комплексний контроль за рухом інформації, мінімізує людський фактор і підвищує ефективність прийняття рішень.

Для систем захищеного зберігання та передавання інформації, які є предметом дослідження цієї дипломної роботи, важливим аспектом є забезпечення конфіденційності та достовірності під час обміну документами. Сучасні рішення в цій галузі базуються на використанні криптографічних протоколів SSL/TLS, асиметричних систем шифрування RSA або ECC, а також алгоритмів хешування для створення цифрових відбитків документів. Ці механізми дозволяють гарантувати, що інформація, яка зберігається або передається в межах ЕДО, не може бути змінена чи прочитана третіми особами без відповідних прав доступу [3-5].

Важливою тенденцією є впровадження хмарних систем електронного документообігу, які забезпечують високу доступність і масштабованість, але водночас вимагають посилених засобів захисту даних. Використання хмарних технологій дозволяє підприємствам уникнути великих витрат на власні сервери, забезпечити мобільний доступ до документів і оперативну взаємодію між підрозділами. Однак для реалізації надійного захищеного середовища необхідно застосовувати політики шифрування як під час зберігання, так і при передаванні інформації, а також автентифікацію користувачів на основі багатофакторних методів.

Отже, електронний документообіг є комплексною системою, що об’єднує технологічні, організаційні та правові аспекти управління інформацією. Його впровадження сприяє підвищенню ефективності бізнес-процесів, прозорості діяльності, оптимізації ресурсів та підвищенню рівня інформаційної безпеки. Для досягнення максимальної ефективності важливо не лише застосовувати сучасні програмні рішення, а й створювати комплексну стратегію захисту даних, що охоплює всі етапи життєвого циклу електронного документа – від створення до архівації. У подальших розділах роботи буде розглянуто методи реалізації таких систем, їх архітектуру, а

також підходи до розробки програмного забезпечення, орієнтованого на забезпечення захищеного зберігання та передавання інформації в межах ЕДО.

1.2. Принципи побудови та захисту інформації в системах електронного документообігу

Електронний документообіг являє собою сукупність технологічних, організаційних і програмних рішень, які забезпечують створення, реєстрацію, передачу, зберігання та контроль електронних документів. Його основною метою є мінімізація людського фактору, підвищення оперативності та прозорості процесів, а також гарантування безпеки переданої інформації. Системи ЕДО (рис. 1.2) функціонують у межах як внутрішніх корпоративних мереж, так і у міжорганізаційному середовищі, коли документи передаються між різними юридичними особами. У цьому контексті питання інформаційного захисту набуває особливого значення, адже саме надійність та достовірність переданої інформації визначають рівень довіри до електронного документообігу [3, 4].

Саму повну і максимально надійну схему обміну електронними документами, яка враховує обов’язкові етапи інформаційного захисту даних, можна представити у вигляді послідовності процедур: формування відправником електронної документації (електронного документа), накладання кваліфікованого електронного підпису, передавання документа засобами програми документообігу адресату, забезпечення інформаційного захисту на всіх етапах передавання, здійснення кіберзахисту середовища та інформаційних мереж, отримання документа адресатом, його підписання КЕП отримувача та повернення завізованого екземпляра відправнику (рис. 1.3). У процесі підписання користувачі ЕДО отримують повідомлення про проміжні статуси документа, такі як «доставлено», «погоджено» або «відхилено». Це дозволяє організувати чіткий контроль за життєвим циклом

документа та відстежувати всі дії, які з ним виконуються.

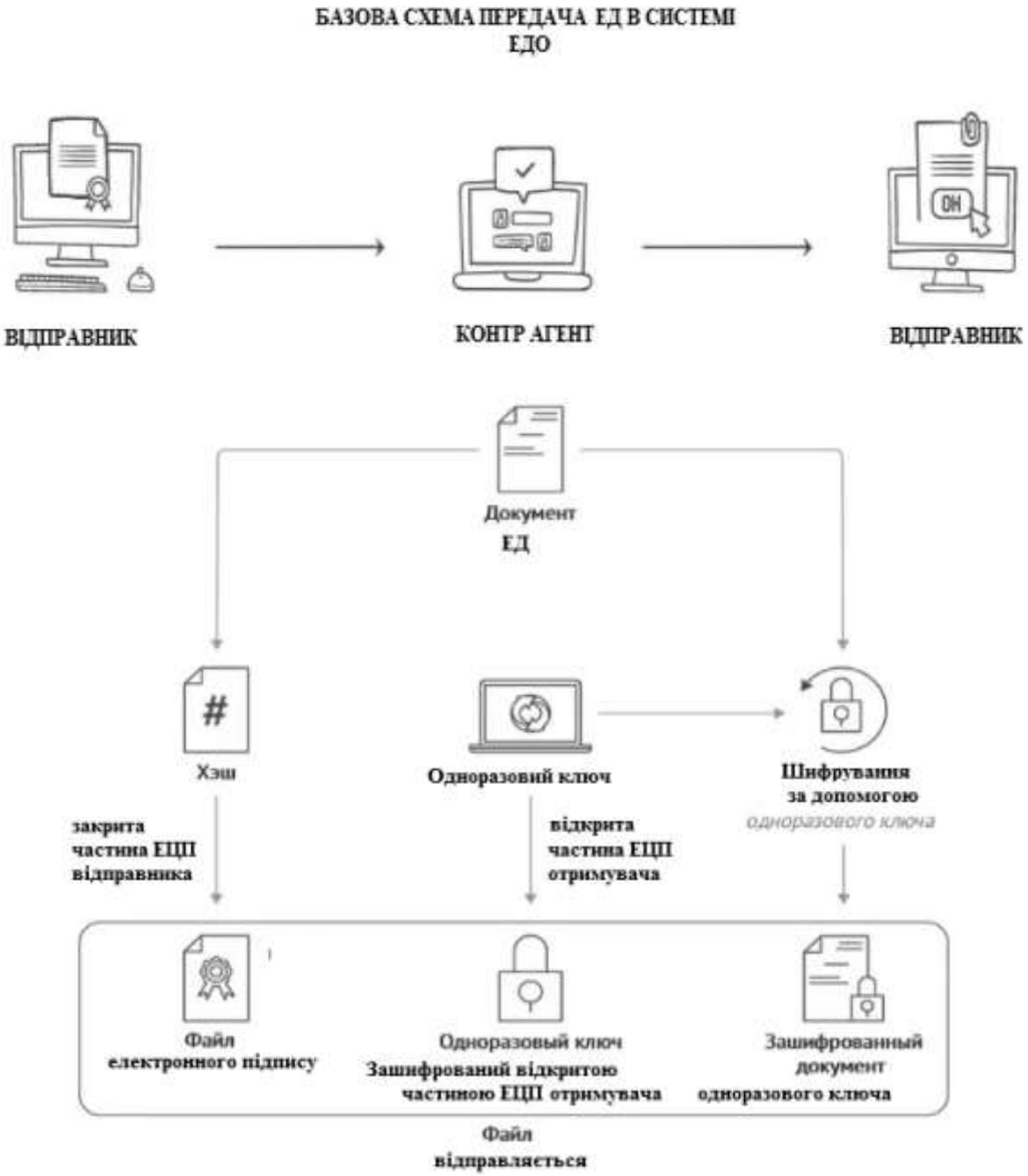

Рис. 1.2. Базова схема передачі електронного документу в системі ЕДО

Процес підписання електронного документа є центральним елементом забезпечення інформаційного захисту. Зазвичай користувачі ЕДО підписують електронні документи базовим одним електронним підписом (ЕЦП). Проте при великому обсязі документообігу в організації створюється спеціальний регламент ведення електронного документообігу, у якому визначаються

порядок застосування електронного підпису, політики безпеки та правила доступу до документів [3, 4].

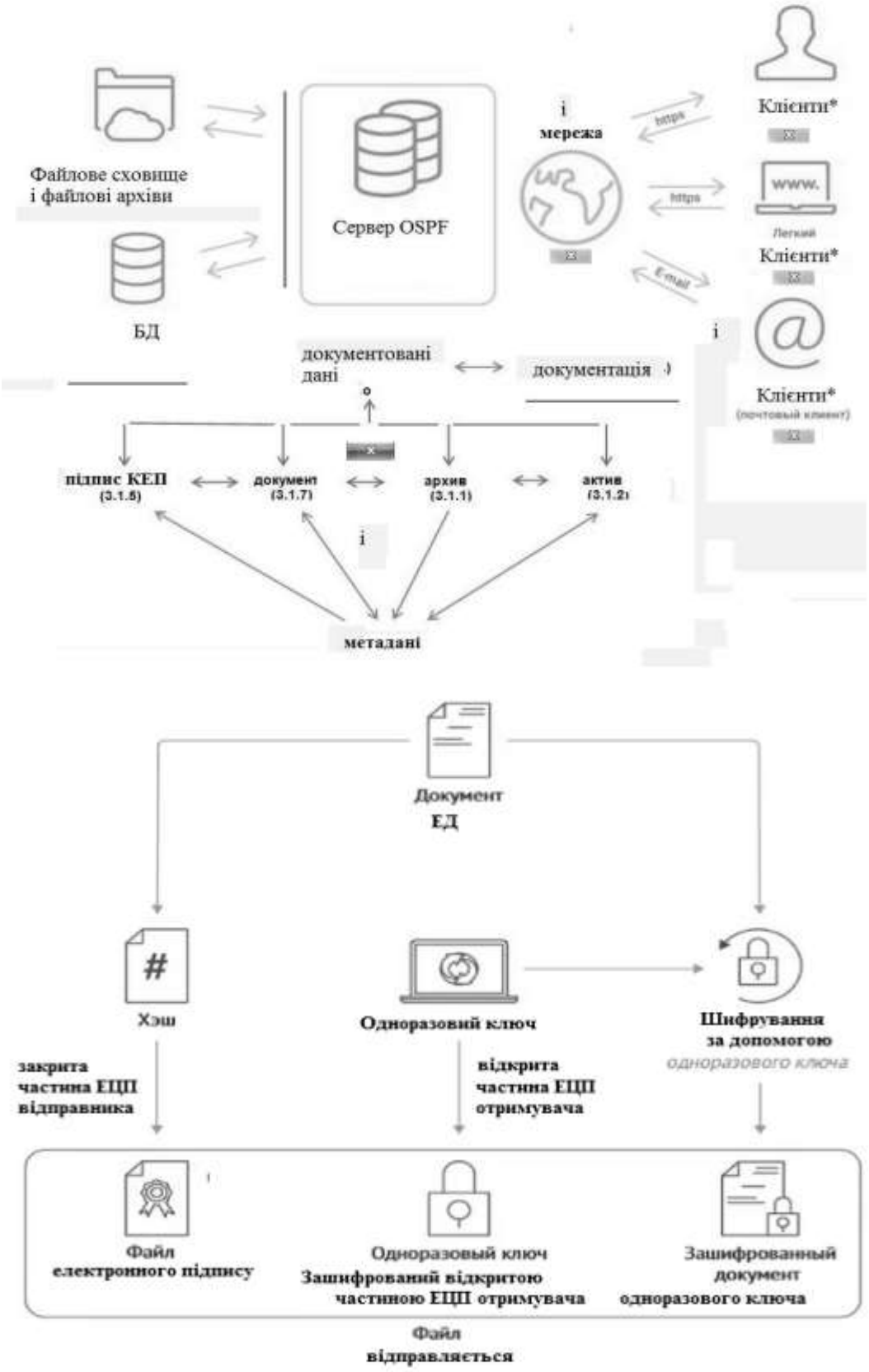

Рис. 1.3. Схема передачі електронного документу в системі ЕДО із ЕЦП

Ключ електронного підпису, відомий як кваліфікований електронний підпис, складається з секретного (особистого) ключа та сертифіката відкритого ключа, які використовуються виключно в парі. Секретний ключ генерується як унікальна послідовність випадкових символів, тоді як сертифікат відкритого ключа формується на його основі. Важливо, що неможливо отримати секретний ключ із сертифікату відкритого ключа, що забезпечує криптографічну стійкість системи [3-5].

Сертифікат відкритого ключа містить персональні дані власника – ім’я, реєстраційний номер, орган, який видав сертифікат, та строк його дії. Він підписується секретним ключем Центру сертифікації ключів, який гарантує достовірність та авторитетність підпису. Центр сертифікації виступає довіреною третьою стороною, яка підтверджує, що певний відкритий ключ дійсно належить конкретній особі. У системах ЕДО такі центри є основою інфраструктури відкритих ключів (PKI), без якої неможливо забезпечити юридичну значущість електронних документів [5, 6].

Під час підписування електронного документа його вміст залишається незмінним, а до файлу додається спеціальний блок даних – електронний підпис. Формування цього підпису складається з декількох етапів (рис. 1.4). Спочатку від тексту документа обчислюється хеш – унікальний цифровий відбиток, що створюється за допомогою криптографічної хеш-функції (наприклад, SHA-256). Потім цей відбиток шифрується секретним ключем підписувача за допомогою алгоритму асиметричного шифрування, як-от RSA або ECDSA. У результаті формується цифровий підпис, який додається до документа.

Під час перевірки підпису отримувач розшифровує його за допомогою відкритого ключа автора та повторно обчислює хеш отриманого документа (рис. 1.5). Якщо обидва відбитки співпадають, це означає, що документ не зазнав змін, а підпис справді належить вказаному автору. У випадку, якщо хоча б один байт інформації у документі змінено, його цифровий відбиток буде іншим, і система вкаже на невідповідність підпису. Таким чином,

цифровий відбиток (ЦВ) і ЕЦП є основними засобами забезпечення цілісності й автентичності документів [5, 6].

Рис. 1.4. Схема формування ЕЦП

Рис. 1.5. Схема перевірки справжностиі ЕЦП

При модифікації електронного документа змінюється його хеш-функція або контрольна сума, що може слугувати індикатором

несанкціонованого втручання або інформаційної модифікації. Саме тому перевірка електронних підписів є обов’язковою процедурою у процесі обміну документами. Вона дозволяє не лише виявляти зміни у вмісті, а й підтверджувати авторство, що є важливою складовою юридичної значущості електронного документообігу.

Розшифрування електронного цифрового підпису та отримання початкового цифрового відбитка, який відповідає документу, можливе лише за допомогою сертифіката відкритого ключа. Перевірка підпису відбувається у кілька етапів: спочатку отримувач визначає унікальний цифровий відбиток отриманого документа, потім розшифровує електронний підпис за допомогою сертифіката відкритого ключа автора і отримує відбиток початкового документа, після чого система порівнює обидва значення. Якщо вони збігаються, документ вважається автентичним і незміненим [3-6].

Загалом, системи електронного документообігу поділяються на внутрішні та зовнішні. Внутрішній ЕДО передбачає обмін електронними документами всередині однієї організації, включаючи кадрові накази, розпорядження, внутрішні листи, звіти, аналітичні довідки тощо. Для таких систем зазвичай використовуються корпоративні рішення типу BAS або M.E.Doc, які дозволяють створювати, підписувати і зберігати документи у межах однієї структури. Зовнішній ЕДО забезпечує обмін документами між різними підприємствами, установами або державними органами. До цієї категорії належать договори, рахунки-фактури, акти виконаних робіт, накладні, довіреності, офіційні листи та інші документи, що мають юридичну силу. Усі ці документи можуть бути перетворені з паперової форми у цифрову з дотриманням вимог безпеки та автентичності.

Важливою складовою побудови систем ЕДО є організація інформаційного захисту. Безпека інформації в таких системах забезпечується на кількох рівнях: програмному, апаратному та організаційному. До основних механізмів захисту належать ідентифікація та автентифікація користувачів, керування правами доступу, шифрування даних, цифровий

підпис, аудит дій користувачів, контроль цілісності баз даних, а також резервне копіювання та відновлення інформації [5, 6].

Ідентифікація користувачів дозволяє точно визначити особу, яка виконує дії у системі, тоді як автентифікація підтверджує справжність цієї особи. У сучасних системах ЕДО для автентифікації використовують багаторівневі методи: паролі, токени, сертифікати, біометричні дані. Після успішної автентифікації користувачу надаються певні права доступу відповідно до його ролі. Це дозволяє реалізувати принцип мінімально необхідних привілеїв, згідно з яким кожен користувач має доступ лише до тих ресурсів, що потрібні для виконання службових обов’язків.

Одним із найважливіших аспектів є захист комунікаційних каналів, через які передаються документи. Для цього застосовуються протоколи SSL/TLS, які забезпечують шифрування переданих даних і запобігають перехопленню або модифікації повідомлень під час передачі. У корпоративних мережах використовуються також VPN-з’єднання, що створюють захищений тунель між клієнтом і сервером системи ЕДО [6, 7].

Цілісність інформації забезпечується за допомогою контрольних сум і журналів аудиту, які фіксують усі зміни в системі. Автоматизовані системи моніторингу дозволяють відстежувати дії користувачів, аналізувати логи, виявляти підозрілі операції та своєчасно реагувати на інциденти безпеки. У разі виявлення аномалій адміністратор може заблокувати обліковий запис користувача або обмежити доступ до системи.

Особливу увагу слід приділяти захисту даних під час зберігання. Сучасні системи ЕДО зберігають документи у базах даних або файлових сховищах, доступ до яких здійснюється через спеціалізовані програмні інтерфейси. Важливо, щоб дані зберігалися у зашифрованому вигляді з використанням надійних алгоритмів, таких як AES або 3DES. Для забезпечення стійкості системи до збоїв необхідно впроваджувати регулярне резервне копіювання та мати плани відновлення після аварій [6, 7].

У сучасних умовах розвитку інформаційних технологій системи ЕДО

поступово інтегруються з іншими сервісами, зокрема хмарними сховищами, сервісами електронної ідентифікації, бухгалтерськими системами та аналітичними платформами. Такі інтеграції дозволяють підвищити ефективність документообігу, проте створюють додаткові виклики у сфері кібербезпеки. Саме тому у хмарних рішеннях ЕДО особливу увагу приділяють автентифікації користувачів, контролю доступу, шифруванню трафіку та перевірці цілісності даних.

Подальший розвиток систем електронного документообігу пов’язаний із впровадженням технологій блокчейн, які забезпечують незмінність історії документів і прозорість усіх операцій. Завдяки розподіленому характеру зберігання даних у блокчейні практично неможливо підробити або видалити запис без відображення цього факту в усьому ланцюгу. Інтеграція блокчейн-технологій у ЕДО дозволяє створювати децентралізовані платформи з високим рівнем довіри між учасниками.

Крім того, у перспективі системи ЕДО можуть використовувати інструменти штучного інтелекту для автоматизації класифікації документів, виявлення аномалій, прогнозування ризиків безпеки та оптимізації маршрутизації інформаційних потоків. Такі рішення сприятимуть подальшому підвищенню надійності, стабільності та ефективності систем електронного документообігу.

Отже, принципи побудови та захисту інформації в системах ЕДО базуються на комплексному підході, який охоплює технічні, криптографічні та організаційні заходи. Забезпечення конфіденційності, цілісності та доступності даних, впровадження кваліфікованого електронного підпису, керування доступом, використання сучасних протоколів шифрування й засобів моніторингу безпеки є фундаментом для побудови надійної системи документообігу, здатної функціонувати у сучасних умовах цифрової економіки.

1.3. Проблеми забезпечення інформаційної безпеки в системах електронного документообігу та захисту електронних документів

Основною проблемою сучасних систем ЕДО є забезпечення комплексного захисту інформації, яка циркулює у процесі створення, зберігання, оброблення та передачі електронних документів. Інформаційна безпека в ЕДО охоплює як технічні, так і організаційні аспекти. З технічного боку – це питання криптографічного захисту, управління доступом, цілісності даних, резервного копіювання та відновлення, а з організаційного – регламентація процедур, управління ризиками, контроль дій користувачів і підготовка персоналу. У контексті розроблення програмного забезпечення для захищеного зберігання і передавання інформації актуальним стає поєднання обох підходів у єдину модель безпеки, що здатна протидіяти сучасним кіберзагрозам.

Однією з найпоширеніших проблем є витік конфіденційних документів. Це може бути результатом як зовнішнього втручання, так і внутрішніх порушень політики безпеки. У випадку зовнішнього витоку причиною можуть бути атаки на сервери ЕДО, перехоплення мережевого трафіку, фішингові кампанії або використання шкідливого програмного забезпечення, яке отримує доступ до сховищ даних. Внутрішні витоки найчастіше зумовлені недоліками у системі контролю доступу або навмисними діями співробітників, які мають повноваження переглядати чи копіювати документи. Для мінімізації цього ризику використовуються засоби розмежування прав доступу, журнали аудиту дій користувачів, системи виявлення аномальної поведінки, а також обов’язкове шифрування усіх файлів, що передаються через мережу [5-7].

Другою суттєвою загрозою є несанкціоноване спотворення або модифікація документів. Навіть незначна зміна даних може мати серйозні наслідки для організації, оскільки електронні документи часто мають юридичну силу. Для захисту від модифікацій застосовуються електронні

цифрові підписи та хеш-функції, які дозволяють підтвердити автентичність документа. Проте на практиці можливі спроби підробки підписів або використання компрометованих ключів. Проблема посилюється тим, що алгоритми підпису або засоби зберігання ключів можуть містити вразливості, якими зловмисники користуються для створення фальшивих документів. Надійний захист ЕДО передбачає використання КЕП, сертифікованих криптографічних бібліотек, а також регулярне оновлення сертифікатів та перевірку їх чинності через центри сертифікації ключів [5-7].

Ще однією важливою проблемою є знищення або пошкодження документів, яке може бути як навмисним, так і випадковим. У разі кібератаки зловмисники можуть видалити або шифрувати базу даних, вимагаючи викуп (атаки типу ransomware). Також можлива втрата інформації внаслідок збоїв обладнання або помилок під час оновлення програмного забезпечення. Для запобігання таким інцидентам необхідно забезпечити багаторівневе резервне копіювання, географічно розподілені сховища та автоматизоване відновлення даних із перевіркою цілісності. Програмне забезпечення, що розробляється для захищеного зберігання інформації, повинно мати вбудовані механізми журналювання, контрольних сум і перевірки хешів, що дозволяють відстежувати будь-які зміни у документах.

Критичною загрозою для систем ЕДО є модифікація або підробка електронного підпису. Це може відбутися через викрадення приватного ключа користувача або створення підробленого сертифіката. У таких випадках зловмисник отримує можливість підписувати документи від імені легітимного користувача, що може призвести до серйозних юридичних наслідків. Захист від цієї загрози передбачає використання апаратних криптомодулів (токенів, смарт-карт), які зберігають ключі у зашифрованому вигляді і не дозволяють їх копіювання. Також важливим є застосування двофакторної автентифікації, що ускладнює доступ до ключів навіть у випадку компрометації пароля [7, 8].

Істотною проблемою сучасних систем є недостатня стійкість до атак

нульового дня (zero-day vulnerabilities). Такі уразливості виникають через помилки у програмному коді, які ще не були виявлені розробниками. Зловмисники активно використовують їх для проникнення у системи ЕДО та викрадення інформації. Для протидії цьому необхідно впроваджувати системи моніторингу аномалій, аналізу поведінки процесів, регулярного тестування на проникнення (penetration testing) і використання багаторівневої архітектури безпеки. Сучасні рішення можуть застосовувати машинне навчання для виявлення нетипових дій користувачів або автоматизованих ботів, що намагаються отримати несанкціонований доступ до документів.

Ще одним важливим аспектом є вразливості у програмному забезпеченні систем ЕДО. Багато організацій використовують комерційні або відкриті програмні продукти для управління документообігом, не завжди оновлюючи їх вчасно. Вразливі версії бібліотек, серверів або баз даних створюють ризик проникнення через відомі експлойти. Тому критично важливо впроваджувати політику регулярного оновлення, тестування коду та використання сертифікованих засобів криптографічного захисту інформації (СКЗІ). Під час розроблення нового програмного забезпечення для ЕДО доцільно дотримуватись принципів безпечного програмування (Secure Coding) і стандартів ISO/IEC 27001, які регламентують вимоги до інформаційної безпеки [7, 8].

Велике значення має захист носіїв криптографічних ключів, які використовуються для створення електронних підписів. У багатьох випадках ключі зберігаються на локальних комп’ютерах у вигляді файлів, що створює ризик їх викрадення. Безпечніше використовувати апаратні сховища, які ізолюють криптографічні операції від основної операційної системи. У разі викрадення пристрою дані всередині залишаються недоступними без PIN-коду або біометричної автентифікації. Додатково для кожного користувача має бути передбачена система журналювання дій і перевірки часу використання ключа, що дозволяє оперативно виявляти аномалії.

Нерідко причиною порушень безпеки стає низький рівень кваліфікації

користувачів або відсутність чітких регламентів роботи. Наприклад, співробітники можуть залишати облікові дані на робочому столі, передавати паролі колегам або використовувати незахищені канали зв’язку для обміну документами. Вирішення цієї проблеми потребує розроблення внутрішніх політик інформаційної безпеки, проведення навчань і тестування персоналу. Крім того, системи ЕДО мають автоматично контролювати дотримання політик, наприклад, вимагати регулярної зміни паролів або блокувати доступ після тривалої бездіяльності [7, 8].

Не менш важливою є проблема автентифікації користувачів. У багатьох організаціях досі застосовується проста парольна система, що не забезпечує належного рівня захисту. У сучасних умовах рекомендовано впроваджувати багатофакторну автентифікацію, де крім пароля використовується додатковий фактор – одноразовий код, біометричний параметр або апаратний ключ. Це значно підвищує рівень безпеки і зменшує ризик несанкціонованого входу навіть у разі компрометації облікових даних.

Ще одна поширена загроза – перевищення прав доступу. Нерідко користувачі мають ширші повноваження, ніж потрібно для виконання їхніх функцій. Це створює можливості для випадкового або навмисного пошкодження даних. Принцип мінімальних привілеїв (least privilege) має бути основою політики безпеки. Адміністратор системи повинен надавати кожному користувачу лише ті права, які необхідні для виконання конкретних завдань. Додатково застосовується рольова модель доступу (RBAC), яка дозволяє централізовано керувати повноваженнями [8].

Комплексна система захисту інформації в ЕДО повинна також враховувати загрози внутрішнього характеру, пов’язані із саботажем або помилками персоналу. Для цього необхідно реалізувати систему аудиту дій користувачів, яка фіксує всі операції із документами. Аналіз журналів подій дозволяє швидко виявити підозрілі дії, спроби несанкціонованого доступу або копіювання документів. У поєднанні з аналітичними модулями така система може автоматично сповіщати службу безпеки про потенційні

інциденти.

Окремо варто розглянути загрози, пов’язані з використанням хмарних сервісів для зберігання документів. Незважаючи на зручність і масштабованість, хмарні рішення несуть ризики витоку даних через помилки конфігурації або компрометацію облікових записів постачальника. Для зниження цих ризиків слід використовувати наскрізне шифрування (end-to-end encryption), коли навіть постачальник не має доступу до вмісту файлів. Також важливо обирати провайдерів, які сертифіковані за міжнародними стандартами безпеки.

Загалом, ефективний захист інформації в системах електронного документообігу базується на поєднанні технологічних, криптографічних і організаційних заходів. Розроблення програмного забезпечення для захищеного зберігання й передавання даних повинно враховувати всі ці аспекти. Доцільно реалізувати модульну архітектуру, де окремо функціонують підсистеми автентифікації, управління ключами, шифрування, аудиту та контролю доступу. Це дозволяє швидко оновлювати окремі компоненти без порушення роботи всієї системи. Важливим напрямом розвитку є також інтеграція механізмів штучного інтелекту для прогнозування потенційних загроз і автоматичного реагування на інциденти.

Таким чином, проблеми інформаційної безпеки систем електронного документообігу мають комплексний характер і потребують системного підходу до їх вирішення. Захист електронних документів неможливий без належного управління ключами, моніторингу подій, навчання користувачів і застосування сучасних криптографічних методів. У межах розроблення власного програмного забезпечення для захищеного зберігання та передавання інформації доцільно реалізувати механізми багаторівневого шифрування, контроль доступу за ролями, а також інтелектуальний аналіз логів безпеки. Тільки така інтегрована система може гарантувати цілісність, автентичність і конфіденційність документів, що циркулюють в електронному документообігу сучасних організацій.

1.4. Висновки до розділу 1

У першому розділі проведено аналітичний огляд сучасних технологій електронного документообігу та методів захисту інформації, що застосовуються у корпоративних та державних системах. Розглянуто основні принципи функціонування систем електронного документообігу, включно з організацією потоків документів, їхнім зберіганням, обробкою та контролем доступу. Виявлено, що ефективність таких систем значною мірою залежить від правильної архітектури даних, інтеграції з корпоративними ресурсами та підтримки стандартизованих протоколів обміну інформацією.

Детально проаналізовано принципи побудови систем захисту інформації, включаючи використання криптографічних алгоритмів, цифрових підписів та контролю доступу. Підкреслено важливість комплексного підходу до захисту даних, що поєднує технічні, організаційні та процедурні засоби безпеки.

Виявлено основні проблеми забезпечення інформаційної безпеки в системах електронного документообігу, серед яких високий ризик несанкціонованого доступу, загрози цілісності та конфіденційності електронних документів, а також складність управління правами доступу у великих корпоративних середовищах. Аналіз показав необхідність застосування сучасних технологій шифрування та контролю автентичності документів для підвищення безпеки інформаційних систем.

Отже, проведене дослідження підкреслює актуальність впровадження комплексних заходів інформаційної безпеки в електронному документообігу та обґрунтовує необхідність розробки програмних засобів, які забезпечують одночасно надійний захист інформації та ефективну обробку документів. Отримані результати формують основу для наступного розділу, присвяченого практичній реалізації захищених паралельних алгоритмів шифрування.

РОЗДІЛ 2
МЕТОДИ ТА ЗАСОБИ ІНФОРМАЦІЙНОГО ЗАХИСТУ В СИСТЕМАХ ЗАХИЩЕНОГО ЗБЕРІГАННЯ Й ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

2.1. Способи забезпечення захисту інформації в системах електронного документообігу

Безпосередній захист системи електронного документообігу на підприємстві або в установі може бути організований комплексно – через поєднання програмних, організаційних, криптографічних і технічних заходів. Власники інформації та документів часто побоюються впровадження електронного документообігу саме через питання безпеки – побоюючись витоків, модифікацій або несанкціонованого доступу до інформації. Проте на практиці більшість загроз можна ефективно мінімізувати шляхом використання сучасних засобів захисту даних, перевірених технологій шифрування, розмежування доступів і регулярного аудиту інформаційних систем [5-8].

Одним із базових критеріїв надійності ЕДО є забезпечення збереження електронних документів у складі системи. Збереження включає кілька рівнів: локальне резервне копіювання, архівування в захищених базах даних, використання хмарних сховищ з підвищеним рівнем криптографічного захисту. У межах розробки програмного забезпечення для захищеного зберігання інформації передбачається застосування алгоритмів симетричного та асиметричного шифрування для файлів архіву, що забезпечує неможливість доступу до документів сторонніми особами навіть у випадку компрометації частини інфраструктури. Важливим компонентом є створення багаторівневої системи резервного копіювання, яка гарантує відновлення інформації у випадку збою або атаки типу ransomware [6, 7].

Наступним аспектом є організація закритого доступу до системи ЕДО. Для входу користувача в особистий кабінет або для виконання операцій з

документами необхідна процедура аутентифікації, що може мати різні рівні складності. Найпоширенішим є парольний захист у поєднанні з фізичними токенами або смарт-картами, на яких зберігаються криптографічні ключі. У сучасних рішеннях реалізується багатофакторна аутентифікація (multi-factor authentication, MFA), яка поєднує декілька способів підтвердження особи – наприклад, пароль, одноразовий код, біометричні параметри або цифровий сертифікат. Застосування багаторівневого підходу значно підвищує стійкість системи до атак типу “викрадення облікових даних” або “підміна особи” [8].

Біометричні технології ідентифікації користувачів – такі як розпізнавання обличчя, відбитків пальців, голосу чи сітківки ока – дають змогу забезпечити максимальну достовірність ідентифікації, оскільки біометричні характеристики є унікальними. Однак впровадження таких методів потребує значних фінансових витрат і технічного оснащення користувачів відповідними пристроями, тому їх застосування частіше спостерігається в державних або великих корпоративних структурах.

Не менш важливим елементом є розмежування прав доступу в системі ЕДО. Кожен користувач системи має отримувати лише ті права, які необхідні для виконання його посадових обов’язків. Реалізація цього принципу (“принцип мінімальних прав доступу”) запобігає несанкціонованим діям навіть у випадку компрометації одного з облікових записів. У межах програмного забезпечення розподіл доступу можна реалізувати через гнучку систему ролей (role-based access control, RBAC) або атрибутивну модель (attribute-based access control, ABAC), де рішення про надання доступу приймається на основі набору умов, включно з контекстом операції, рівнем користувача, часом доби чи типом пристрою [8].

Забезпечення конфіденційності даних в ЕДО є одним із ключових завдань. Для цього застосовуються криптографічні методи шифрування як на рівні зберігання, так і під час передавання документів між учасниками системи. Використання сучасних алгоритмів (AES, RSA, ECC) дозволяє запобігти несанкціонованому перегляду або модифікації даних навіть у разі

перехоплення мережевого трафіку. Для підвищення рівня безпеки програмне забезпечення повинно реалізовувати протоколи захищеного передавання інформації, зокрема TLS 1.3, що забезпечує шифрування каналу зв’язку між клієнтом і сервером.

Збереження достовірності інформації в електронному документообігу реалізується через використання ЕЦП, який гарантує, що документ не було змінено після підписання і що авторство документа може бути підтверджене. Удосконалений електронний підпис (УЕП) і кваліфікований електронний підпис є двома основними типами, які застосовуються в Україні відповідно до чинного законодавства. КЕП має вищий рівень захисту, оскільки створюється із застосуванням сертифікованого засобу та зберігається на захищеному носії (токені або у хмарі сертифікованого провайдера). Під час накладання КЕП формується хеш-функція документа, яка потім шифрується приватним ключем підписувача. Перевірка підпису здійснюється з використанням відкритого ключа, і будь-яка зміна в документі після підписання призводить до невідповідності контрольної суми, що унеможливлює фальсифікацію [8, 9].

Для захищеного передавання документів у межах системи розробляються механізми взаємної автентифікації, коли кожен учасник процесу підтверджує свою особу за допомогою сертифікатів відкритих ключів. Такий підхід гарантує, що документ може бути надісланий лише довіреному адресату. При цьому застосовується подвійне шифрування – спочатку симетричним ключем, потім шифрування самого ключа відкритим ключем отримувача. Це забезпечує конфіденційність і автентичність інформації навіть у відкритих мережах.

Важливою складовою комплексного захисту є протоколювання дій користувачів і подій системи. Журнали аудиту дають змогу відстежувати спроби несанкціонованого доступу, модифікацій документів або спроб обійти політики безпеки. У сучасних системах реалізуються алгоритми аналізу поведінки користувачів (User Behavior Analytics), які за допомогою

методів машинного навчання виявляють аномальні дії, що можуть свідчити про внутрішні загрози або зловживання правами доступу.

Додаткову роль у захисті ЕДО відіграє політика управління паролями та кібергігієною користувачів. Програмні рішення повинні забезпечувати автоматичний контроль складності паролів, регулярну зміну облікових даних, обмеження кількості невдалих спроб входу та автоматичне блокування облікових записів при підозрі на компрометацію. Важливо також проводити навчання користувачів основам інформаційної безпеки – адже більшість інцидентів пов’язані з людським фактором.

У контексті розробки програмного забезпечення для захищеного зберігання й передавання інформації одним із перспективних напрямів є впровадження технологій блокчейн для реєстрації фактів підписання, передавання й отримання документів. Завдяки розподіленій природі блокчейн-технології дані про операції не можуть бути змінені без виявлення, що забезпечує прозорість, достовірність і довіру до системи.

Високий рівень захисту вимагає також використання сучасних засобів контролю мережевого трафіку, міжмережевих екранів, систем виявлення вторгнень (IDS/IPS) та антивірусного захисту. Для підвищення стійкості системи до атак нульового дня (zero-day) застосовуються механізми оновлення компонентів програмного забезпечення, моніторинг актуальних уразливостей і застосування патчів безпеки.

У процесі впровадження електронного документообігу важливо також враховувати фізичну безпеку серверного обладнання, безпечне зберігання резервних носіїв та захист середовища зберігання криптографічних ключів. Використання апаратних модулів безпеки (Hardware Security Module, HSM) дозволяє ізолювати ключову інформацію від решти системи, що істотно зменшує ризик її компрометації.

Таким чином, ефективний захист систем електронного документообігу базується на поєднанні трьох основних складових: технічної, організаційної та програмної. Програмне забезпечення для захищеного зберігання й

передавання інформації повинно реалізовувати комплексну архітектуру безпеки, у якій кожен рівень – від автентифікації користувачів до зберігання даних – має власні механізми контролю доступу, шифрування та аудиту. Реалізація таких підходів забезпечує не лише відповідність законодавчим вимогам, а й створює основу для довіри користувачів до електронного документообігу як до безпечного, надійного й ефективного інструменту сучасного інформаційного суспільства.

2.2. Способи захищеного передавання та зберігання інформації в системах електронного документообігу

У сучасних інформаційних системах ЕДО однією з ключових проблем є забезпечення надійного та безпечного обміну електронними документами ЕД між користувачами системи. Питання інформаційної безпеки охоплює як внутрішні процеси організації, так і зовнішні канали передачі даних, у тому числі мережеві. Ненадійне з’єднання або відкритість каналів комунікації може призводити до втрат конфіденційної інформації, перехоплення даних, модифікації електронних документів або реалізації атак типу «людина посередині» (MITM). Зважаючи на це, розробка програмного забезпечення для системи захищеного зберігання й передавання інформації повинна базуватися на комплексному підході до захисту як самих документів, так і каналів їх передавання [7-9].

Основним елементом захищеного зберігання та передавання інформації в ЕДО є контроль доступу користувачів та аутентифікація. Доступ до системи має бути обмежений і багаторівневим: від базового введення пароля до використання криптографічних токенів та біометричних даних. Багатофакторна аутентифікація дозволяє знизити ризик несанкціонованого доступу, адже навіть при компрометації одного з факторів – пароля чи ключа – третя особа не зможе отримати повний доступ до системи. Для підвищення надійності біометрична аутентифікація використовує відбитки пальців,

сканування сітківки ока або голосові дані користувача, що забезпечує високий рівень безпеки, хоча й вимагає відповідного апаратного забезпечення та підготовки користувачів. Крім того, розмежування прав доступу до документів дозволяє обмежити коло користувачів, які можуть редагувати, переглядати або підписувати певні електронні документи, що особливо важливо у великих організаціях з багаторівневою структурою управління.

Для забезпечення цілісності та достовірності електронних документів у сучасних системах ЕДО використовується електронний цифровий підпис. Основні його види включають кваліфікований електронний підпис та удосконалений електронний підпис. КЕП зберігається на захищеному носії, такому як токен або хмарний сервіс провайдера, і забезпечує високий рівень захисту від несанкціонованої модифікації документу, а також підтверджує авторство. УЕП зазвичай зберігається на локальних носіях користувача і має нижчий рівень захисту, хоча також дозволяє підтверджувати достовірність документів. При накладанні ЕЦП на документ формується цифровий відбиток (hash), який перевіряється під час отримання документа. Зміни у вмісті документа після підписання призводять до невідповідності хешів, що дозволяє виявити спроби підробки або модифікації. Цей механізм є базовим у забезпеченні довіри до електронних документів у рамках розробки захищених систем ЕДО [5, 7].

Захищене передавання електронних документів через інформаційні мережі – не менш важливий аспект безпеки ЕДО. Найбільш поширеними протоколами для передачі файлів є FTP та його безпечна модифікація SFTP. Класичний FTP (рис. 2.1) передає дані у відкритому вигляді, що робить його вразливим до перехоплення даних і компрометації облікових записів. Протокол SFTP (Secure File Transfer Protocol) забезпечує шифрування всієї інформації, включно з обліковими даними, через використання протоколу SSH. Це дозволяє забезпечити конфіденційність, цілісність та автентичність переданих даних. У SFTP аутентифікація може здійснюватися за допомогою

пароля або пари криптографічних ключів, що додатково підвищує рівень безпеки. Важливим аспектом SFTP є підтримка широкого спектра клієнтських додатків, таких як FileZilla, WinSCP або CyberDuck, що спрощує інтеграцію цього протоколу у корпоративні системи ЕДО [5-7].

Рис. 2.1. Схема роботи протоколу FTP

Альтернативною архітектурою для передавання даних є однорангові P2P (Peer-to-Peer) мережі, де кожен вузол виступає одночасно клієнтом і сервером. P2P-системи забезпечують високу відмовостійкість та масштабованість при великому числі користувачів, оскільки передача даних відбувається частинами через незалежні канали. Проте P2P-системи мають складніший контроль доступу і підвищені ризики поширення шкідливого програмного забезпечення або витоку конфіденційних даних. Для забезпечення безпеки в P2P-мережах доцільно застосовувати криптографічні методи шифрування, автентифікації користувачів та цифрового підпису, що забезпечує відповідність сучасним вимогам до захищених систем ЕДО.

Не менш важливою технологією захищеного доступу є VPN (Virtual Private Network). Використання VPN (рис. 2.2) дозволяє створювати захищені підмережі поверх загальнодоступних мереж, таких як Інтернет, і забезпечує безпечний доступ до корпоративних ресурсів. VPN забезпечує шифрування даних, тунелювання і контроль доступу, використовуючи алгоритми AES, Blowfish або 3DES. VPN може бути реалізовано як апаратними, так і

програмними засобами, включно з мобільними клієнтами, що дозволяє підключатися до корпоративної мережі з будь-якої точки світу. Основні типи VPN включають Remote Access VPN для мобільних співробітників, Intranet VPN для з'єднання центрального офісу з філіями та Extranet VPN для доступу партнерів та постачальників. Завдяки VPN можна забезпечити конфіденційність, цілісність та контроль доступу до даних, що є критично важливим у системах захищеного зберігання й передавання інформації.

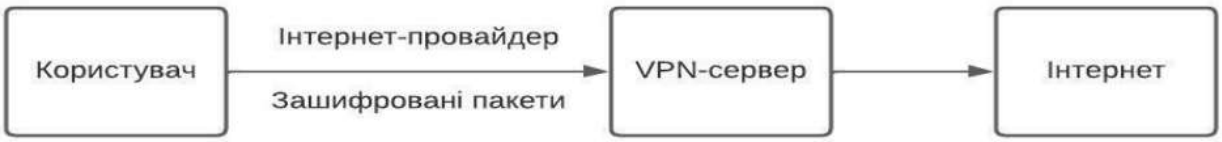

Рис. 2.2. Схема роботи VPN

Для забезпечення безпеки веб-комунікацій у ЕДО застосовується протокол HTTPS, який базується на криптографічному протоколі SSL/TLS. Протокол HTTPS шифрує дані на транспортному рівні, забезпечує автентифікацію сервера та клієнта, а також гарантує цілісність переданих даних. SSL (Secure Sockets Layer) та його наступник TLS (Transport Layer Security) дозволяють інкапсулювати різні протоколи, такі як HTTP, POP3, IMAP або SMTP, і передавати їх через зашифровані канали, що робить передачу інформації захищеною від перехоплення і модифікації. TLS використовує алгоритми шифрування з відкритим ключем, безпечні хеш-функції та коригувальні коди для забезпечення надійності передачі. При цьому існує декілька типів аутентифікації в веб-середовищі: Basic, Digest та Integrated. Для більшості випадків рекомендується використання SSL/TLS разом із аутентифікацією для захисту паролів та цифрових сертифікатів користувачів [6, 7].

Крім описаних протоколів, для захищеного передавання даних в ЕДО використовуються низка додаткових технологій і протоколів, включно з IPSec, PGP, L2TP та іншими, що забезпечують шифрування на мережевому

рівні, інтеграцію з міжмережевими екранами та протоколи обміну ключами (IKE – Inter Key Exchange). Ці протоколи дозволяють створювати захищені канали передачі даних між абонентами системи ЕДО та використовуються у багаторівневих моделях безпеки для забезпечення конфіденційності, цілісності та доступності електронних документів [7, 8].

Одним із ключових протоколів для захищеного передавання електронних документів у системах ЕДО є SFTP (Secure File Transfer Protocol). Його застосування у корпоративних системах дозволяє забезпечити конфіденційність, цілісність та автентичність переданих даних. На відміну від класичного FTP, який передає логіни, паролі та вміст файлів у відкритому вигляді, SFTP використовує повністю зашифрований канал SSH (Secure Shell), що робить перехоплення або модифікацію даних неможливим без доступу до криптографічних ключів. SFTP інтегрується у програмне забезпечення ЕДО як базовий компонент для передавання документів між користувачами, а також для резервного копіювання даних на віддалені сервери та архівування файлів. Система може генерувати пару криптографічних ключів для кожного користувача, забезпечуючи двосторонню аутентифікацію та шифрування всіх переданих файлів [8, 9].

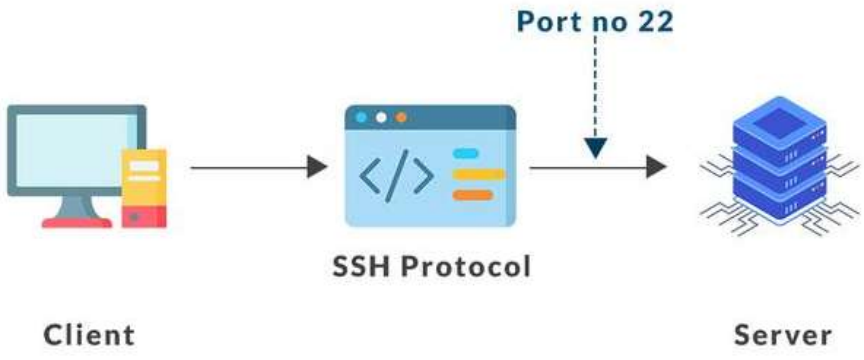

Рис. 2.3. Схема протоколу SSH

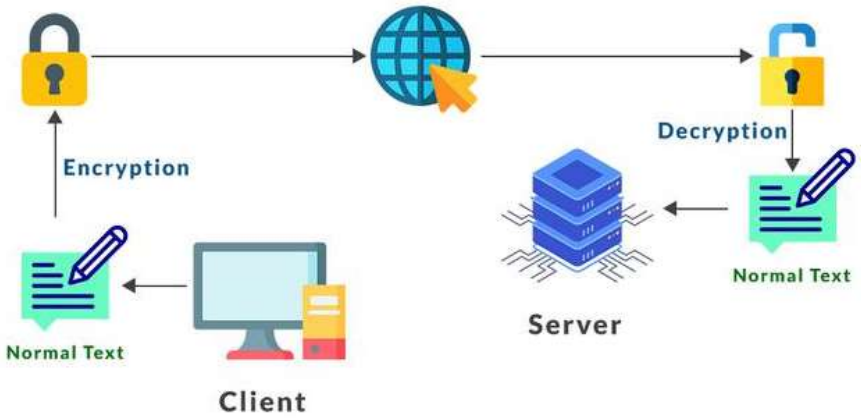

Рис. 2.4. Схема протоколу SFTP

Для забезпечення цілісності переданих даних SFTP використовує контрольні суми і хеш-функції, що дозволяє виявити будь-які зміни у вмісті документа під час його пересилки. Крім того, протокол підтримує роботу через нестабільні або публічні мережі, що робить його зручним для організацій з розподіленою структурою, де користувачі працюють у різних географічних точках. Впровадження SFTP у ПЗ ЕДО дозволяє реалізувати такі функціональні можливості, як передавання, редагування, видалення та архівування файлів у захищеному режимі, що критично для підтримки конфіденційності та довіри до системи.

Однією з альтернативних моделей передачі даних є технологія P2P (Peer-to-Peer). У таких мережах кожен вузол одночасно виступає клієнтом і сервером, обмінюючись файлами безпосередньо з іншими користувачами без централізованого сервера. P2P-системи відзначаються високою стійкістю до відмов, швидким обміном даними при великій кількості учасників та економічною ефективністю, оскільки не потребують оренди серверів. Проте у контексті захищеного зберігання й передавання інформації у ЕДО P2P потребує додаткових заходів безпеки. Для цього застосовуються шифрування каналів зв’язку, автентифікація учасників мережі та цифровий підпис електронних документів. Такий підхід дозволяє мінімізувати ризики перехоплення даних або поширення шкідливих файлів, забезпечуючи при цьому відмовостійкість та швидкість передачі.

У рамках розробки програмного забезпечення для захищеного зберігання й передавання інформації важливо інтегрувати VPN у комплексну систему безпеки. Для цього використовується апаратне або програмне забезпечення, яке реалізує функції VPN-клієнта та VPN-сервера. Апаратні VPN-шлюзи забезпечують шифрування трафіку на рівні мережі та контроль доступу, тоді як програмні клієнти дозволяють підключатися до корпоративної мережі з будь-якого пристрою. При цьому тунелювання даних у VPN реалізується через створення захищених каналів між кінцевими точками, що гарантує конфіденційність переданих документів навіть при використанні відкритих каналів Інтернету.

Протоколи захищеної передачі даних реалізують механізм безпечної оболонки для комунікацій, використовуючи пари ключів для встановлення зашифрованого каналу та забезпечення надійної передачі електронних документів у системах ЕДО. Такі протоколи виконують шифрування пакетів даних у каналах ЕДО, а також самих ЕД, що гарантує конфіденційність повідомлень, автентичність сторін та цілісність інформації.

Процес шифрування (рис. 2.5) повідомлень M передбачає використання симетричного ключа Ks, який генерується на стороні відправника (абонента A) і застосовується для шифрування даних за допомогою симетричної криптографії. Потім цей симетричний ключ Ks шифрується відкритим ключем отримувача (абонента B) із застосуванням асиметричної криптографії (наприклад, RSA). В результаті формується зашифрований ключ EB(Ks(T)) – так званий «цифровий конверт», а також зашифроване повідомлення C = Ks(M(T)), які передаються через канали інформаційної мережі абоненту B.

На стороні отримувача (абонента B) проводиться дешифрування симетричного ключа за допомогою його приватного ключа Dв: Ks = Dв(EB(Ks(T))). Після отримання симетричного ключа виконується дешифрування повідомлення DC = Ks(M(T)) із застосуванням симетричної криптографії [9].

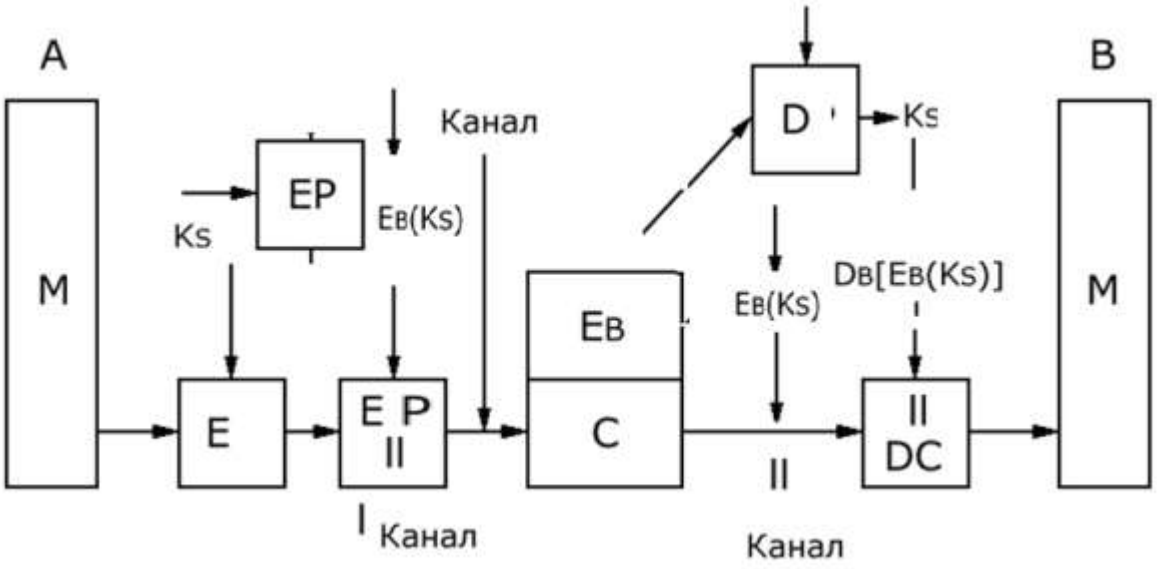

Рис. 2.5. Процес шифрування та дешифрування повідомлень за допомогою протоколів захищеної передачі в каналах ЕДО

Автентифікація повідомлень у каналах ЕДО реалізується через цифровий підпис протоколу, який відрізняється від електронного цифрового підпису для ЕД. Вона використовує криптографію з відкритим ключем та хеш-функції для підтвердження автентичності відправника та цілісності повідомлення. У разі створення ЕЦП для ЕД використовується окремий механізм із власними ключами шифрування, що діють в рамках канального протоколу передачі даних. Закритий ключ протоколу знаходиться лише у відправника, що гарантує неможливість підробки підпису сторонніми особами.

Використання надійних алгоритмів хешування, таких як SHA-1 або SHA-X, забезпечує одержувачу впевненість у цілісності повідомлення, тобто гарантує, що ніхто інший не зміг створити повідомлення з тим самим хеш-кодом. Таким чином, схема забезпечує автентичність джерела та цілісність переданих даних [7, 9].

Недоліком криптографії з відкритим ключем є її відносно низька швидкість, тому її застосовують переважно для шифрування коротких

повідомлень, симетричних ключів або хеш-кодів, тоді як великі обсяги даних шифруються симетричними алгоритмами.

2.3. Алгоритм шифрування DES

Алгоритм шифрування DES (Data Encryption Standard) є симетричним блоковим шифром, що працює з блоками даних розміром 64 біти та використовує ключ довжиною 56 біт (фактично 64 біти, але 8 з них зарезервовані для контролю парності). Шифрування ґрунтується на принципах мережі Фейстеля: дані послідовно проходять через 16 раундів криптографічних перетворень, де кожний раунд містить перестановки, підстановки та операції XOR [10].

На початку відкритий 64-бітний блок даних піддається початковій перестановці, яка переставляє біти у визначеному порядку. Далі блок розділяється на дві частини по 32 біти – ліва та права половини. У кожному раунді права частина проходить через функцію F, яка виконує розширення блоку з 32 до 48 біт, змішування з відповідним раундовим ключем і подальше перетворення через набір S-блоків. S-блоки виконують нелінійне заміщення та відіграють ключову роль у створенні криптографічної стійкості, забезпечуючи ефект лавини. Після S-блоків здійснюється ще одна перестановка, після чого отриманий результат XOR-иться з лівою половиною блоку. Наприкінці раунду половини міняються місцями, і процес повторюється для наступного раунду [7, 10].

Після завершення 16 раундів перестановки половини знову обмінюються, і виконується фінальна перестановка, обернена початковій. На виході отримується 64-бітний зашифрований блок.

Формування підключів для кожного раунду здійснюється окремим алгоритмом – ключ обробляється початковою перестановкою, розділяється на дві 28-бітні частини та циклічно зсувається. Після кожного зсуву частини

об’єднуються та проходять через скорочуючу перестановку, що дає 48-бітний раундовий ключ.

Схему роботи алгоритму DES наведено на рис. 2.6.

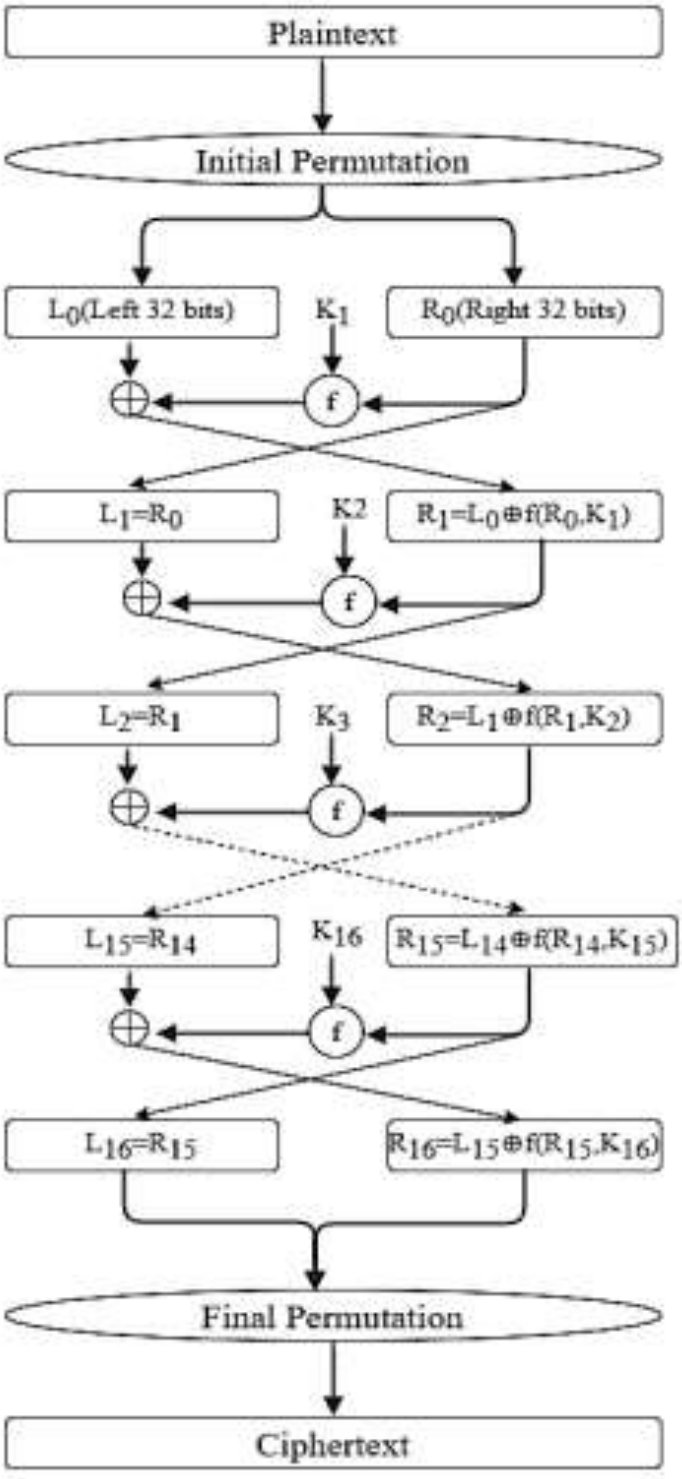

Рис. 2.6. Схема роботи алгоритму DES

Безпека DES ґрунтується на складності повного перебору ключів і на комбінованому ефекті перестановок і підстановок. Проте зі зростанням обчислювальної потужності DES визнано недостатньо стійким: ключ у 56 біт вважається занадто коротким для протидії атаці повним перебором. Це призвело до появи посиленого варіанта – Triple DES (3DES), де DES виконується тричі з різними ключами, значно підвищуючи рівень захисту. Незважаючи на застарілість, DES відіграє важливу роль в історії криптографії, ставши основою для більш сучасних алгоритмів і стандартів.

2.4. Алгоритм шифрування Triple DES

Алгоритм шифрування Triple DES (3DES) є модернізованою версією класичного DES, створеною для підвищення стійкості до криптоаналітичних атак шляхом збільшення довжини ключа та кількості раундів шифрування. Основна ідея полягає у триразовому застосуванні алгоритму DES до одного й того ж блоку даних. Розмір блока, як і в DES, становить 64 біти, проте ключова схема розширена: 3DES використовує три незалежні 56-бітні ключі, утворюючи загальну ефективну довжину ключа 168 біт. У випадку використання лише двох ключів забезпечується 112-бітний рівень криптографічної стійкості, що суттєво перевищує можливості оригінального DES [11].

Процес шифрування у Triple DES (рис. 2.7) реалізується за схемою «шифрування–дешифрування–шифрування» (E–D–E). На першому етапі вихідний блок даних шифрується за допомогою першого ключа. Отриманий результат подається на вхід другого етапу, де здійснюється операція дешифрування з використанням другого ключа. Потім отриманий проміжний блок знову шифрується третім ключем. Такий підхід дозволяє забезпечити сумісність із класичним DES: якщо всі три ключі однакові, алгоритм працює як звичайний DES, що було важливим аспектом при переході на новий

стандарт. У режимі з двома ключами перший та третій ключі збігаються, тому процес набуває форми E–D–E з двома незалежними ключами [5, 7, 11].

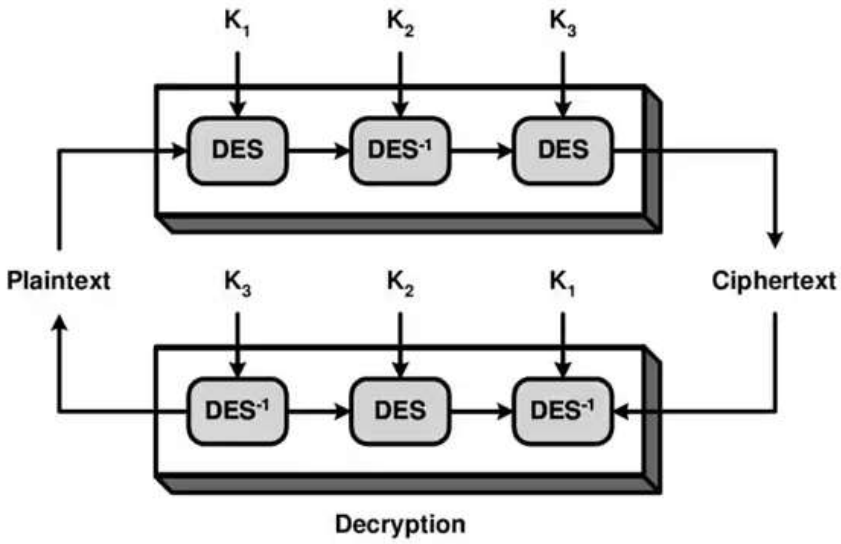

Рис. 2.7. Схема роботи алгоритму Triple DES

Функціонально 3DES успадковує структуру DES, включно з початковою та фінальною перестановками, 16 раундами мережі Фейстеля у кожному етапі та використанням S-блоків для нелінійних перетворень. Кожний етап шифрування або дешифрування використовує свій набір раундових ключів, що генеруються з відповідного ключа за допомогою стандартної процедури розширення та перестановок. Внаслідок потрійного виконання DES обчислювальні витрати збільшуються, що робить 3DES помітно повільнішим порівняно з сучасними алгоритмами. Проте саме триразове застосування DES істотно посилює криптостійкість і унеможливлює атаки, ефективні проти одиничного DES, зокрема атаку «зустріч посередині».

Алгоритм Triple DES тривалий час вважався надійним стандартом симетричного шифрування і широко застосовувався у фінансових системах, банківських протоколах, платіжних картках та телекомунікаційних мережах. Однак із розвитком обчислювальних технологій його продуктивність стало складно вважати відповідною до сучасних вимог, а довжина блока у 64 біти

почала створювати потенційні ризики колізій. У результаті 3DES поступово витісняється з критичної інфраструктури алгоритмом AES, який забезпечує вищу продуктивність, більшу гнучкість довжини ключів та ширший рівень безпеки. Тим не менш, Triple DES продовжує використовуватися у системах, що потребують сумісності зі старими стандартами або мають жорсткі вимоги до перевірених криптографічних механізмів.

2.5. Алгоритм шифрування AES

Одним із ключових механізмів забезпечення криптографічного захисту даних у сучасних системах захищеного зберігання та передавання інформації, зокрема в системах електронного документообігу, є використання алгоритму симетричного шифрування AES (Advanced Encryption Standard). Його впровадження стало результатом масштабного міжнародного конкурсу, організованого Національним інститутом стандартів і технологій США для заміни застарілого алгоритму DES, який перестав відповідати сучасним вимогам криптостійкості через недостатню довжину ключа та появу більш ефективних методів криптоаналізу. Переможцем конкурсу був визнаний криптографічний алгоритм Rijndael, розроблений бельгійськими науковцями Вінсентом Райменом та Йоаном Дайменом, який у 2000 році був стандартизований під назвою AES та став сучасним міжнародним стандартом для криптографічного захисту конфіденційної інформації [12].

Алгоритм AES є модифікованою версією Rijndael, оскільки початкова версія підтримувала три можливі розміри блоку – 128, 192 і 256 біт, тоді як офіційний стандарт закріпив використання блоку фіксованої довжини 128 біт. При цьому можливі три довжини ключа: 128, 192 і 256 біт. Така гнучкість дозволяє масштабувати рівень захисту відповідно до вимог конкретної інформаційної системи. У системах електронного документообігу

зазвичай використовуються ключі 256 біт, що зумовлено високими вимогами до безпеки корпоративних та державних даних.

Структура AES належить до класу мереж заміщення-перестановки, де кожен етап шифрування забезпечує нелінійність, дифузію та ускладнення криптоаналітичного аналізу. Шифрування складається з початкової трансформації AddRoundKey, серії раундів (10, 12 або 14 залежно від довжини ключа) та фінального перетворення. У кожному раунді виконуються послідовні операції: SubBytes, що забезпечує нелінійну заміну кожного байта за допомогою S-box, сформованого на основі математичних операцій у полі $GF(2^8)$; ShiftRows, під час якої відбувається циклічний зсув рядків матриці стану з різними зсувами, що сприяє перемішуванню байтів; MixColumns, де виконується лінійна трансформація кожного стовпця матриці з використанням операцій у скінченному полі, що забезпечує максимальну дифузію; та AddRoundKey, під час якої виконується побітове XOR між поточним станом і раундовим ключем. У заключному раунді операція MixColumns не проводиться, що оптимізує обчислення без втрати криптографічної стійкості [5, 7, 12]. Схему роботи алгоритму AES наведено на рис. 2.8.

Процес дешифрування виконується аналогічно, але із застосуванням зворотних операцій InvSubBytes, InvShiftRows та InvMixColumns. Симетричність обчислень забезпечує високу продуктивність AES як у програмних, так і в апаратних реалізаціях, що є важливим для систем з високим навантаженням, таких як корпоративні системи документообігу, сервери аутентифікації та системи захищеного файлового зберігання.

Алгоритм AES має низку переваг, що забезпечили йому статус сучасного стандарту криптографічного захисту інформації. До основних його сильних сторін належать висока швидкодія, універсальність реалізації, стійкість до відомих типів криптоаналітичних атак, зокрема диференціальної та лінійної криптоаналізи, а також значний запас криптостійкості завдяки великому простору ключів. На сьогодні не існує практичних атак, що

дозволяють зламати AES при повній реалізації алгоритму, а його ефективність підтверджена як у програмному, так і в апаратному виконанні. Завдяки цьому AES став основним механізмом шифрування в багатьох міжнародних стандартах та протоколах безпеки, включно з TLS/SSL, IPsec, SSH та протоколами захищеної передачі файлів.

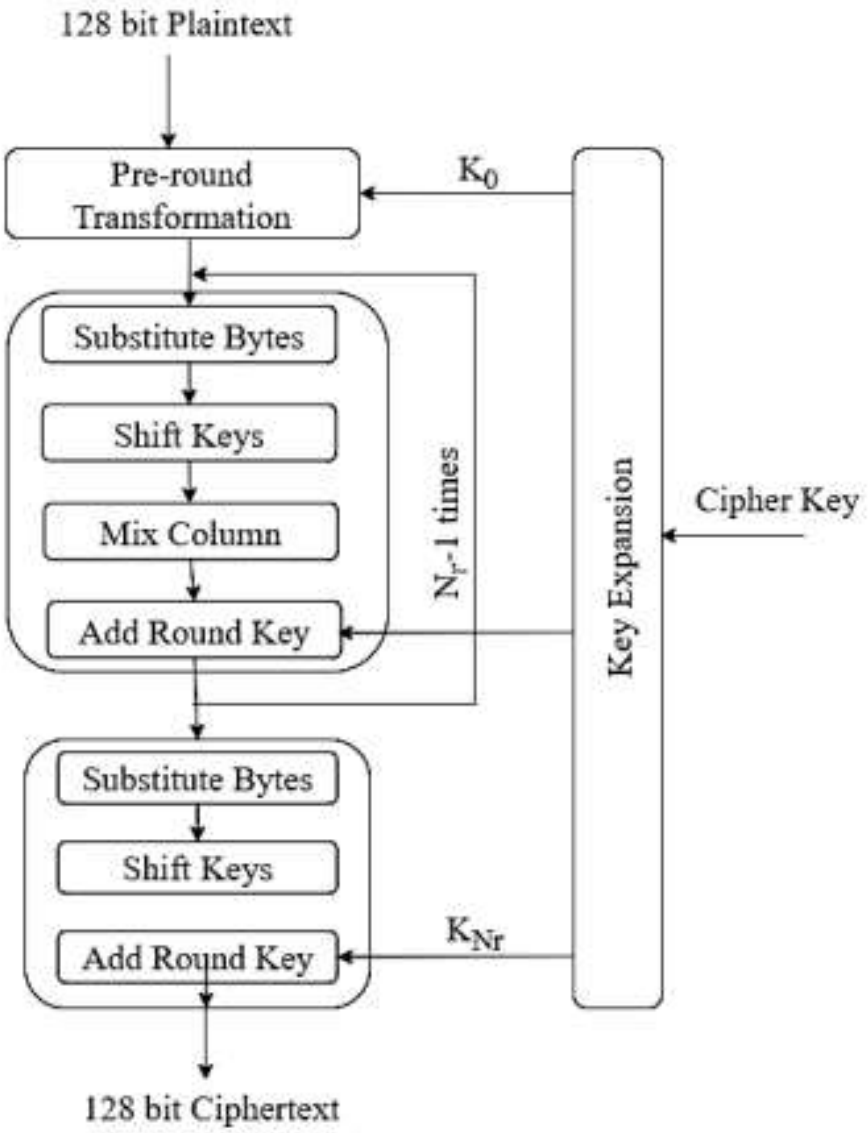

Рис. 2.8. Схема роботи алгоритму AES

2.6. Алгоритм шифрування Blowfish

Алгоритм шифрування Blowfish є симетричним блочним криптографічним механізмом, який був розроблений Брюсом Шнайєром у 1993 році як альтернатива комерційним алгоритмам, зокрема DES, що на той

час уже вважався недостатньо стійким через обмежену довжину ключа. Blowfish належить до сімейства швидких і відкритих криптографічних алгоритмів, що забезпечують високий рівень безпеки, допускають гнучкі розміри ключів та ефективно реалізуються на програмному рівні. Алгоритм працює з блоками даних розміром 64 біти, а довжина ключа може змінюватися в межах від 32 до 448 біт, що робить Blowfish придатним для широкого спектра криптографічних задач [13].

Структурно Blowfish побудований на основі мережі Фейстеля та містить 16 раундів криптографічних перетворень. У кожному раунді виконується поділ блока на дві половини, після чого одна з них пропускається через нелінійну функцію, яка включає підстановки та арифметичні операції, після чого результат XOR-ується з іншою половиною. На кожному кроці відбувається обмін частинами блока, а після завершення раундів здійснюється фінальне переставляння. Основними криптографічними компонентами Blowfish є P-масив (P-array), який складається із 18 32-бітних підключових значень, та чотири S-блоки, кожен з яких містить 256 32-бітних значень. Саме S-блоки забезпечують необхідну нелінійність та складність перетворень у Blowfish, а механізм генерування підключів робить алгоритм стійким до атак з відкритим текстом та вибраним відкритим текстом. Схему роботи алгоритму Blowfish наведено на рис. 2.9.

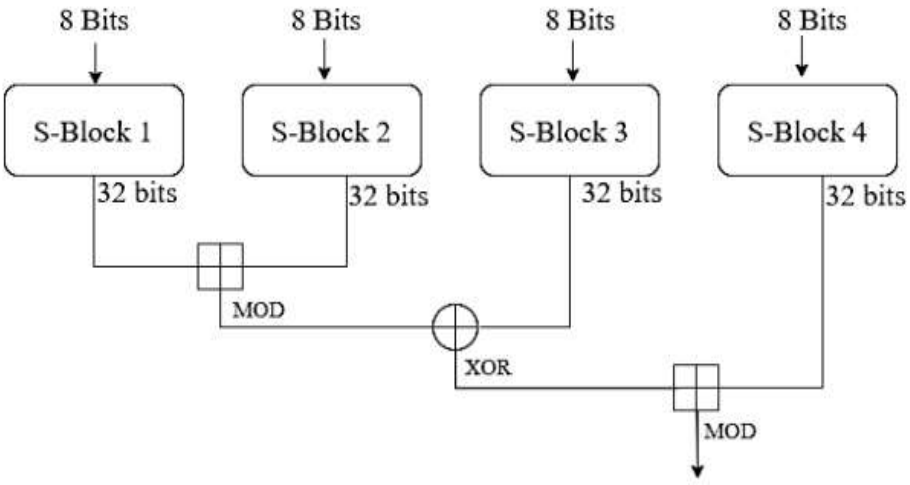

Рис. 2.9. Схема роботи алгоритму Blowfish

Особливістю Blowfish є складна процедура створення ключового розкладу, під час якої вихідні ключові дані послідовно змішуються з константами та застосовуються до P-масиву та S-блоків. Початкові значення таблиць узяті з числа π, що забезпечує їх випадкову природу. Кожен елемент таблиць модифікується шляхом шифрування нульового блока, після чого вихідні значення послідовно замінюються на отримані результати. Цей процес є обчислювально затратним, проте він виконується лише один раз перед використанням ключа, що робить Blowfish швидким і ефективним у процесі шифрування великих обсягів даних [9, 13].

Blowfish відомий своєю криптостійкістю – станом на сьогодні не існує практичних атак, які б повністю зламали алгоритм при правильній реалізації та достатній довжині ключа. Разом із тим, через 64-бітний розмір блока алгоритм у певних сценаріях може піддаватися ризикам, пов’язаним із повторенням блоків при шифруванні великих масивів даних, що стало однією з причин появи його наступника – алгоритму Twofish, також розробленого Шнайєром. Попри це Blowfish досі широко використовується у системах, де важливими є відкритість, відсутність патентних обмежень та висока швидкодія, наприклад у криптографічних бібліотеках, захисті паролів та мережевих протоколах.

Таким чином, Blowfish є важливим представником класичних блокових шифрів, який став одним із перших відкритих алгоритмів, здатних забезпечити високу криптостійкість та продуктивність на програмних платформах, ставши основою для подальшого розвитку симетричної криптографії.

2.8. Алгоритм шифрування Twofish

Алгоритм шифрування Twofish є симетричним блочним криптографічним алгоритмом, розробленим Брюсом Шнайєром та його командою як наступник Blowfish, із метою забезпечити більшу гнучкість та

стійкість до сучасних криптоаналітичних атак. Twofish працює з блоками даних розміром 128 біт і підтримує ключі довжиною 128, 192 або 256 біт. На відміну від Blowfish, алгоритм розроблено із врахуванням вимог до високої швидкості, ефективності на програмному та апаратному рівні, а також з можливістю стійкої інтеграції у сучасні протоколи захищеної передачі даних.

Структура Twofish побудована на принципах мережі Фейстеля, але з модифікацією, яка включає використання гнучкої матриці PHT (Pseudo-Hadamard Transform) для додаткового перемішування даних і забезпечення високої дифузії. Алгоритм складається з 16 раундів, у кожних з яких виконуються операції підстановки та перестановки, а також XOR з ключовими значеннями, що генеруються з основного ключа. Twofish застосовує складну схему ключового розкладу, де ключі розділяються на підключі, які впливають на кожен раунд шифрування, та використовуються для модифікації S-блоків, що підвищує криптографічну стійкість [14].

Криптографічні функції Twofish включають нелінійні перетворення через S-блоки, пермутації, а також побудовану на алгебраїчних операціях PHT для кожного 32-бітного слова, що забезпечує рівномірний розподіл бітів вихідного блоку. Під час шифрування блок даних розділяється на чотири 32-бітні слова, які обробляються паралельно у межах кожного раунду. Завдяки цьому алгоритм є ефективним при апаратних реалізаціях і підтримує високу швидкість шифрування великих обсягів даних [5, 14]. Схему роботи алгоритму Twofish наведено на рис. 2.10.

Однією з особливостей Twofish є його стійкість до атак на основі диференційного та лінійного криптоаналізу завдяки використанню комплексної структури S-блоків і високому рівню дифузії. Крім того, алгоритм підтримує ключі великої довжини, що ускладнює проведення атак методом повного перебору. Twofish також розроблений з урахуванням вимог до апаратної оптимізації, що робить його придатним для вбудованих систем, захисту мережевих протоколів і корпоративних систем з високими вимогами до безпеки [7, 14].

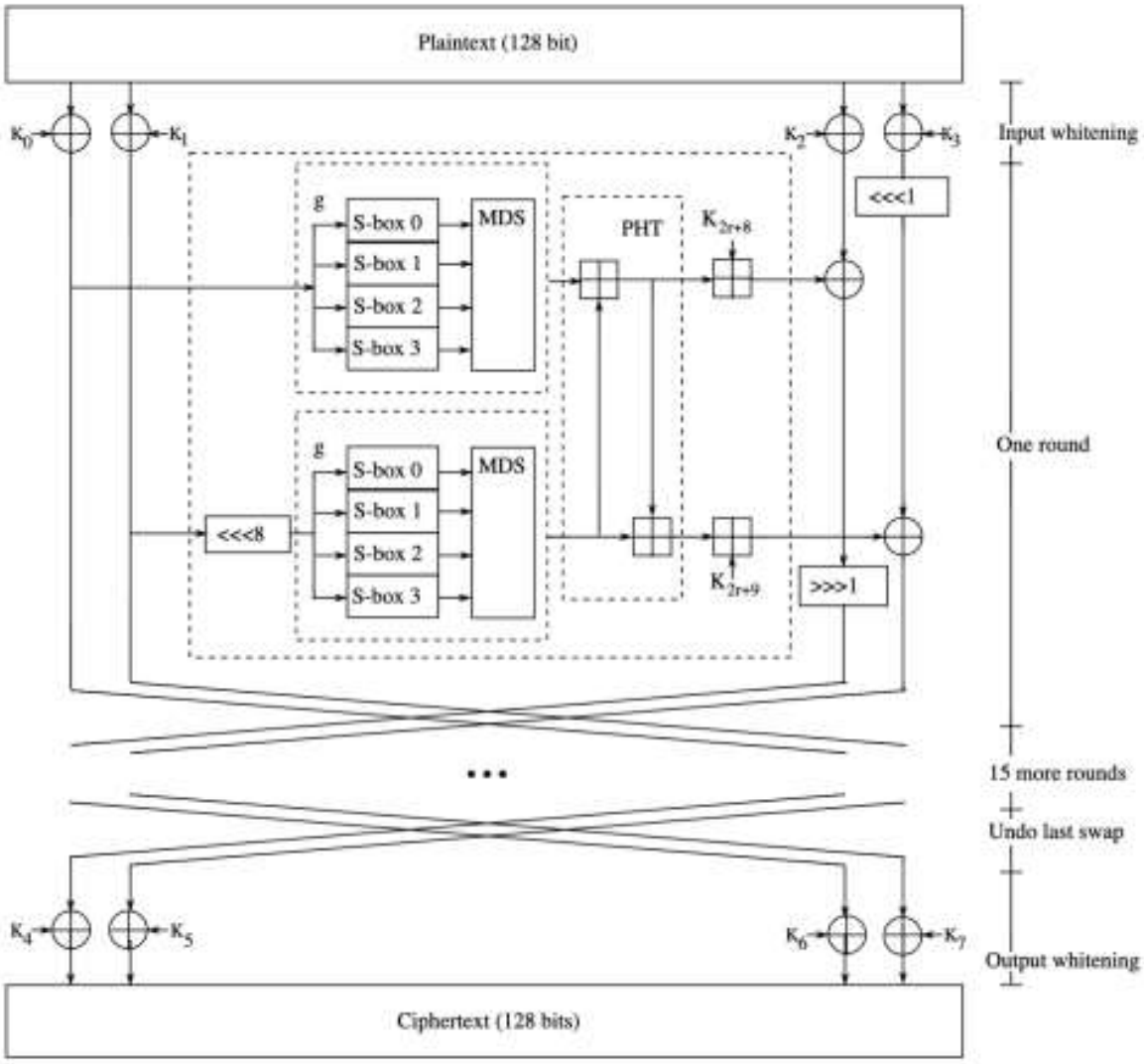

Рис. 2.10. Схема роботи алгоритму Twofish

Алгоритм Twofish знайшов широке застосування у програмних бібліотеках та системах з відкритим кодом, включаючи шифрування файлів, побудову захищених каналів передачі даних та системи зберігання конфіденційної інформації. Його особливості дозволяють комбінувати Twofish з іншими криптографічними механізмами, такими як AES або RSA, для створення багаторівневих систем захисту даних у корпоративних та урядових мережах.

Таким чином, Twofish представляє собою сучасний симетричний блочний шифр, який поєднує високу швидкість, гнучкість використання ключів та надійний захист від криптоаналітичних атак, роблячи його

ефективним рішенням для реалізації систем захищеного зберігання й передачі інформації.

2.8. Алгоритм шифрування RSA

Алгоритм RSA є одним із найвідоміших і найпоширеніших асиметричних криптографічних алгоритмів, який використовується для забезпечення конфіденційності, цілісності та автентичності даних. RSA був розроблений у 1977 році Роном Рівестом, Аді Шаміром та Леонардом Адлеманом і базується на складності факторизації великих простих чисел, що забезпечує його стійкість до криптоаналітичних атак [15].

Принцип роботи алгоритму полягає на використанні пари ключів: відкритого ключа для шифрування та закритого ключа для дешифрування. Генерація ключів починається з вибору двох великих простих чисел p та q, після чого обчислюється їх добуток $n=p\cdot q$, який слугує модулем для обох ключів. Далі обчислюється функція Ейлера $\phi(n)=(p-1)(q-1)$, на основі якої вибирається відкритий ключ e, що є взаємно простим з $\phi(n)$, тобто $\gcd(e,\phi(n))=1$. Закритий ключ d обчислюється як мультиплікативний обернений елемент до e по модулю $\phi(n)$, тобто $d\cdot e\equiv 1 \pmod{\phi(n)}$.

Шифрування повідомлення M здійснюється шляхом піднесення його до степеня e та взяття залишку від ділення на n, що можна записати формулою $C=M^e \bmod n$, де C – зашифроване повідомлення. Дешифрування відбувається за допомогою закритого ключа d аналогічним чином: $M=C^d \bmod n$. Таким чином, лише власник закритого ключа може відновити оригінальне повідомлення, навіть якщо шифротекст перехоплено сторонньою особою [5, 7, 9, 15].

Однією з ключових особливостей RSA є можливість цифрового підпису. Для цього повідомлення хешується за допомогою стійкої хеш-функції, а отриманий хеш підписується закритим ключем відправника.

Одержувач, використовуючи відкритий ключ підписанта, може перевірити справжність підпису та цілісність повідомлення. Це дозволяє реалізувати автентифікацію та захист від підробки даних у системах електронного документообігу.

Сильні сторони RSA полягають у його широкому визнанні та сумісності з багатьма протоколами, такими як SSL/TLS, PGP та S/MIME, а також у можливості поєднувати його із симетричними алгоритмами, наприклад AES, для забезпечення ефективного шифрування великих обсягів даних. Основним обмеженням є порівняно низька швидкість обробки великих повідомлень, тому на практиці RSA застосовується переважно для шифрування симетричних ключів або підписування, а безпосереднє шифрування великих файлів здійснюється швидшими симетричними алгоритмами [15].

Важливим аспектом безпеки RSA є правильне управління ключами та вибір достатньо великих простих чисел, що робить алгоритм стійким до атак на основі факторизації. Застосування RSA у системах електронного документообігу дозволяє створювати захищені канали передачі даних, забезпечувати конфіденційність, підтверджувати авторство документів та гарантувати їх цілісність, що робить його критично важливим елементом сучасних систем безпечного зберігання та передавання інформації.

2.9. Висновки до розділу 2

У другому розділі досліджено сучасні методи та засоби інформаційного захисту, що застосовуються в системах електронного документообігу для забезпечення конфіденційності, цілісності та доступності даних. Було розглянуто різноманітні способи захищеного зберігання та передавання інформації, включно з використанням протоколів шифрування, цифрових підписів та механізмів контролю доступу.

Особлива увага приділялася криптографічним алгоритмам, що забезпечують надійний захист даних: DES, Triple DES, AES, Blowfish, Twofish та RSA. Кожен із розглянутих алгоритмів характеризується певними перевагами та обмеженнями, зокрема щодо швидкості обробки даних, рівня криптографічного захисту та можливостей використання у паралельних обчислювальних середовищах. Аналіз показав, що симетричні алгоритми (DES, 3DES, AES, Blowfish, Twofish) ефективні для швидкого шифрування великих обсягів даних, тоді як асиметричний алгоритм RSA доцільно застосовувати для захищеної передачі ключів та автентифікації.

Отримані результати свідчать про необхідність комбінованого застосування різних алгоритмів шифрування та захисних механізмів для досягнення високого рівня безпеки інформаційних систем. Це створює основу для розробки ефективних паралельних алгоритмів шифрування та подальшого експериментального дослідження продуктивності криптографічних систем у наступному розділі.

РОЗДІЛ 3
РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СИСТЕМИ ЗАХИЩЕНОГО ЗБЕРІГАННЯ Й ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

Розробка програмного забезпечення для системи захищеного зберігання й передавання інформації передбачає створення ефективного механізму криптографічної обробки даних, здатного забезпечити високу продуктивність і стійкість до зовнішніх атак. В умовах постійного зростання обсягів електронних документів у сучасних системах електронного документообігу критично важливим стає не лише рівень захисту, але й швидкість виконання криптографічних операцій, оскільки системи ЕДО працюють у режимах реального або наближеного до реального часу. Традиційні реалізації алгоритмів шифрування, які виконуються послідовно, часто демонструють недостатню швидкодію при обробці великих обсягів даних або одночасній роботі численних користувачів. Саме тому виникає потреба у застосуванні паралельних обчислювальних методів для підвищення ефективності криптографічних процесів.

3.1. Вибір мови програмування та засобів паралельного програмування

Для реалізації системи захищеного зберігання та передавання інформації, орієнтованої на паралельне виконання алгоритмів шифрування, ключовим етапом є вибір мови програмування та інструментів паралельної обробки даних. Враховуючи вимоги до продуктивності, ефективного використання апаратних ресурсів і можливості гнучкої оптимізації криптографічних процедур, було обрано мову програмування C++ у поєднанні з бібліотекою Parallel Patterns Library (PPL).

C++ є мовою системного програмування з високим рівнем контролю

над пам’яттю, потоками та апаратними ресурсами, що дозволяє отримувати максимальну продуктивність при реалізації складних криптографічних алгоритмів. На відміну від інтерпретованих мов, таких як Python чи JavaScript, C++ забезпечує компіляцію у машинний код, що мінімізує затримки виконання та гарантує високу швидкість обробки великих обсягів даних, характерних для систем електронного документообігу та захищених каналів передачі. Також C++ підтримує багатопарадигмальний підхід – об’єктно-орієнтоване, процедурне та шаблонне програмування, що дозволяє створювати модульні та масштабовані програмні системи з чітким розмежуванням функцій та відповідальностей [17].

Для забезпечення паралельного виконання криптографічних операцій обрана бібліотека PPL. Вона є високорівневим засобом організації багатопотоковості та забезпечує автоматичний розподіл обчислювальних задач між доступними ядрами процесора. PPL надає зручні механізми для реалізації паралельних циклів, обробки масивів даних, а також запуску задач у асинхронному режимі, зокрема через конструкції parallel_for, parallel_invoke і task_group. Цей підхід дозволяє застосовувати концепцію задачної паралелізації, де обчислення розбиваються на незалежні блоки та виконуються одночасно. Порівняно з ручним керуванням потоками, що потребує значних зусиль і може призвести до синхронізаційних помилок, використання PPL суттєво спрощує розробку і підвищує надійність реалізації [17].

Поєднання C++ і PPL забезпечує оптимальні умови для реалізації паралельної криптографічної системи, яка здатна обробляти великі файли та високі потоки даних. Такий вибір інструментів дозволяє не лише підвищити швидкість шифрування та дешифрування, але й забезпечити масштабованість рішення під сучасні багатоядерні архітектури [17].

3.2. Розробка паралельних алгоритмів шифрування

Проєктування паралельних криптографічних алгоритмів ґрунтується на ідеї поділу вхідних даних на незалежні фрагменти, що можуть оброблятися одночасно різними обчислювальними потоками. Сучасні шифрувальні методи засновані на інтенсивних математичних трансформаціях, які повторюються для кожного блоку інформації. Саме тому підхід із паралельною обробкою блоків даних є надзвичайно ефективним і логічним шляхом оптимізації криптографічних операцій. Концепція єдиної програми, що працює над множиною даних (SPMD), найкраще відповідає особливостям симетричних і асиметричних алгоритмів, що передбачають обробку численних незалежних фрагментів інформації [18].

Розробка будь-якої паралельної криптографічної системи проходить кілька важливих етапів. Перший крок полягає у вивченні оригінальної (послідовної) версії алгоритму та виявленні частин, які можна виконувати одночасно без порушення коректності результатів. Далі формується паралельна структура програми та створюється прототип – початкова версія системи, що дає змогу перевірити обрану стратегію розпаралелення на практиці. Прототипування дозволяє швидко перевірити життєздатність ідей та оцінити їхню ефективність із мінімальними витратами на розробку. На цьому етапі особливо важливо визначити потенційні синхронізаційні конфлікти, колізії доступу до спільних даних та можливі «вузькі місця», що можуть сповільнити виконання [18, 19].

Після створення прототипу наступним етапом є налагодження, спрямоване на виявлення та усунення помилок, які виникають через паралельний доступ до ресурсів. Важливим завданням є оптимізація архітектури програми для мінімізації блокувань, зменшення накладних витрат на перемикання потоків і забезпечення ефективного масштабування. Коректно організована паралельна обробка передбачає правильне планування потоків, використання локальних змінних у кожному потоці,

мінімізацію спільного доступу до пам’яті та уникнення жорстких фіксованих послідовностей виконання там, де це можливо.

Процес побудови паралельних криптографічних алгоритмів базується на кількох ключових принципах: визначення незалежних частин обчислень; вибір правильної стратегії розподілу задач – зверху вниз або знизу вгору; врахування майбутнього розширення кількості обчислювальних ядер; застосування потокобезпечних бібліотек та механізмів синхронізації; використання високорівневих засобів паралельності там, де це можливо. У разі необхідності допускається модифікація алгоритму – навіть якщо це ускладнює його структуру – за умови отримання виграшу в продуктивності та синхронізації.

Особливе значення має можливість розподілу криптографічних операцій на два рівні паралелізації. Перший рівень – внутрішній, коли обробка блоків даних виконується паралельно у багатопотоковому середовищі одного комп’ютера або процесора. Цей підхід добре працює для алгоритмів, що оперують фіксованими блоками інформації, – таких як AES, DES, Triple DES, Blowfish та Twofish. Другий рівень – міжвузловий, коли великі обсяги даних поділяються між декількома обчислювальними вузлами, що дає змогу реалізувати шифрування у кластерних системах або хмарних середовищах. Такий підхід особливо корисний у випадках, коли потрібно обробити великі документообіги або значні масиви інформації, характерні для систем електронного документообігу [3, 18, 19].

Асиметричні алгоритми, такі як RSA, також можуть бути адаптовані до паралельної обробки шляхом поділу вхідного повідомлення на сегменти однакового розміру, які шифруються або дешифруються незалежно. При такій організації кожен потік виконує одну й ту саму математичну операцію над свою частиною даних, що суттєво скорочує час обробки довгих повідомлень. Для реалізації багаторівневого паралелізму можуть застосовуватися спеціалізовані засоби, зокрема багатоядерні CPU, GPU або обчислювальні кластери.

У межах даного дослідження була розроблена паралельна система шифрування даних, орієнтована на використання багатоядерних архітектур сучасних процесорів. Для забезпечення високої продуктивності застосовано механізм розпаралелювання криптографічних операцій, що дозволяє розподіляти процеси шифрування та дешифрування між кількома ядрами процесора. Такий підхід зменшує загальний час обробки файлів, забезпечує масштабованість обчислень і дозволяє ефективно використовувати апаратні ресурси. У реалізації програмної системи використано стандартні криптографічні API-бібліотеки для виконання шифрування та дешифрування, а також бібліотеку паралельного програмування Parallel Programming Library, яка надає засоби для зручного створення паралельних потоків та управління ними. Підхід із використанням паралельних обчислень дозволяє виконувати шифрування кількох блоків інформації або кількох файлів одночасно, що особливо ефективно для блочних шифрів.

Для дослідження ефективності запропонованої моделі було проведено експеримент, у рамках якого генерувалися файли фіксованих розмірів. Це дало можливість об’єктивно оцінити час виконання криптографічних операцій та масштабованість системи при обробці різних обсягів даних. Була реалізована й протестована паралельна версія декількох найпоширеніших алгоритмів шифрування, серед яких DES, Triple DES, AES, Blowfish та Twofish. Їх обрано через поширене застосування в системах електронного документообігу, різну криптографічну структуру та відмінності у швидкодії й рівні стійкості. Впровадження паралельного виконання дозволило значно скоротити час обробки даних у порівнянні з традиційними послідовними методами шифрування.

Для об'єктивної оцінки ефективності алгоритмів було створено програмне забезпечення, яке дозволяє користувачу завантажувати файли та здійснювати запуск послідовних і паралельних реалізацій методів шифрування. Для тестування використовувались заздалегідь сформовані файли розміром 5 МБ, 10 МБ, 100 МБ та 1000 МБ, що дозволило провести

порівняння швидкодії алгоритмів на різних обсягах даних. Експерименти виконувалися на комп'ютері з операційною системою Windows 10 та 16 ГБ оперативної пам’яті. Для підвищення точності дослідження було обрано кілька процесорних платформ: двоядерний Intel Core i5-6500U (2.50 ГГц), чотириядерний Intel Core i7-6700HQ (2.60 ГГц) та шестиядерний Intel Core i7-6700Q (3.20 ГГц). Кожен тест проводився тричі, після чого обчислювалася медіана отриманих значень, що дозволило мінімізувати вплив випадкових процесів і фонових навантажень на результати. Таким чином, було забезпечено коректне порівняння продуктивності криптографічних алгоритмів та достовірність отриманих висновків.

3.3. Оцінювання продуктивності та ефективності паралельної криптографічної системи

Важливим етапом розробки програмного забезпечення для систем захищеного зберігання і передавання інформації є оцінювання його продуктивності. Аналіз швидкодії дозволяє не лише встановити реальні характеристики реалізованих алгоритмів, але й визначити проблемні місця у їхній структурі, оптимізувати паралельне виконання та покращити загальну ефективність. Вимірювання продуктивності дає змогу оцінити рівень масштабованості, тобто здатність системи зберігати або покращувати продуктивність при зростанні кількості задіяних обчислювальних ресурсів.

Для аналізу паралельної реалізації криптографічних алгоритмів використовуються два класичних індикатори: прискорення (speedup) та ефективність (efficiency). Вони дозволяють об’єктивно порівнювати роботу послідовної та паралельної версій алгоритмів і оцінювати вплив кількості потоків обробки на результат [19, 20].

Прискорення (Speedup) характеризує, наскільки швидше виконується паралельна версія алгоритму порівняно з його послідовною реалізацією. Воно визначається відношенням часу виконання послідовного алгоритму T_s

до часу виконання паралельної версії T_p:

$$S = \frac{T_s}{T_p},$$

де S – коефіцієнт прискорення [19, 20].

Ефективність паралельного виконання (Efficiency) показує, наскільки раціонально використовуються доступні обчислювальні ресурси при паралельному запуску програми. Вона визначається як відношення коефіцієнта прискорення S до кількості задіяних процесорних потоків або ядер P:

$$E = \frac{S}{P},$$

де E – ефективність використання ресурсів. Значення E близьке до 1 свідчить про високий рівень продуктивності системи та майже ідеальне масштабування. Якщо ефективність знижується зі збільшенням кількості потоків, це може вказувати на суттєві накладні витрати, пов’язані з синхронізацією, комунікацією між потоками або надмірним контекстним перемиканням. В окремих випадках збільшення кількості потоків понад оптимальне значення може навіть призводити до погіршення загальної продуктивності, що зумовлено обмеженнями архітектури процесора та гіперчутливістю алгоритмів до паралельного перевантаження [19].

Метрики прискорення та ефективності дозволяють обґрунтовано оцінити можливість застосування паралельного підходу для криптографічних алгоритмів, визначити оптимальну конфігурацію обчислювального середовища та вибрати найбільш продуктивні методики організації потоків. На основі цих показників можна зробити висновки щодо рівня масштабованості, продуктивності та відповідності паралельної реалізації криптографічних процедур вимогам систем електронного документообігу, які потребують високої швидкості обробки даних та гарантованої надійності під час шифрування та дешифрування інформації.

3.4. Аналіз продуктивності та обговорення результатів експериментального дослідження

У межах дослідження було реалізовано дві версії програмного забезпечення для системи захищеного зберігання та передавання даних – послідовну та паралельну, використовуючи мову програмування C++ та бібліотеку PPL, що забезпечує багатопотокове виконання на багатоядерних процесорах. Робота програми починалася із завантаження вихідного файлу, після чого обирався криптографічний алгоритм та ключ шифрування, а на завершальному етапі фіксувався час виконання шифрування та дешифрування для різних конфігурацій.

Для кожного з алгоритмів були зафіксовані значення часу виконання як у класичному, так і у паралельному режимі. Оцінювання здійснювалося для кількох розмірів файлів, що дозволило отримати порівняльні характеристики та виявити вплив масштабування даних на швидкодію. Спочатку було проаналізовано роботу послідовної реалізації, після чого проводилось тестування паралельної версії з різною кількістю задіяних ядер процесора. Таким чином, дослідження дало можливість оцінити ефективність розпаралелювання криптографічних операцій.

Зведені результати експериментів для алгоритмів DES, Triple DES, AES, Blowfish, Twofish, подано у таблицях 3.1-3.3.

Аналіз результатів дослідження продуктивності алгоритмів шифрування демонструє чітку перевагу паралельної обробки над послідовною. Для алгоритму DES на рис. 3.1 подано порівняння часу виконання для різних розмірів файлів та кількості задіяних процесорних ядер. Із графіка видно, що паралельна реалізація забезпечує значно менший час обробки даних. Динаміка приросту швидкодії для цього алгоритму представлена на рис. 3.2, а рівень ефективності використання ресурсів багатоядерної системи – на рис. 3.3.

Таблиця 3.1.

Часові показники виконання послідовної та паралельної реалізації алгоритмів шифрування

Алгоритм		5MB	10 MB	100 MB	1000 MB
DES	Послідовний алгоритм	112 мс	224 мс	2251 мс	22428 мс
	2 процеси	92 мс	192 мс	1872 мс	18463 мс
	4 процеси	78 мс	89 мс	846 мс	8600 мс
	6 процесів	56 мс	64 мс	557 мс	5592 мс
Triple DES	Послідовний алгоритм	298 мс	582 мс	5657 мс	56987 мс
	2 процеси	110 мс	229 мс	2148 мс	20585 мс
	4 процеси	116 мс	209 мс	1910 мс	19001 мс
	6 процесів	66 мс	139 мс	1099 мс	11085 мс
AES	Послідовний алгоритм	77 мс	148 мс	1332 мс	13597 мс
	2 процеси	71 мс	142 мс	1445 мс	14703 мс
	4 процеси	35 мс	63 мс	617 мс	6543 мс
	6 процесів	25 мс	47 мс	405 мс	5304 мс
Blowfish	Послідовний алгоритм	73 мс	148 мс	1456 мс	14352 мс
	2 процеси	128 мс	248 мс	2498 мс	24201 мс
	4 процеси	47 мс	74 мс	695 мс	6935 мс
	6 процесів	50 мс	98 мс	898 мс	9623 мс
Twofish	Послідовний алгоритм	70 мс	131 мс	1292 мс	13215 мс
	2 процеси	349 мс	721 мс	7759 мс	78550 мс
	4 процеси	59 мс	112 мс	1087 мс	11051 мс
	6 процесів	73 мс	174 мс	1399 мс	16137 мс

Таблиця 3.2.

Показники прискорення для послідовної та паралельної реалізації алгоритмів шифрування

Алгоритм		5MB	10 MB	100 MB	1000 MB
DES	Послідовний алгоритм	1,00	1,00	1,00	1,00
	2 процеси	1,22	1,17	1,20	1,21
	4 процеси	1,44	2,52	2,66	2,61
	6 процесів	2,00	3,50	4,04	4,01
Triple DES	Послідовний алгоритм	1,00	1,00	1,00	1,00
	2 процеси	2,71	2,54	2,63	2,77
	4 процеси	2,57	2,78	2,96	3,00
	6 процесів	4,52	4,19	5,15	5,14
AES	Послідовний алгоритм	1,00	1,00	1,00	1,00
	2 процеси	1,08	1,04	0,92	0,92
	4 процеси	2,20	2,35	2,16	2,08
	6 процесів	3,08	3,15	3,29	2,56
Blowfish	Послідовний алгоритм	1,00	1,00	1,00	1,00
	2 процеси	0,57	0,60	0,58	0,59
	4 процеси	1,55	2,00	2,09	2,07
	6 процесів	1,46	1,51	1,62	1,49
Twofish	Послідовний алгоритм	1,00	1,00	1,00	1,00
	2 процеси	0,20	0,18	0,17	0,17
	4 процеси	1,19	1,17	1,19	1,20
	6 процесів	0,96	0,75	0,92	0,82

Таблиця 3.2.

Показники ефективності для послідовної та паралельної реалізації алгоритмів шифрування

Алгоритм		5MB	10 MB	100 MB	1000 MB
DES	Послідовний алгоритм	1,00	1,00	1,00	1,00
	2 процеси	0,61	0,58	0,60	0,61
	4 процеси	0,36	0,63	0,67	0,65
	6 процесів	0,33	0,58	0,67	0,67
Triple DES	Послідовний алгоритм	1,00	1,00	1,00	1,00
	2 процеси	1,35	1,27	1,32	1,38
	4 процеси	0,64	0,70	0,74	0,75
	6 процесів	0,75	0,70	0,86	0,86
AES	Послідовний алгоритм	1,00	1,00	1,00	1,00
	2 процеси	0,54	0,52	0,46	0,46
	4 процеси	0,55	0,59	0,54	0,52
	6 процесів	0,51	0,52	0,55	0,43
Blowfish	Послідовний алгоритм	1,00	1,00	1,00	1,00
	2 процеси	0,29	0,30	0,29	0,30
	4 процеси	0,39	0,50	0,52	0,52
	6 процесів	0,24	0,25	0,27	0,25
Twofish	Послідовний алгоритм	1,00	1,00	1,00	1,00
	2 процеси	0,10	0,09	0,08	0,08
	4 процеси	0,30	0,29	0,30	0,30
	6 процесів	0,16	0,13	0,15	0,14

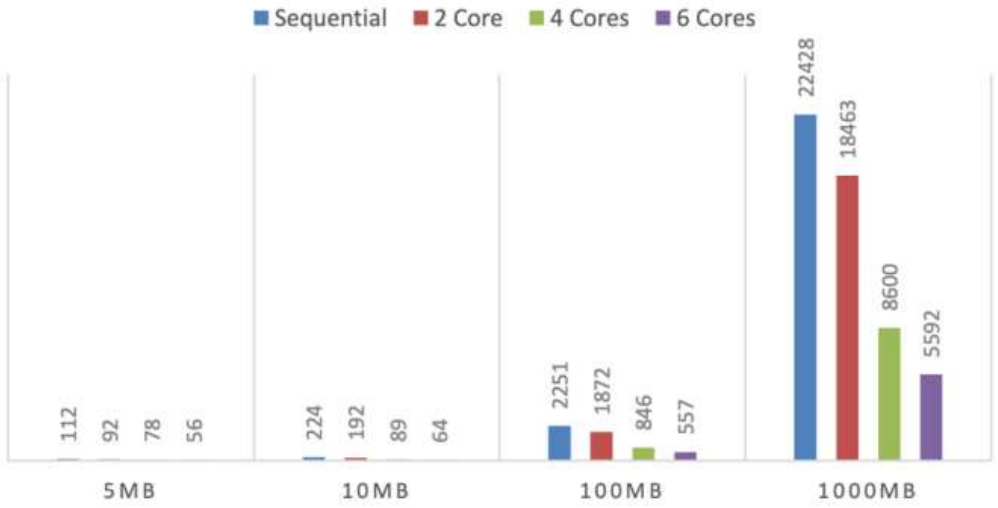

Рис. 3.1. Часові показники виконання алгоритму шифрування DES

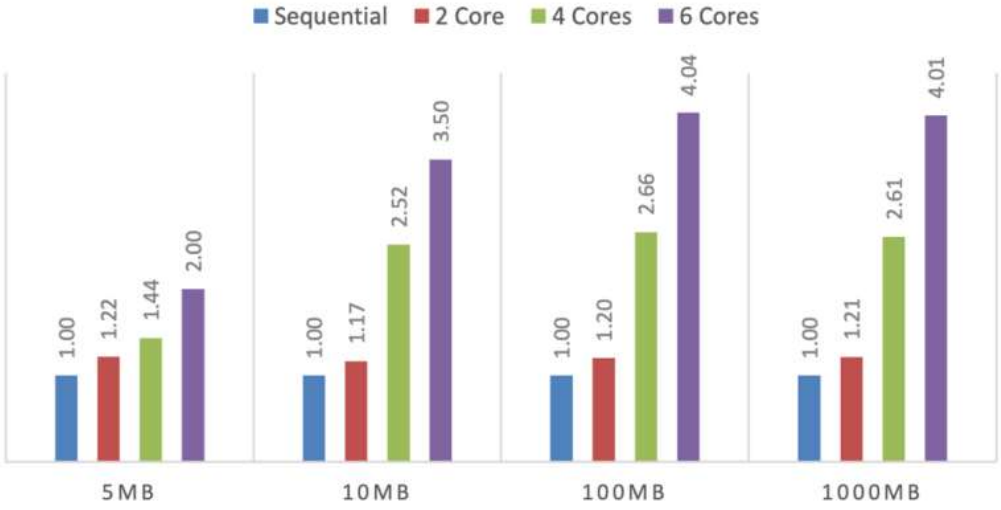

Рис. 3.2. Показники прискорення для алгоритму шифрування DES

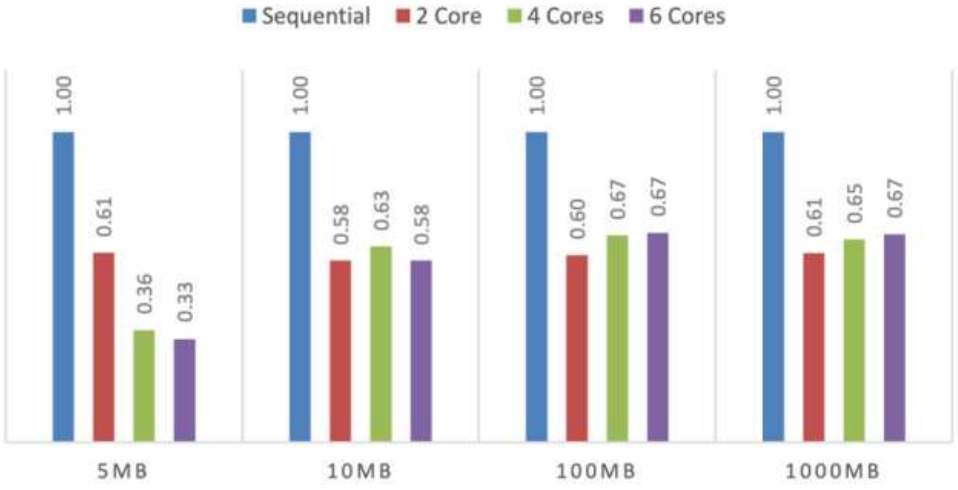

Рис. 3.3. Показники ефективності для алгоритму шифрування DES

Аналогічний підхід застосовано для аналізу алгоритму 3DES. З графічного матеріалу на рис. 3.4 видно, що збільшення кількості ядер також сприяє скороченню часу шифрування. Отримані значення прискорення та продуктивності наведено відповідно на рис. 3.5 та 3.6, де прослідковується позитивний вплив паралелізації, хоча ефект менш виражений у порівнянні з DES через більш ресурсоємну природу алгоритму.

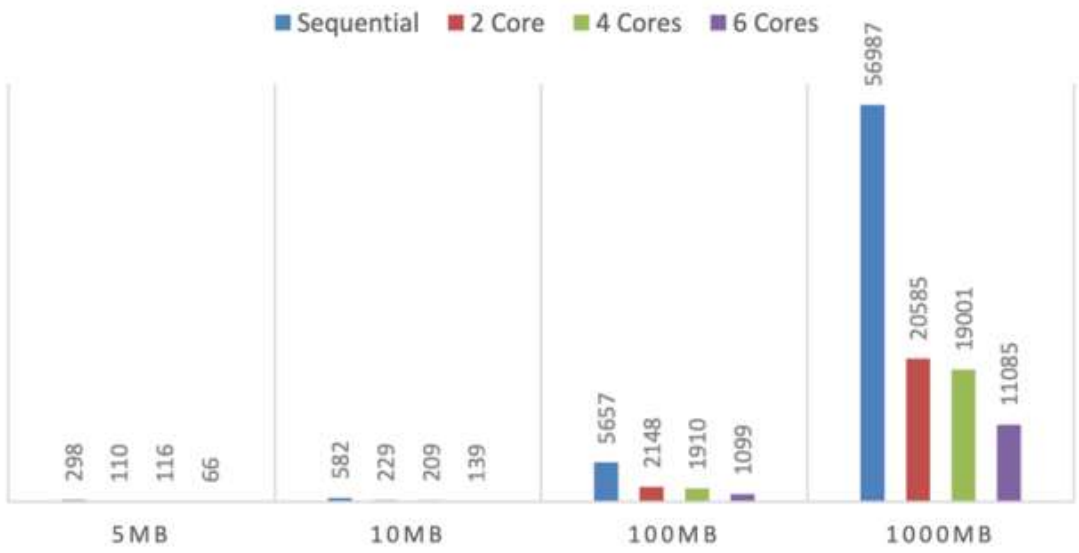

Рис. 3.4. Часові показники виконання алгоритму шифрування 3DES

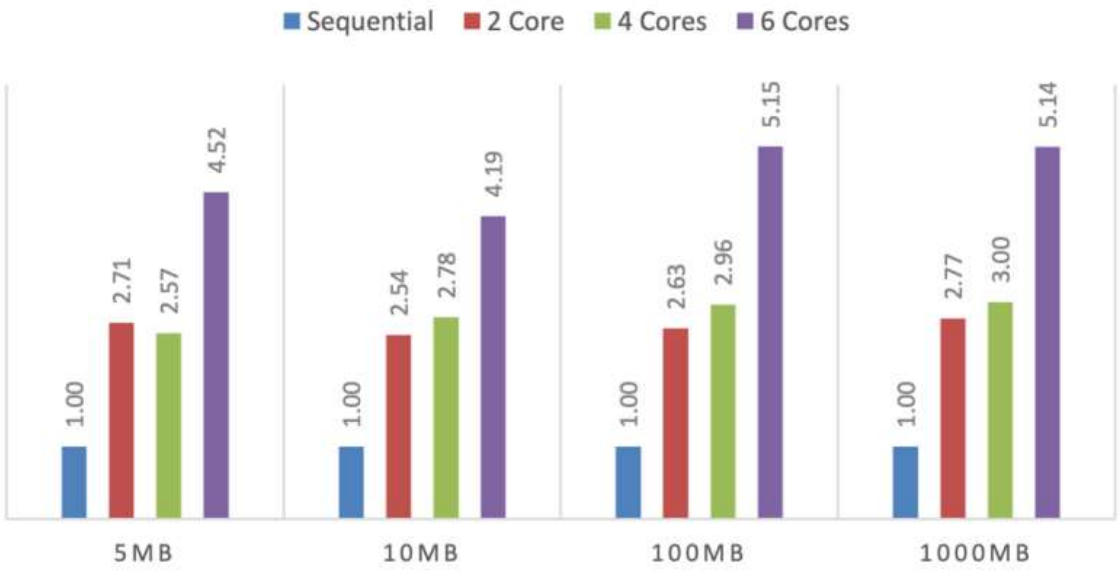

Рис. 3.5. Показники прискорення для алгоритму шифрування 3DES

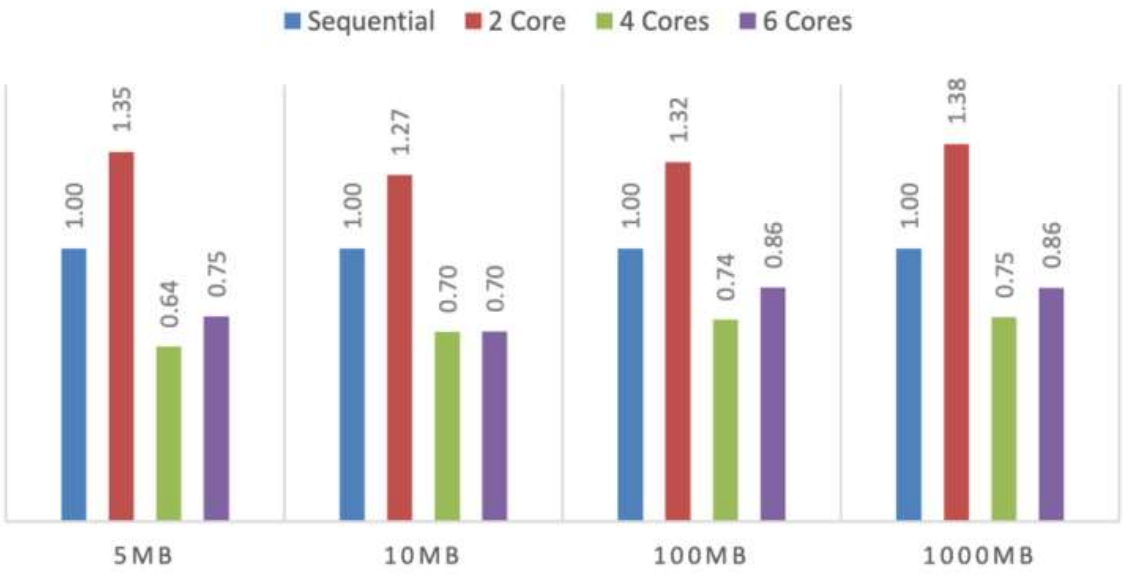

Рис. 3.6. Показники ефективності для алгоритму шифрування 3DES

На рис. 3.7 показано результат часових вимірювань для алгоритму AES. Видно, що використання паралельного виконання забезпечує стабільний виграш у продуктивності. Графічне представлення коефіцієнта прискорення (рис. 3.8) та ефективності (рис. 3.9) підкреслює, що при збільшенні розміру файлу та кількості ядер результативність паралельної обробки підвищується.

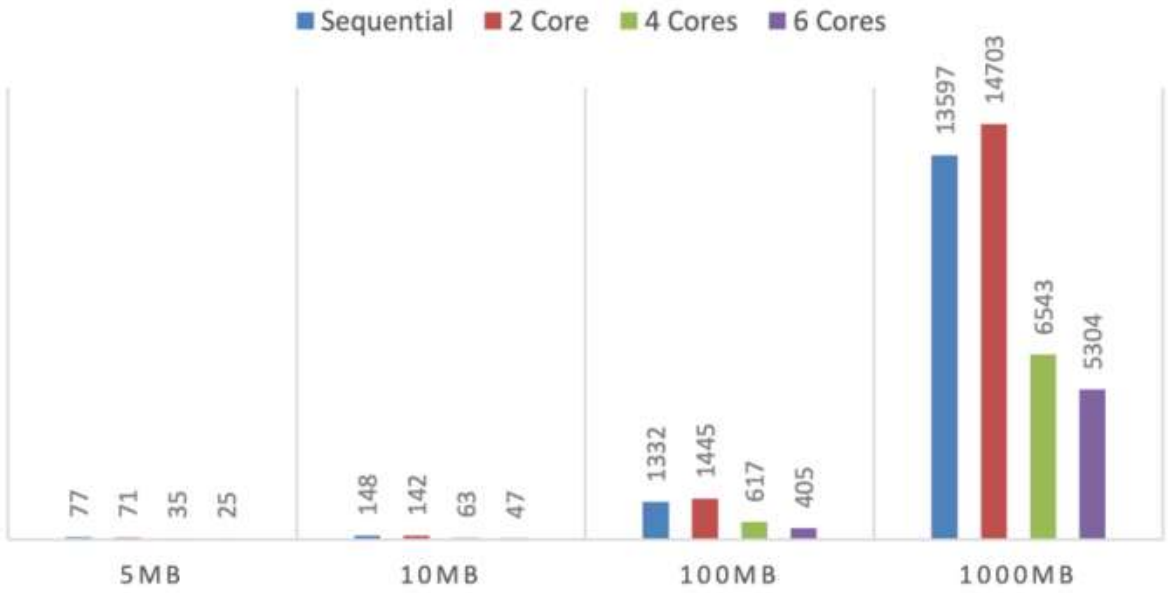

Рис. 3.7. Часові показники виконання алгоритму шифрування AES

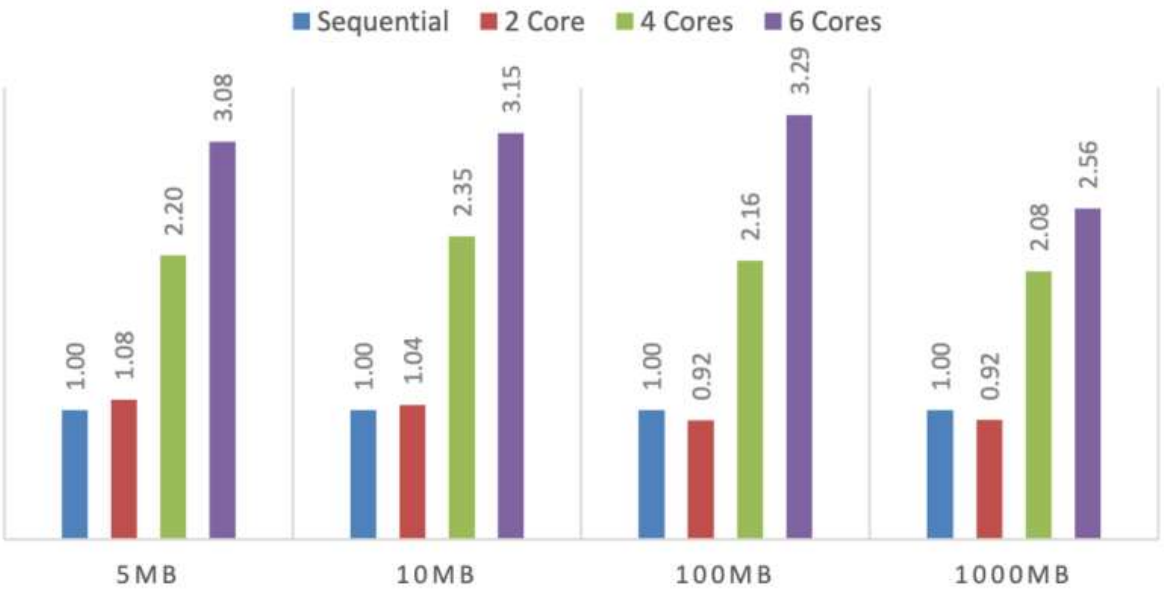

Рис. 3.8. Показники прискорення для алгоритму шифрування AES

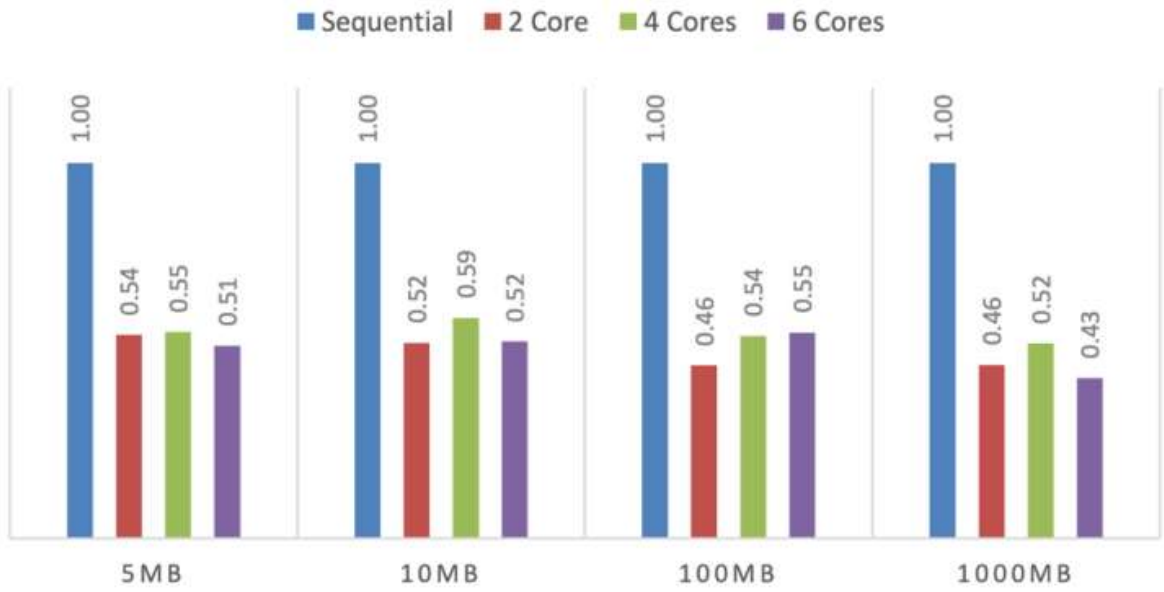

Рис. 3.9. Показники ефективності для алгоритму AES

Для алгоритму Blowfish на рис. 3.10 наведено залежність часу обробки від конфігурації системи, що підтверджує доцільність застосування паралелізації. Переваги паралельного виконання відображені на рис. 3.11 (прискорення) та 3.12 (ефективність), де можна побачити закономірність приросту продуктивності із збільшенням числа обчислювальних потоків.

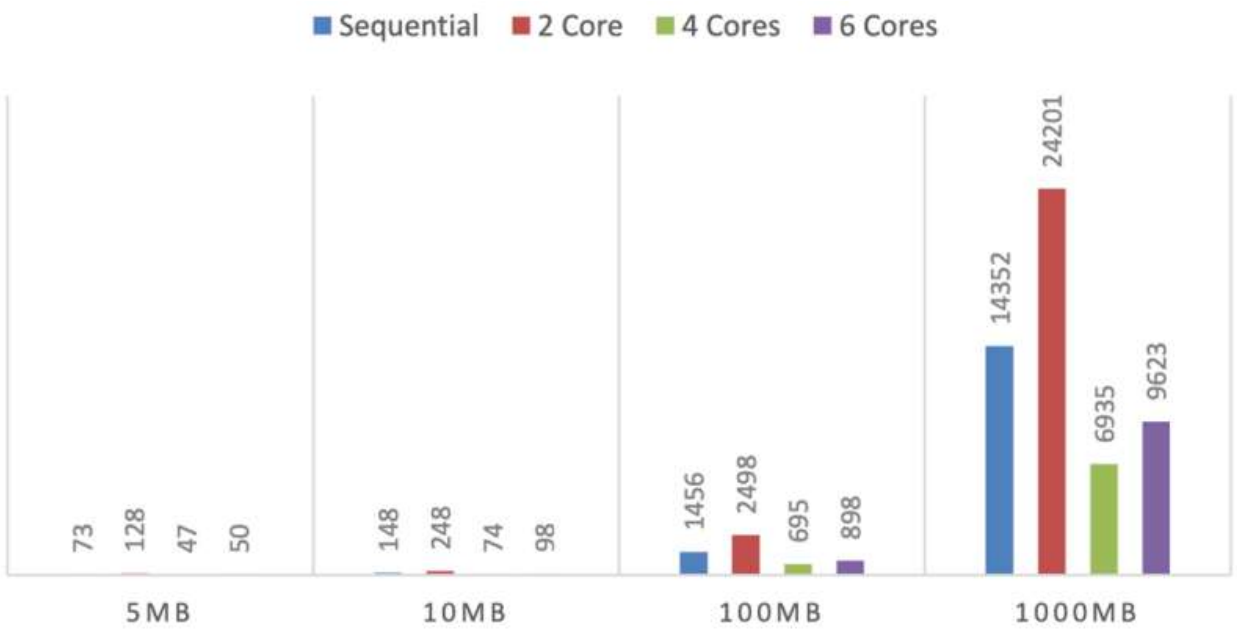

Рис. 3.10. Часові показники виконання алгоритму шифрування Blowfish

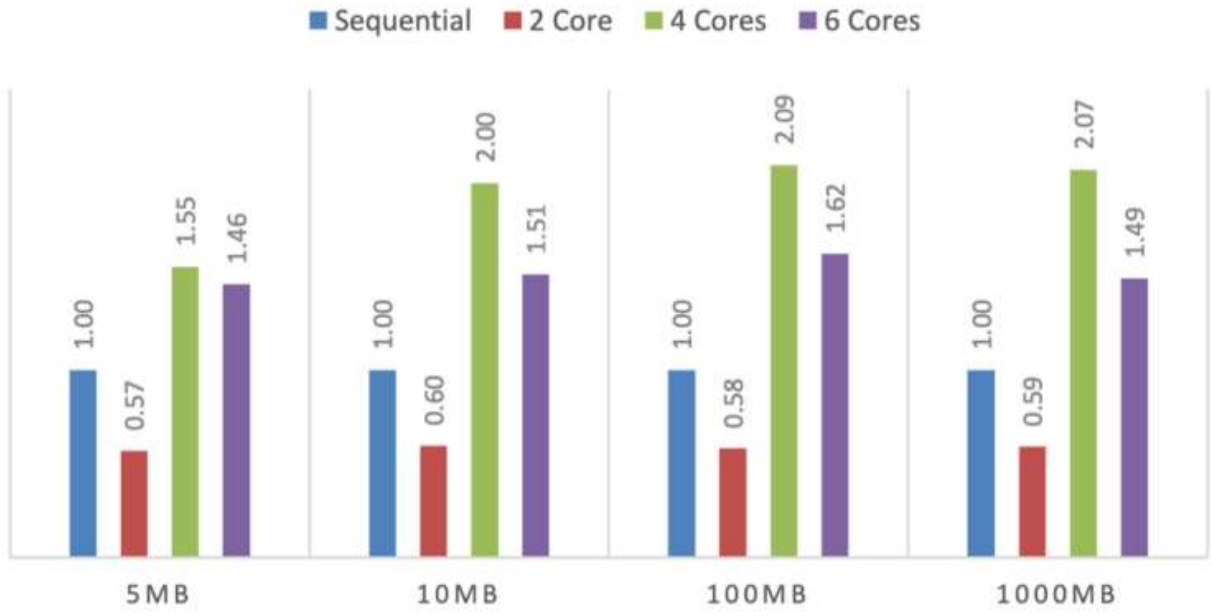

Рис. 3.11. Показники прискорення для алгоритму шифрування Blowfish

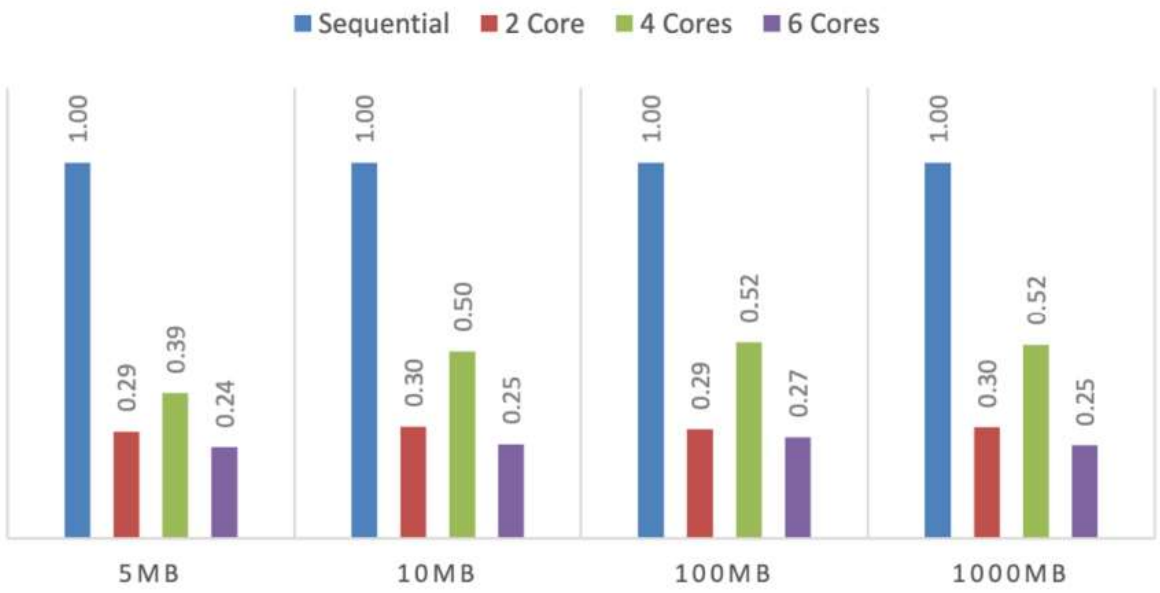

Рис. 3.12. Показники ефективності для алгоритму шифрування Blowfish

Останнім було досліджено алгоритм Twofish. Значення часу виконання представлено на рис. 3.13, де також чітко простежується тенденція до скорочення часу за рахунок паралельного виконання. Зміни коефіцієнтів прискорення і ефективності наведено відповідно на рис. 3.14 та 3.15, і вони підтверджують ефективність масштабування при збільшенні числа ядер.

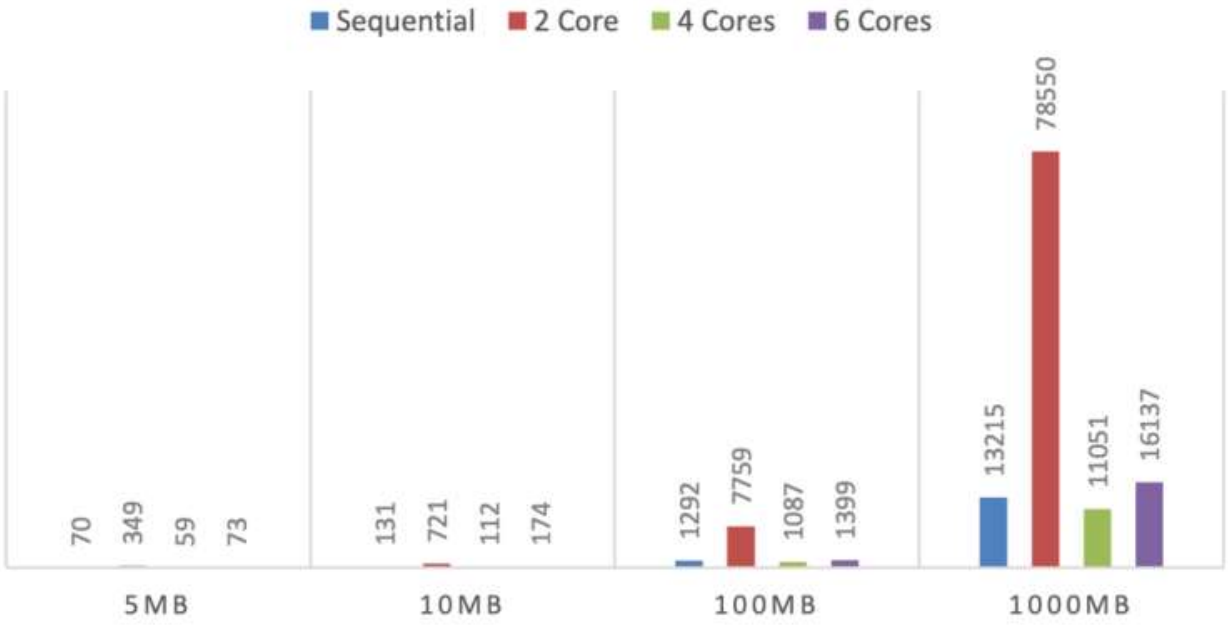

Рис. 3.13. Часові показники виконання алгоритму шифрування Twofish

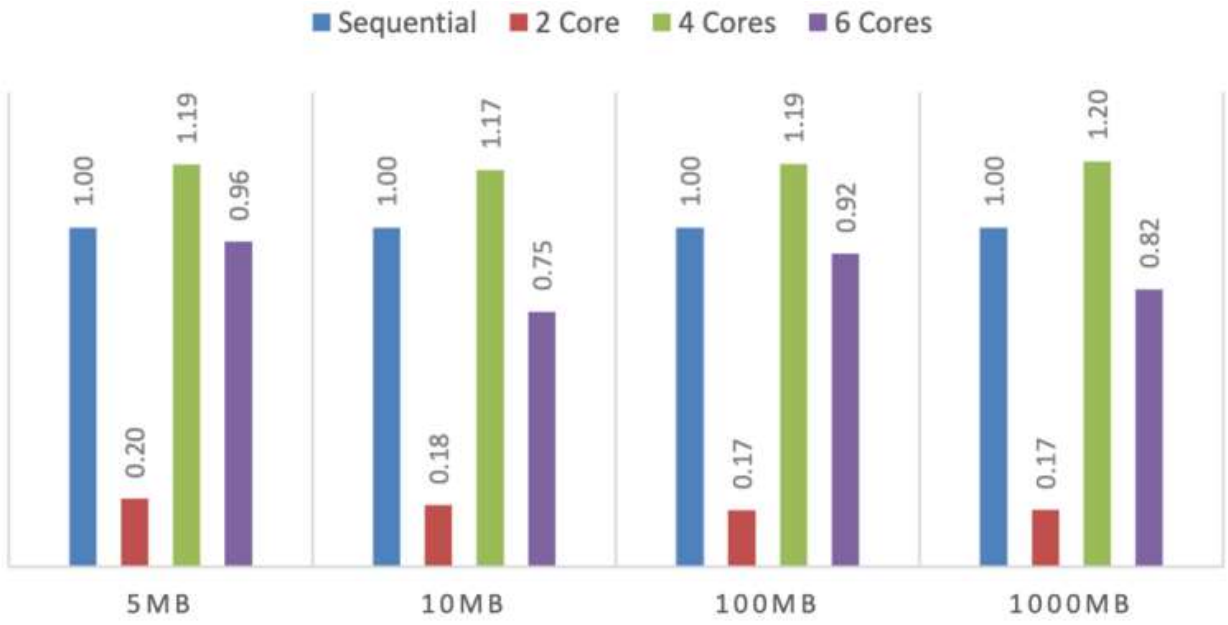

Рис. 3.14. Показники прискорення для алгоритму шифрування Twofish

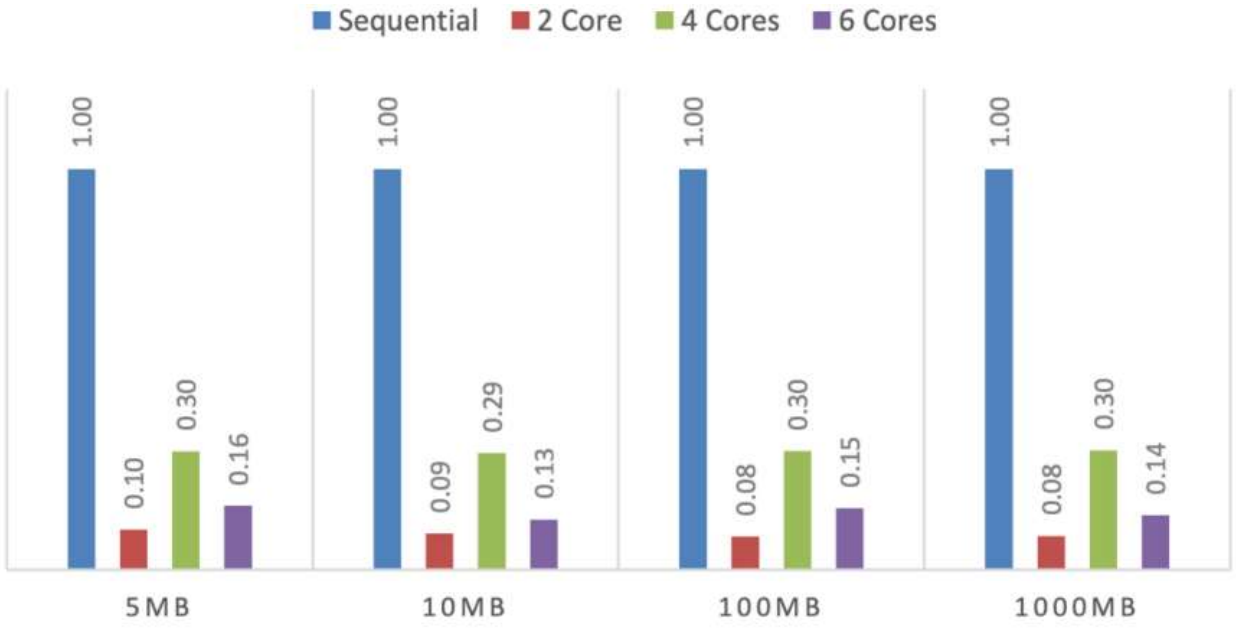

Рис. 3.15. Показники ефективності для алгоритму шифрування Twofish

Загалом, результати експериментального дослідження свідчать про те, що паралельна обробка даних забезпечує значне зниження часу шифрування та підвищення продуктивності для всіх розглянутих алгоритмів. При цьому рівень прискорення та ефективності залежить від обчислювальної складності криптоалгоритму та розміру оброблюваних даних: найвищі показники

зафіксовано для DES і Blowfish, тоді як ресурсоємні алгоритми, як-от 3DES, демонструють відносно менший, але стабільний приріст продуктивності.

3.5. Висновки до розділу 3

У третьому розділі було здійснено розроблення та експериментальне дослідження програмного забезпечення для системи захищеного зберігання й передавання інформації з використанням механізмів паралельного шифрування. На основі аналізу вимог до продуктивності та масштабованості криптографічних систем обґрунтовано вибір мови програмування C++ з використанням бібліотек криптографічних API та інструментів паралельного програмування Parallel Programming Library. Такий підхід забезпечив доступ до низькорівневих можливостей роботи з пам’яттю, підтримку апаратного прискорення та ефективний розподіл обчислювальних потоків між ядрами процесора [20, 21].

Було реалізовано паралельні версії поширених симетричних криптоалгоритмів, серед яких DES, 3DES, AES, Blowfish і Twofish, що дозволило забезпечити порівняння їх ефективності в умовах багатоядерних архітектур. У представленій реалізації застосовано модель паралельної обробки блоків даних, що є особливо релевантною для блочних шифрувальних алгоритмів та систем електронного документообігу.

Проведено вимірювання часу виконання, прискорення та ефективності паралельних і послідовних реалізацій на різних конфігураціях процесорів та різних обсягах даних. Експериментальні результати показали, що паралелізація криптографічних операцій дає відчутний приріст продуктивності порівняно з традиційним послідовним обчисленням. Найбільший виграш зафіксовано для алгоритмів DES та Blowfish, що мають нижчу обчислювальну складність. Алгоритми AES та Twofish також продемонстрували суттєве зменшення часу обробки при збільшенні кількості

обчислювальних ядер. У випадку 3DES приріст продуктивності є помітним, проте менш вираженим через його багатократну операційну складність.

Таким чином, проведене дослідження підтвердило доцільність використання паралельних обчислень у процесі шифрування великих обсягів даних. Використання паралельної моделі дозволяє істотно скоротити час обробки, підвищити масштабованість системи та забезпечити раціональне використання ресурсів сучасних багатоядерних процесорів. Отримані результати можуть бути застосовані в реальних системах електронного документообігу, хмарних сховищах та інших сервісах, де критичними є як безпека даних, так і швидкодія криптографічних операцій.

ВИСНОВКИ

У кваліфікаційній роботі було виконано дослідження та розробка програмного забезпечення для системи захищеного зберігання й передавання інформації, що дозволило системно оцінити сучасні технології електронного документообігу та методи забезпечення інформаційної безпеки.

У першому розділі проведено аналітичний огляд систем електронного документообігу, їхніх принципів функціонування та механізмів захисту інформації. Виокремлено основні проблеми забезпечення інформаційної безпеки, включаючи загрози конфіденційності, цілісності та доступності даних, що підтвердило необхідність впровадження комплексних захисних заходів при роботі з електронними документами.

У другому розділі розглянуто сучасні методи та засоби інформаційного захисту, включаючи алгоритми шифрування DES, Triple DES, AES, Blowfish, Twofish та RSA. Проведений аналіз показав, що симетричні алгоритми забезпечують високу швидкість обробки великих обсягів даних, а асиметричні алгоритми ефективні для безпечної передачі ключів та автентифікації. Комбіноване застосування різних методів шифрування дозволяє досягти високого рівня безпеки та стійкості систем електронного документообігу до потенційних атак.

У третьому розділі розроблено програмне забезпечення для паралельного шифрування даних, вибрано мову програмування та засоби паралельного програмування, створено та оптимізовано паралельні алгоритми шифрування. Експериментальне дослідження підтвердило, що паралельна реалізація алгоритмів значно підвищує продуктивність і ефективність обробки даних порівняно з послідовною реалізацією, забезпечуючи суттєве прискорення процесів шифрування при роботі з файлами різних розмірів.

Таким чином, проведені дослідження довели доцільність використання паралельних алгоритмів шифрування для підвищення продуктивності систем

захищеного зберігання та передавання інформації. Розроблене програмне забезпечення та отримані результати експериментального дослідження можуть бути використані для практичної реалізації безпечних систем обміну та зберігання електронних документів, а також для подальших досліджень у сфері криптографії та інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Карпенко М. Ю. Системи електронного документообігу : конспект лекцій для студентів усіх форм навчання першого (бакалаврського) рівня вищої освіти спеціальності 122 – Комп’ютерні науки / М. Ю. Карпенко ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2021. – 68 с.

2. Електронне урядування та електронна демократія : навч. посіб. : у 15 ч. / за заг. ред. А. І. Семенченка, В. М. Дрешпака. – Київ, 2017.

3. Грицяк Н. В. Електронний документообіг та захист інформації : навчальний посібник. – Київ : НАДУ, 2015. – 84 с.

4. Копняк К. В., Костунець Т. А. Автоматизація документообігу як складова підвищення ефективності діяльності підприємства. Економіка, фінанси, менеджмент. 2017. № 11. С. 57–68.

5. Євсеєв С. П., Шматко О. В., Ахієзер О. Б., Горбач Т. В. Основи кібербезпеки : навчально-практичний посібник / за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», Львів : «Новий Світ-2000», 2025. – 95 с. – (Серія «Кібербезпека та штучний інтелект»).

6. Галкін О. В., Шкільняк О. С. Основи криптології : навчальний посібник / О. В. Галкін, О. С. Шкільняк. – Київ, 2023. – 119 с.

7. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування. – Харків : Форт, 2012. – 870 с.

8. Федорук О. Безпека та захист інформації у системах електронного документообігу: підвищення рівня кіберзахисту. Вісник Книжкової палати, № 4, 2024. DOI: https://doi.org/10.36273/2076-9555.2024.4(333).39-44

9. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. – CRC Press, 2021. – 648 p.

10. Data Encryption Standard / Wikipedia: The Free Encyclopedia [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Data_Encryption_Standard

11. Triple DES [Електронний ресурс] / Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki/Triple_DES

12. Advanced Encryption Standard [Електроний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard

13. Blowfish [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Blowfish

14. Twofish [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Twofish

15. RSA [Електронний ресурс] / Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki/RSA

16. Вступ до програмування мовою С++. Організація обчислень : навч. посіб. / Ю. А. Бєлов, Т. О. Карнаух, Ю. В. Коваль, А. Б. Ставровський. – Київ : Видавничо-поліграфічний центр “Київський університет”, 2012. – 175 с.

17. Основи програмування на С++ [Електронний ресурс] : навч. посіб. / О. О. Водка [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2021. – 112 с. – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/52280

18. Минайленко Р. М. Паралельні та розподілені обчислення : навч. посіб. – Кропивницький : Видавець Лисенко В. Ф., 2021. – 153 с.

19. Малашонок Г. І., Сідько А. А. Паралельні обчислення на розподіленій пам’яті: OpenMPI, Java, Math Partner : підручник. – Київ : НаУКМА, 2020. – 266 с.

20. Rainer Grimm. Concurrency with Modern C++. What every professional C++ programmer should know about concurrency. Packt Publishing, 2019. – 727 p.

21. Richard Ansorge. Programming in Parallel with CUDA: A Practical Guide. Cambridge University Press, 2022. – 395 p.