МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Складанівського Дениса Валерійовича

УДК 004:6

КВАЛІФІКАЦІЙНА РОБОТА

Інформаційна система паралельного шифрування даних мережевого трафіку

122 «Комп'ютерні науки»

Подається на здобуття освітнього ступеня бакалавр

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____Складанівський Д.В
(підпис,ініціали та прізвище здобувача вищої освіти)

Керівник роботи

Воронтіков В.В
д.т.н., доцент

Житомир – 2021

Висновок
кафедри_____

За результатами попереднього
захисту:_____

Протокол засідання
кафедри_____

№__від «___»_____2021р.

Завідувач
кафедри_____

_____ _____ _____
(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)

«_____»_____2021р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти_____ захистила
(прізвище, ім'я, по батькові)
кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою_____
за шкалою ECTS_____
за національною шкалою_____

Секретар ЕК

_____ _____ _____
(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)

АНОТАЦІЯ

Складанівський Д.В Інформаційна система паралельного шифрування даних мережевого трафіку. - Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 122 – комп'ютерні науки. – Поліський національний університет, Житомир, 2021.

Метою кваліфікаційної роботи є розробка інформаційної системи паралельного шифрування даних мережевого трафіку алгоритмами паралельного шифрування для забезпечення захисту конфіденційних даних. Проведено аналіз необхідності розробки та впровадження інформаційної системи в мережі. Розроблено діаграму прецедентів, діаграму послідовності, блок-схему алгоритму роботи.

В результаті дипломного проєктування була створена інформаційна система паралельного шифрування даних мережевого трафіку.

Ключові слова: інформаційна система, шифрування, мережевий трафік, паралельне шифрування, мережа.

SUMMARY

The quality of the work for the purpose of the bachelor's degree for specialty 122 - computers of science. - Polisky National University, Zhytomyr, 2021.

By the method of the diploma robot's data the creation of an information system and parallel encryption of the given hemline traffic, which is a cipher text by parallel encryption algorithms, for the retrieval of confidential data. The analysis of the need for the development and implementation of the information system in the framing was carried out. The diagrams of precedents, the diagrams of connotations, and the block diagram of the robot's algorithm are broken down.

As a result of the diploma course, the information system of parallel encryption of the given hemline traffic was launched.

Keywords: INFORMATION SYSTEM, ENCRYPTION, NETWORK TRAFFIC, PARALLEL ENCRYPTION, NETWORK.

ЗМІСТ

ВСТУП

XXI століття – століття інформаційних технології, тому і поширеним стала робота з інформацією. Розвиток електронно-обчислювальної техніки дає зловмисникам все більше можливостей для дешифрування інформації. З часом алгоритми шифрування повинні покращуватися і до них висуваються все більш сурові вимоги, а кожен новий метод повинен перевірятися на кількість вразливих місць які були раніше. А через те, що паралельне шифрування даних підвищує швидкість і захищеність даних то цю систему можна вважати не тільки актуальною, але і перспективною на багато років вперед.

Однією із важливих функціональних характеристик алгоритмів шифрування є швидкість шифрування і криптостійкість. Результати швидкості шифрування показують, що технологія паралельного шифрування може підвищити ефективність передачі інформації та значно підвищити її безпеку. Для шифрування одержувач генерує *n* парних ключів (один для шифрування, а другий для дешифрування) і виробляє їх передачу на вузли. Після отримання частини тексту кожен вузловий комп'ютер виробляє шифр-текст і передає його в точку прийняття інформації для подальшого дешифрування і збору цільного тексту. Отже, суть роботи полягає в захисті переданих даних і збільшенні швидкості обробки за допомогою декількох етапів шифрування.

Мета і завдання дослідження. Метою кваліфікаційної роботи є розробка інформаційної системи паралельного шифрування даних мережевого трафіку.

Досягнення поставленої мети передбачає виконання таких завдань:

- провести аналіз існуючих алгоритмів паралельного шифрування;
- визначити призначення та область застосування інформаційної системи;
- розробити функціональні вимоги до інформаційної системи паралельного шифрування даних мережевого трафіку;
- побудувати діаграми прецедентів, діяльності та послідовності;
- описати схему DES;

- розробити інтерфейс користувача;
- виконати тестування програмного забезпечення.

Об’єкт дослідження. Процес побудови інформаційної системи паралельного шифрування даних мережевого трафіку.

Предмет дослідження. Методика розробки інформаційної системи паралельного шифрування даних мережевого трафіку.

Методи дослідження. Для досягнення поставленої мети та виконання завдань кваліфікаційної роботи застосовувались криптографічні методи захисту інформації.

Публікації автора за темою роботи:

1. Складанівський Д.В. Шифрування та захист бази даних: матеріали І міжнародної науково-практичної конференції м. Житомир, 3-4 червня 2021 року. С.103-104.
2. Складанівський Д.В Інформаційна система паралельного шифурвання даних мережевого трафіку: матеріали науково-практичної студентської конференції Поліського національного університету м.Житомир, 01 червня 2021 року. С.91-92.

Практичне значення отриманих результатів. Розроблена інформаційна система даних мережевого трафіку яка може використовуватись для шифрування конфіденційних даних в державних установах, організаціях та в особистому користуванні.

Структура та обсяг роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 27 сторінок тексту, 16 рисунків та 1 додатку.

РОЗДІЛ 1 АНАЛІЗ ОСОБЛИВОСТЕЙ СИСТЕМИ ПАРАЛЕЛЬНОГО ШИФРУВАННЯ ДАНИХ МЕРЕЖЕВОГО ТРАФІКУ

1.1. Аналіз алгоритмів паралельного шифрування

Паралельне шифрування створено для підвищення ефективності алгоритмів. Дослідження швидкості шифрування показали, що послідовне шифрування повільніше в часі виконання, ніж паралельна. Алгоритми порівнюються в часі виконання при шифруванні та дешифруванні інформації.

Advanced Encryption Standard (AES) - симетричний алгоритм блочного шифрування (розмір блока 128 біт). Розроблений бельгійськими криптографами Діменом та Рійменом. AES також раніше мав назву Rijndael і вважається одним із найбільш часто використовуваних і безпечних алгоритмів шифрування на сьогоднішній день. Зі збільшенням обчислювальної потужності AES вважається вразливим. Агентство національної безпеки (NSA) використовують цей шифр в своїх документах з високим рівнем таємності.

Blowfish – це перший симетричний алгоритм шифрування, створений Брюсом Шнайєром у 1993 році. Симетричне шифрування використовує єдиний ключ шифрування як для шифрування, так і для дешифрування даних. З самого початку цей шифр призначався як альтернатива DES. В загальному випадку алгоритм складається з двох етапів - розширення ключа і шифрування, дешифрування вихідних даних.

Twofish - шифр Фейстеля був одним із п’яти фіналістів конкурсу AES. Як і AES, розмір блоку Twofish становить 128 біт, він підтримує три довжини ключа 128, 192 та 256 біт. Twofish розбиває вхідний 128-бітний блок даних на чотири 32-бітних підблока.

Data Encryption Standard (DES) - найпопулярніший алгоритм безпеки. Це симетричний алгоритм, який означає, що ті ж ключі використовуються для шифрування та дешифрування даних. Довжина ключа - 8 байт (64 біт). Розмір блоку 64 біти, ключ також складається з 64 бітів, однак лише 56 насправді є ключовими решта 8 це біти перевірки парності.

Serpent - це симетричний блоковий шифр, який як і Rijndael був фіналістом у конкурсі Advanced Encryption Standard (AES). Serpent посів друге місце у цьому конкурсі. Шифр розроблений Росом Андерсоном, Елі Біхамом та Ларсом Кнудсеном. Має розмір блоку 128 біт і можливі довжини ключа 128, 192 або 256 біт. Алгоритм являє собою 32-раундовий шифр на основі SP-мережі, яка представляє собою ряд пов'язаних математичних операцій, що використовуються в блочних шифрах.

Triple DES - потрійний алгоритм DES такий же, як і алгоритм DES, за винятком того, що ми застосовуємо його три рази.

RSA (Rivest, Shamir,Adleman - ПЕРЕКЛАД) - алгоритм характеризується досконалою безпекою, простим управлінням ключами, він є простим у виконанні та розумінні. Криптосистема RSA стала першою системою, придатної і для шифрування, і для цифрового підпису. Популярність алгоритму RSA походить від того, що публічні та приватні ключі можуть шифрувати повідомлення для забезпечення конфіденційності, цілісності, достовірності та безвідмовність електронних комунікацій та даних за допомогою цифрових підписів [9].

1.2. Призначення та область застосування інформаційної системи паралельного шифрування

Шифрування захищає конфіденційні дані, але все одно не розповсюджене серед звичайних користувачів комп'ютера. Зараз шифрування більш поширене в організаціях, ніж в особистому користуванні.

Сфери в яких активно використовують шифрування:

1. Шифрування електронної пошти. Офісні працівники часто відправляють листи які містять конфіденційну інформацію. Електронна пошта не дає стовідсоткової гарантії захисту інформації , тому потребує додаткового захисту. Наприклад, hushMail – сервіс електронної пошти з шифруванням.
2. Інтернет-трафік зазвичай шифрується шляхом налаштування віртуальної приватної мережі (VPN).

3. Шифрування жорсткого диску. Найпоширеніші на сьогоднішній день операційні системи - Microsoft Windows та Apple OS X - включають для цього шифрування даних на рівні системи. Функція шифрування Windows називається BitLocker, тоді як Apple – FileVault. Інформацію потрібно шифрувати, але шифрувати кожен документ не завжди зручно, особливо якщо інформації багато. Є рішення, здатне забезпечити надійне зберігання конфіденційної інформації - віртуальний зашифрований диск. Наприклад, спеціалізована програма для шифрування TrustPort Tools.

4. Шифрування бази даних. Метод API: це шифрування на рівні програми, яке підходить для будь-якого продукту бази даних (Oracle, MSSQL тощо). Запити в зашифрованих стовпцях змінюються в додатку, що вимагає практичної роботи. Якщо бізнес має велику кількість даних, це може зайняти багато часу. Крім того, шифрування, яке функціонує на рівні програми, може призвести до збільшення проблем із продуктивністю.

5. Шифрування використовується в схемах електронних грошей для захисту звичайних даних транзакцій, таких як номери рахунків та суми транзакцій, цифрові підписи можуть замінити рукописні підписи або авторизацію кредитної картки, а шифрування відкритим ключем може забезпечити конфіденційність.

1.3 Функціональні вимоги до інформаційної системи паралельного шифрування даних мережевого трафіку

Інформаційна система має забезпечувати:

а) конфіденційність інформації;

б) простий та зрозумілий інтерфейс користувача, незалежно від операційної системи;

в) надійний захист файлів;

г) оптимальне зберігання даних

д) надійне збереження даних;

Висновки до першого розділу

Проведено аналіз предметної області дослідження, в результаті якого визначено основні вимоги до інформаційної системи паралельного шифрування даних мережевого трафіку. Проведено аналіз різних алгоритмів паралельного шифрування, визначено їх переваги та недоліки Визначено, що паралельне шифрування більш ефективне, ніж лінійне.

РОЗДІЛ 2 ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПАРАЛЕЛЬНОГО ШИФРУВАННЯ ДАНИХ МЕРЕЖЕВОГО ТРАФІКУ

2.1 Опис діаграм прецедентів

Однією з діаграм, яка використовується при проєктуванні ІС, є діаграма прецедентів (діаграма прецедентів, use case diagram), яка має на меті описати концептуальну модель роботи системи в середовищі.

Основними елементами діаграми прецедентів є:

- actor - елемент, що вказує на роль користувача, що взаємодіє з певною сутністю;
- прецедент - відображає елементи дій, що виконуються системою (включаючи зазначення можливих варіантів), і призводять до результатів, які спостерігає актор.

Можна встановити взаємозв'язок між прецедентами в моделі, наприклад:

- узагальнення - показує спільність ролей;
- включення - вказує на взаємозв'язок декількох застосувань, серед яких основною функцією завжди є використання пов'язаних прецедентів;
- розширення - представляє взаємозв'язок між базовим варіантом використання та варіантом використання як його особливий варіант використання.

У діаграмі прецедентів учасниками є користувачі рис. 2.1.

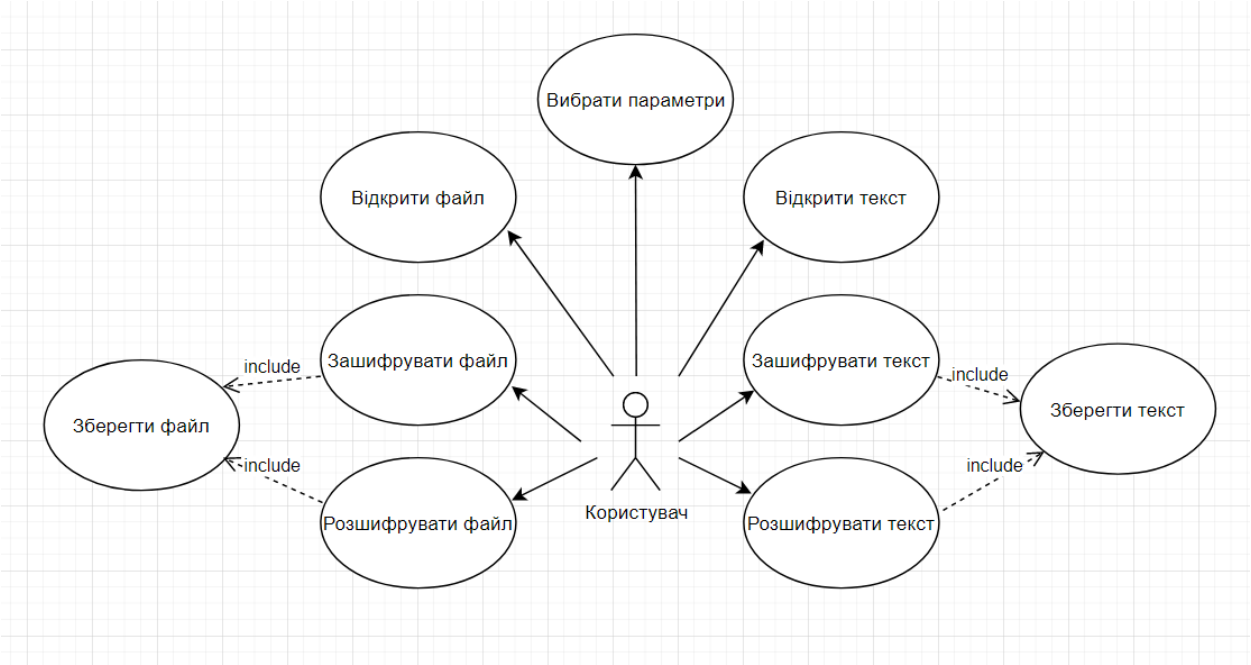

Рисунок 2.1 – Діаграма прецедентів

2.2 Опис діаграми діяльності

Діаграма діяльності - схема, що використовується для моделювання бізнес-процесів, яка показує декомпозицію компонентів діяльності, а саме: скоординоване виконання окремих дій та вкладених видів дій, які взаємопов’язані потоком з виходу одного вузла до входу іншого вузла, із зазначенням їх виконавців.

Діаграми діяльності мають багато спільних з іншими діаграмами (ім’я і графічне наповнення, що є проекцією моделі) та містить дії, вузли діяльності, потоки і значення об’єктів, примітки й обмеження.

Елементи діаграми:

- закруглені прямокутники представляють дії;
- ромби являє собою рішення;
- риски вказує на початок (розподіл) або закінчення (об’єднання) паралельних дій;
- чорне коло вказує на початок процесу (початковий стан);
- чорне коло в колі вказує на кінець (кінцевий стан);
- стрілки вказують від початку до кінця та вказують порядок, в якому відбуваються дії.

Розроблена діаграма діяльності наведена на рис. 2.2.

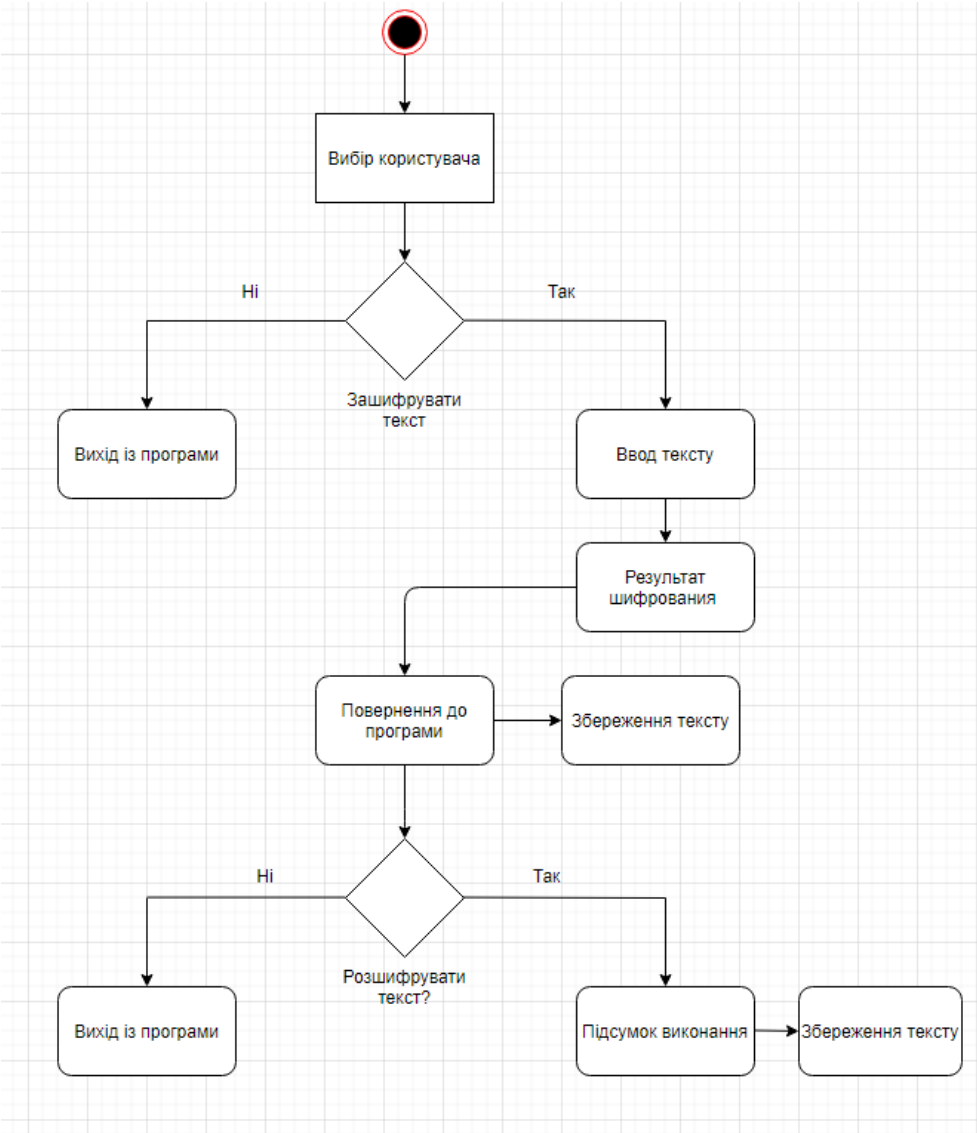

Рисунок 2.2 – Діаграма діяльності

2.3 Опис діаграми послідовності

Діаграма послідовностей - це схема, що показує послідовність інтерактивних проявів об’єктів.

Дана діаграма графічно демонструє порядок взаємодії певних об’єктів програми у часі. Як правило, в цій діаграмі демонструється, як користувачі (актори з діаграми варіантів використання) взаємодіють з іншими компонентами програми під час реалізації тих чи інших варіантів використання програми, та як при цьому взаємодіють інші компоненти програмної системи. Зазвичай, одна діаграма

послідовності присвячена опису одного з варіантів використання, зазначеного у Use-case діаграмі [7].

Діаграми послідовності є одним із способів формалізації сценаріїв використання. Перевага полягаю в тому, що на початковиї стадіях описування сценаріїв можливо з’ясувати склад взаємодіючих компонентів та описати потік повідомлень від одних компонентів до інших. Ці компоненти та потоки повідомлень в подальшому будуть трансформовані в конкретні класи (об’єкти), методи цих об’єктів (якщо говорити термінологією мови Java). Відповідно, одразу ж з’ясовується і модель системи подій (Actions), які дані класи (об’єкти) будуть підтримувати та обробляти [7].

Розроблена діаграма діяльності наведена на рис. 2.3.

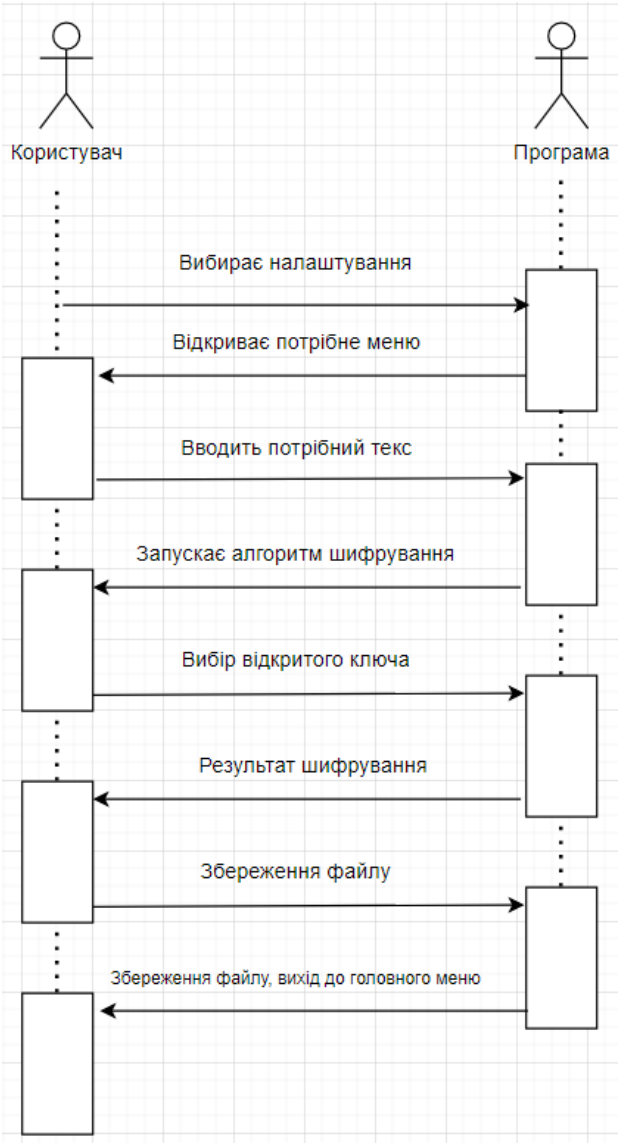

Рисунок.2.3 – Діаграма послідовності

2.4 Загальна схема DES

DES - алгоритм блочного шифрування. Алгоритм був розроблений у 1977 році та прийнятий як стандарт.

DES - це класична мережа Фейштеля з двома гілками. Дані шифруються в 64-розрядних блоках за допомогою 56-розрядного ключа. Алгоритм за кілька раундів перетворить 64-розрядний вхід у 64-розрядний вихід. Довжина ключа 56 біт. Процес шифрування включає чотири етапи. Перший виконує початкову перестановку 64-розрядного вихідного тексту, під час якого біти відповідають стандартній таблиці. Наступний етап складається з 16 раундів однієї і тієї ж функції з використанням операцій зсуву та заміни. На третьому етапі ліва і права половини результату кінцевої (16-ї) ітерації змінюють положення. Нарешті, на четвертому етапі класифікуються результати, отримані на третьому етапі.

Загальну схему алгоритму зображено DES на рис. 2.4.

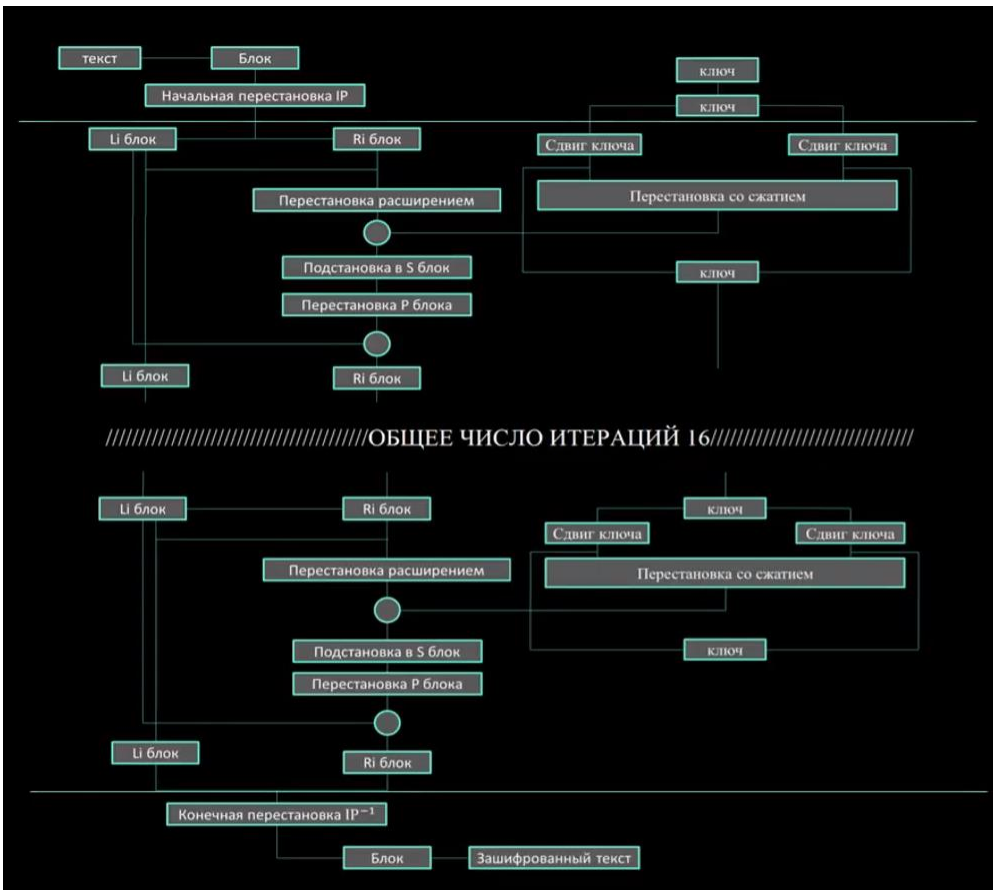

Рисунок 2.4 – Загальна схема DES

Висновки до другого розділу

Для інформаційної системи паралельного шифрування даних мережевого трафіку розроблено діаграму прецедентів, діяльності і послідовності, які описують взаємодії між користувачами та системою, дозволяють моделювати послідовності бізнес-процесів або дій, реалізованих методами класів, а саме: скоординованого виконання окремих дій і вкладених видів діяльності., графічно демонструють порядок взаємодії певних програмних об’єктів. Описана загальна схема алгоритму DES в якому виконується чотири етапи шифрування.

РОЗДІЛ 3 ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПАРАЛЕЛЬНОГО ШИФРУВАННЯ ДАНИХ МЕРЕЖЕВОГО ТРАФІКУ

3.1 Розробка програмного забезпечення інформаційної системи паралельного шифрування даних мережевого трафіку

Для реалізації інформаційної системи паралельного шифрування даних мережевого трафіку було обрано мову програмування C Sharp.

Переваги C #:

- C # - це об'єктноорієнтована, проста і в той же час потужна мова програмування, яка дозволяє розробникам створювати багатофункціональні програми;
- c # відносиця до мов компільованого типу, тому має всі переваги таких мов;
- C # об'єднує кращі ідеї сучасних мов програмування Java, C ++, Visual Basic і т.д;
- через велике розмаїття синтаксичних конструкцій і можливості працювати з платформою Net. C # дозволяє швидше, ніж будь-яка мова, розробляти програмні рішення;
- c # відрізняється надійністю і елегантністю;
- підтримка переважної більшості продуктів Microsoft;
- безкоштовність ряду інструментів для невеликих компаній і деяких індивідуальних розробників - Visual Studio, хмара Azure, Windows Server, Parallels Desktop для Mac Pro і ін;
- типи даних мають фіксований розмір (32-бітний int і 64-бітний long), що підвищує «мобільність» мови і спрощує програмування, так як ви завжди знаєте точно, з чим ви маєте справу.
- Автоматичне «очищення памяті» Це означає, що нам в більшості випадків не доведеться піклуватися про звільнення пам'яті. CLR сама викличе збирач сміття і очистить пам'ять.

- велика кількість «синтаксичного цукру»- спеціальних конструкцій, розроблених для розуміння і написання коду. Вони не мають значення при компіляції;
- низький поріг входження. Синтаксис C # має багато схожого з іншими мовами програмування, завдяки чому полегшується перехід для програмістів. Мова C # часто визнають найбільш зрозумілим і придатним для новачків;

Середовищем розробки було обрано Visual Studio.

3.2 Розробка інтерфейсу користувача

Стандартне меню де, можна звернути, розвернути і закрити програму, рис. 3.2.

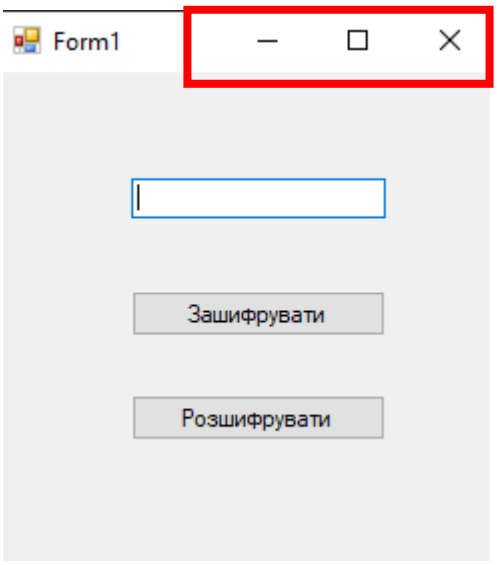

Рисунок 3.2 - Стандартне меню

Поле вводу ключа шифрування, рис. 3.2.1.

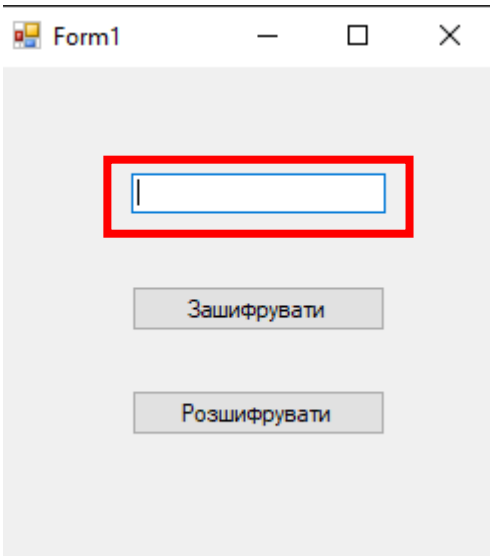

Рисунок 3.2.1 - Поле вводу ключа

Кнопка «Зашифрувати» виконує вибір файлу, після вибору виконується операція шифрування, а потім і збереженя, рис. 3.2.2.

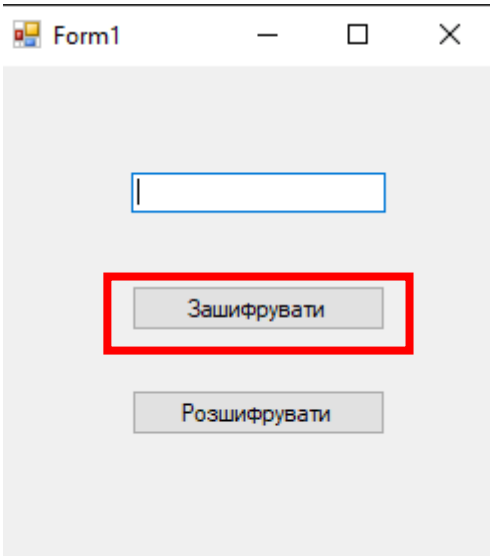

Рисунок 3.2.2- Кнопка шифрування

Кнопка «Розшифрувати» виконує розшифрування файлу і потім зберігає його, рис. 3.2.3.

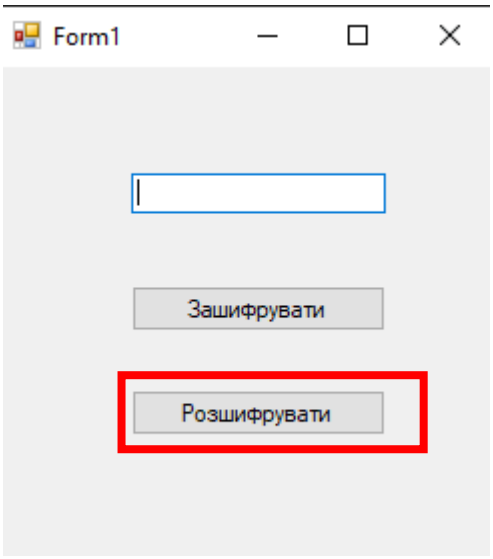

Рисунок 3.2.3 - Кнопка розшифрування

3.3 Тестування програмного забезпечення інформаційної системи паралельного шифрування даних мережевого трафіку

Тестування програмного забезпечення інформаційної системи паралельного шифрування даних мережевого трафіку починається з вводу ключа, який повинен бути мінімум з восьми символів або цифр, для того щоб гарантувати більшу безпеку, рис. 3.3.

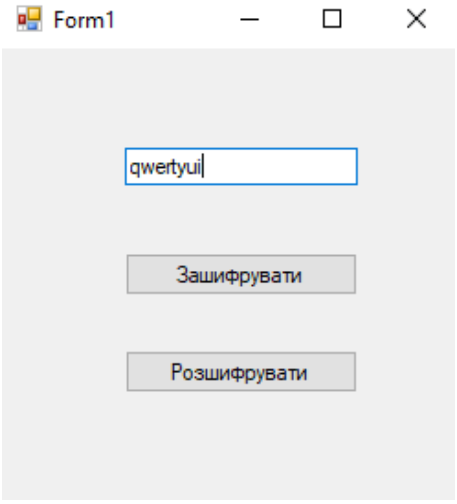

Рисунок 3.3 - Поле для ключа

Файл з інформацією, яка буде шифруватися зображено на рис. 3.3.1.

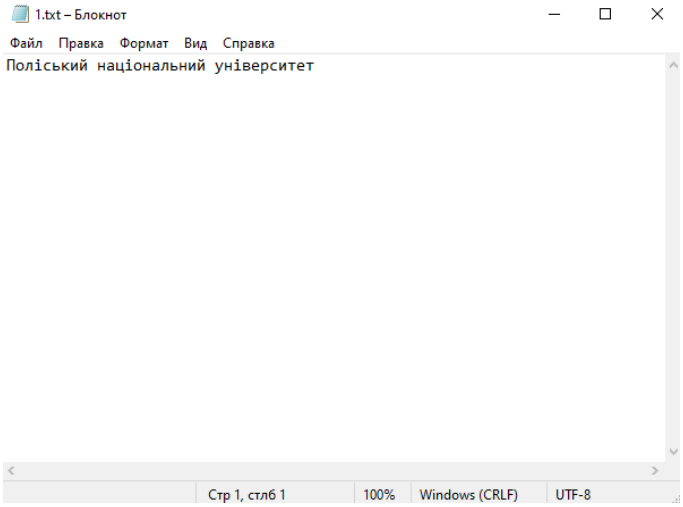

Рисунок 3.3.1 - Текст який буде шифруватися

Кнопка «зашифрувати» відкриє навігаційний файловий менеджер – провідник операційної системи Windows, в якому потрібно вибрати файл який буде

шифруватися, рис. 3.3.2.

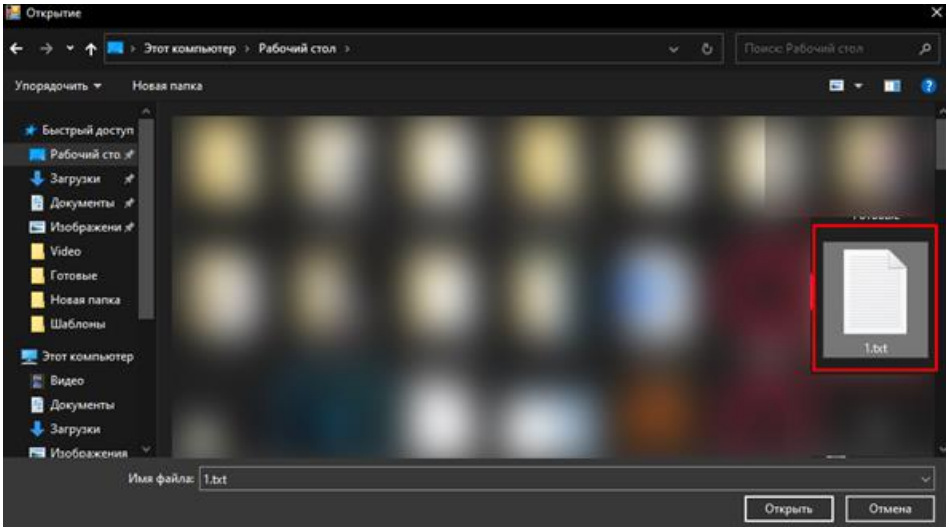

Рисунок 3.3.2 - Вибір файлу

Програма шифрування відразу виконує операцію і зберігає уже зашифрований файл у форматі des, рис. 3.3.3.

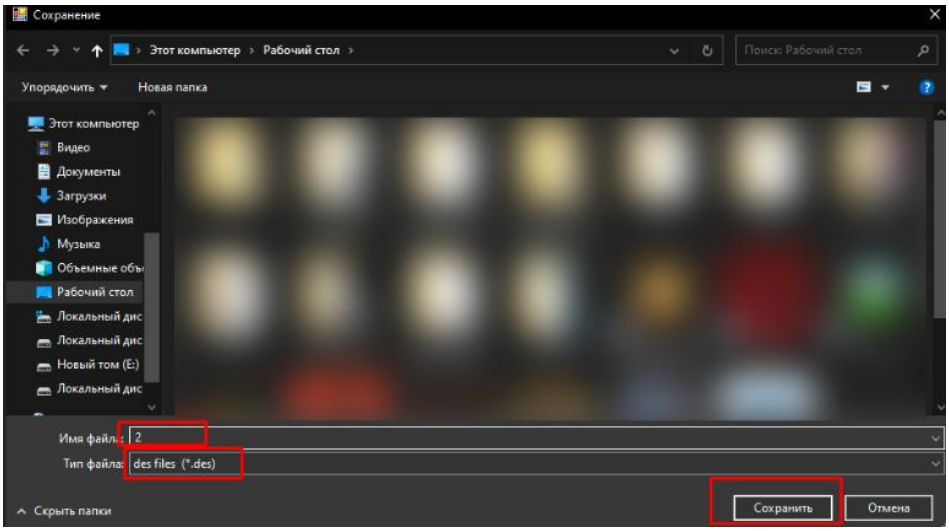

Рисунок 3.3.3 - Збереження файлу формату des

Відкриваємо (за допомогою блокноту) файл з розширенням .des для перевірки зашифрованого тексту, рис. 3.3.4.

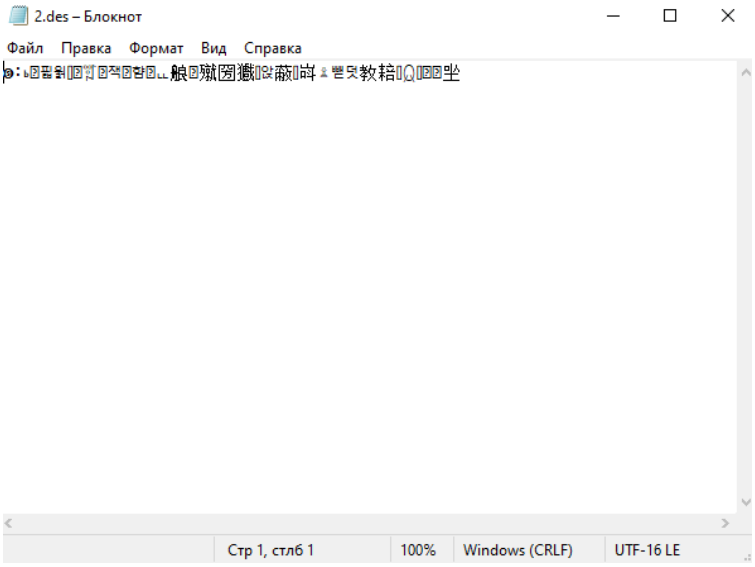

Рисунок 3.3.4 - Вигляд зашифрованого файлу

Кнопка «розшифрувати» розшифровує раніше зашифрований файл з форматом .des, рис. 3.3.5.

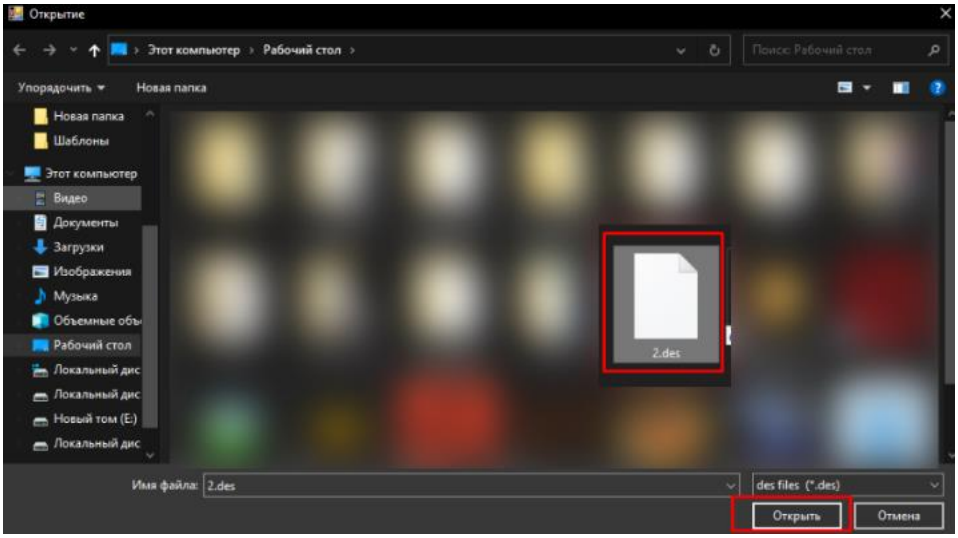

Рисунок 3.3.5 - Вибір зашифрованого файлу des

Програма розшифрувала файл, тепер зберігає його в розширені .txt, рис 3.3.6.

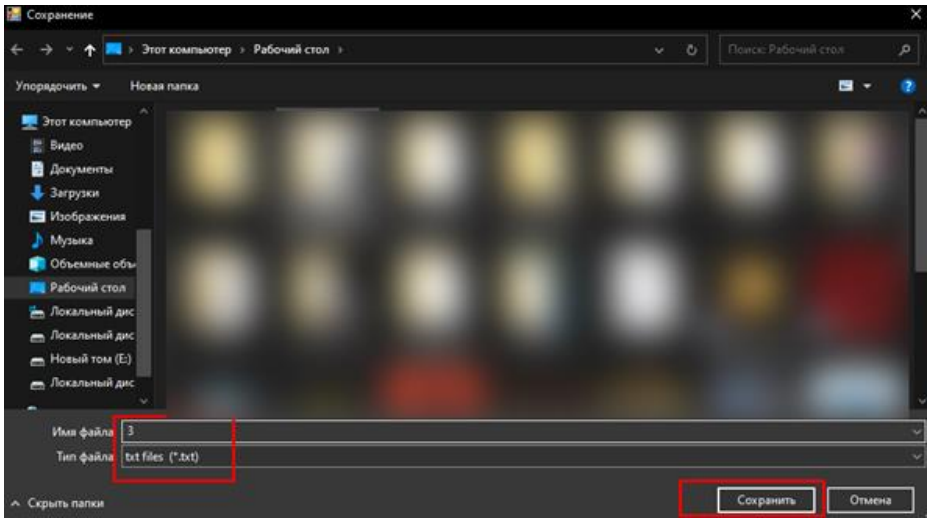

Рисунок 3.3.6 - Збереження розшифрованого файлу

Порівняння початкового і розшифрованого файлу, рис. 3.3.7.

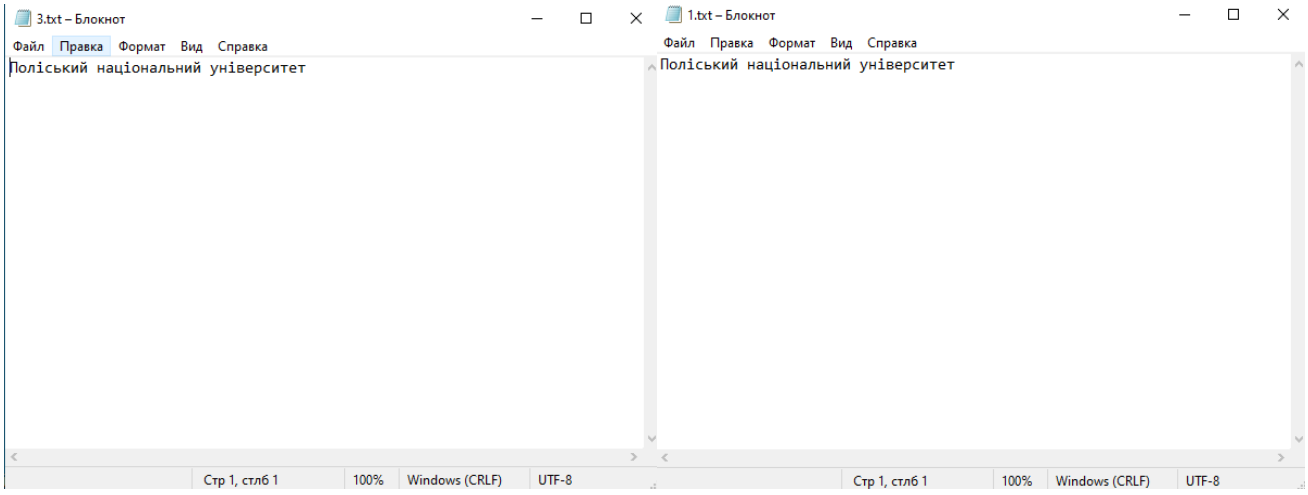

Рисунок 3.3.7 - Вигляд розшифрованого файлу

Висновки до третього розділу

Розроблено інформаційну систему паралельного шифрування даних мережевого трафіку на мові програмування C#. Побудовано інтерфейс інформаційної системи паралельного шифрування даних мережевого трафіку, на мові програмування C#. Середовищем розробки було обрано Visual Studio. Проведено тестування програмного забезпечення інформаційної системи паралельного шифрування даних мережевого трафіку і було доведено, що програма виконує шифрування обраного файлу.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було застосовано наукові методи та запропоновано підходи до процесу створення інформаційної системи паралельного шифрування даних мережевого трафіку.

В ході реалізації поставленої мети були виконані такі завдання:

1. Проведено аналіз необхідності розробки tas впровадження інформаційної системи. Визначено, що паралельне шифрування більш ефективне, ніж лінійне. Обрані паралельні алгоритми шифрування, визначено їх слабкі і сильні місця. Визначена область та призначення інформаційної системи паралельного шифрування даних мережевого трафіку.
2. Розроблено діаграму прецедентів, діаграму діяльності і діаграму послідовності.
3. Представлена загальна схема алгоритму DES в якому виконується чотири етапи шифрування та детально описується кожний етап.
4. Розроблено інформаційну систему паралельного шифрування даних мережевого трафіку на мові програмування C#, середовищем розробки було обрано Visual Studio.

В результаті дипломного проєктування була розроблена інформаційна система паралельного шифрування даних мережевого трафіку, яка забезпечує :

- конфіденційність інформації;
- збереження файлу;
- шифрування файлу;
- захист файлу;
- розшифрування файлу;

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Панасенко С. Алгоритми шифрування. Спеціальний довідник. - СПб.: БХВ-Петербург, 2009. - 576 с.
2. Бабенко Л. К., Сидоров І. Д. Паралельні алгоритми криптоаналізу асиметричних систем. Актуальні аспекти захисту інформації в Південному федеральному університеті. Монографія. - Таганрог: Изд-во ТТІ ПФУ, 2011. - С. 207-252.
3. Бабенко Л. К., Іщукова Е. А., Сидоров І. Д. Паралельні Алгоритми факторизації для аналізу асиметричних криптосистем // Матеріали міжнародної конференції «Моделювання сталого регіонального розвитку». - Нальчик:Вид-во КБНЦ РАН, 2011. - С. 78-84.
4. М. Гарленд, С. Ле Гранд та Дж. Ніколлз та ін. Досвід паралельних обчислень із CUDA. IEEE Micro, вип. 28, ні. 4, с. 13-27, 2008.
5. Хабр Сообщество IT–специалистов веб–сайт. URL: https://habr.com (дата звернення 01.06.2021).
6. Онацкий А. В., Йона Л.Г. Асимметричные методы шифрования. – Модуль 2 Криптографические методы защиты информации в телекоммуникационных системах и сетях: Учеб. Пособие/ Под ред. Н.В. Захарченко – Одесса: ОНАС им. А.С Попова, 2010 – 148с.
7. Dut Державний університет комунікацій веб–сайт. URL: http://www.dut.edu.ua (дата звернення 15.06.2021).
8. Бабаш А.В., Баранова Е.К. Оперативные методы криптографии. - М.: РГСУ, 2017. - 104 с.
9. ELAKPI Електронний архів наукових та освітніх матеріалів веб–сайт. URL: https://ela.kpi.ua (дата звернення 15.06.2021).
10. Адаменко М.В. Основы классической криптологии. Секреты шифров и кодов. - М.: ДМК Пресс, 2017. - 256 с.
11. Studfile Файловый архив студентов веб–сайт. URL: https://studfile.net (дата звернення 01.06.2021).