МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Факультет електроніки та інформаційних технологій

Кафедра електроніки і комп'ютерної техніки

«До захисту допущено»
Завідувач кафедри ЕКТ

_____ Анатолій ОПАНАСЮК
(підпис) (Ім’я та ПРІЗВИЩЕ)
____ _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня «бакалавр»

зі спеціальності 171 «Електроніка»

освітньо-професійної програми «Електронні системи та компоненти»

на тему:

ПРИСТРІЙ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ АЛГОРИТМУ ПОДВІЙНОЇ ПЕРЕСТАНОВКИ

Здобувача групи ЕС-01 _____ Биваліна Руслана Андрійовича

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

_____ _____
(підпис) (Ім’я та ПРІЗВИЩЕ)

Керівник, доцент, к.т.н., доцент Ольга БЕРЕЖНА _____
(підпис)

Консультант, директор ЕСП
«ТОВ «Преобразователь», Володимир АРБУЗОВ _____
(підпис)

Суми – 2024

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Факультет електроніки та інформаційних технологій

Кафедра електроніки і комп'ютерної техніки

Напрям підготовки 171 Електроніка

Освітня програма Електронні системи та компоненти

ЗАТВЕРДЖУЮ

Зав. кафедрою Опанасюк А. С.

"___"_____ 2024 р.

З А В Д А Н Н Я

на кваліфікаційну роботу бакалавра

Бивалін Руслан Андрійович

1. Тема роботи «Пристрій криптографічного захисту інформації на базі алгоритму подвійної перестановки»

затверджена наказом по університету "13" березня 2024 р. № 0256-VI.

2. Термін здачі студентом завершеної роботи 12.06.2024

3. Вихідні дані до роботи Розробити пристрій криптографічного захисту інформації на базі алгоритму подвійної перестановки. Синтез пристрою виконати на базі мікропроцесора.

4. Зміст розрахунково-пояснювальної записки (перелік питань, що належить розробити): 1) Огляд літератури та постановка задачі роботи. 2) Розробка структурної схеми проектованого електронного пристрою. 3) Розробка алгоритму роботи проектованого електронного пристрою. 4) Розробка принципових схем блоків проектованого електронного пристрою. 5) Розробка програмного забезпечення проектованого електронного пристрою.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) 1) Схема електрична структурна. 2) Схема алгоритму. 3) Схема електрична принципова.

6. Дата видачі завдання 13.03.2024

7. Керівник роботи Бережна О.В.

8. Завдання прийняв до виконання Бивалін Р.А.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проекту	Термін виконання етапів роботи	Примітки
1	Огляд літератури та постановка завдання проектування	27.04.24	
2	Розробка схеми електричної структурної проектованого електронного пристрою	01.05.24	
3	Розробка алгоритму роботи проектованого електронного пристрою	06.05.24	
4	Розробка принципових схем блоків проектованого електронного пристрою	13.05.24	
5	Розробка програмного забезпечення проектованого електронного пристрою	17.05.24	
6	Оформлення пояснювальної записки	25.05.24	
7	Оформлення графічного матеріалу	01.06.24	
8	Представлення роботи керівнику і отримання відгуку	09.06.24	
9	Представлення роботи кафедрі для отримання рецензії	09.06.24	

Студент _____ Р.А. Бивалін
(підпис)

Керівник кваліфікаційної роботи _____ О.В. Бережна
(підпис)

«____»_____2024 р.

РЕФЕРАТ

Пояснювальна записка містить: 58 аркушів, 23 рисунків, 12 таблиць, 11 джерел літератури.

Графічна частина роботи містить: схему алгоритму роботи пристрою, структурну та принципову електричні схеми.

Пояснювальна записка містить три розділи: огляд літератури і постановку завдання проектування, розроблення схеми електричної структурної пристрою та алгоритму його функціонування, розроблення схеми електричної принципової пристрою.

Перший розділ містить загальну інформацію про криптографію, розділи сучасної криптографії, криптографічні методи, а також постановку завдання на проектування.

Другий розділ присвячений розробленню алгоритму функціонування та схеми електричної структурної проектованого пристрою.

Третій розділ присвячений розробленню схеми електричної принципової пристрою.

ЗМІСТ

ВСТУП

Сьогодні головним чинником, що впливає на політичні та економічні аспекти національної безпеки, є рівень захищеності інформації та інформаційного середовища.

У цьому контексті криптографія виступає невід'ємним елементом інформаційної безпеки, пропонуючи різноманітні методи для шифрування даних. Одним з ефективних методів є алгоритм подвійної перестановки, який, завдяки своїй структурній простоті та високому рівню захисту, знаходить застосування у різних галузях.

Алгоритм подвійної перестановки полягає у дворазовій зміні порядку символів у повідомленні, що забезпечує додатковий рівень складності для зловмисників, які намагаються зламати шифр. Цей метод дозволяє перетворити оригінальний текст у вигляд, який практично неможливо розпізнати без знання ключів перестановки. Розуміння та впровадження пристроїв криптографічного захисту на базі цього алгоритму є важливим кроком на шляху до створення безпечного інформаційного простору [8].

Під час обробки інформації з обмеженим доступом необхідно забезпечувати її захист від несанкціонованого доступу, неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення, тобто гарантувати її конфіденційність, цілісність, доступність і спостережуваність. Зокрема, передача службової таємної інформації між системами здійснюється в зашифрованому вигляді або через захищені канали зв'язку за допомогою технічних та криптографічних засобів захисту. Криптографічний захист реалізується програмними, програмно-апаратними та апаратними засобами шляхом перетворення інформації з використанням спеціальних (ключових) даних для приховування або відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Сукупність засобів криптографічного захисту інформації, а також необхідної ключової, нормативної, експлуатаційної та іншої документації (зокрема такої, що визначає заходи безпеки), яка забезпечує належний рівень захищеності оброблюваної, збереженої та переданої інформації, називається криптографічною системою (криптосистемою). Система криптографічного

захисту інформації включає органи, підрозділи, групи та підприємства, установи і організації, що займаються розробкою, виробництвом, експлуатацією та розповсюдженням криптосистем і засобів криптографічного захисту [8].

Криптографія виникла історично через потребу в захищеній передачі секретної інформації. Спочатку вона зосереджувалася на розробці спеціальних методів, що перетворювали інформацію у форму, недоступну для потенційних зловмисників. Згодом зросло використання електронних способів передачі та обробки даних, і криптографія стала широко застосовуватися в комп'ютерних інформаційних технологіях. Сучасна криптографія вирішує численні завдання, які виходять за межі простого засекречування інформації.

Нинішні виклики криптографії включають розробку систем електронного цифрового підпису, методів таємного електронного голосування, протоколів електронного жеребкування, ідентифікації віддалених користувачів, а також методів захисту від підроблених повідомлень тощо. Багато практичних завдань інформатики можна вирішити тільки за допомогою криптографічних методів [3].

У криптографії враховується діяльність зловмисника (криптоаналітика, опонента, нелегального користувача), який обізнаний про використовувані криптографічні алгоритми, протоколи та методи і намагається їх скомпрометувати. Компрометація криптосистеми може виражатися, наприклад, у несанкціонованому читанні інформації, підробці підписів, зміні результатів голосування, порушенні таємниці голосування, чи складно виявлюваній модифікації даних. Такі дії зловмисника називаються криптоаналітичними атаками.

Криптографія має особливість розробляти методи, що забезпечують стійкість до будь-яких дій зловмисника, навіть коли на момент створення криптосистеми неможливо передбачити всі можливі способи майбутніх атак, які можуть виникнути завдяки новим досягненням у теорії та технологіях. Оцінка надійності криптографічних рішень, зокрема трудомісткості атак на криптосистеми, є складним завданням і основним предметом криптоаналізу. Криптографія і криптоаналіз утворюють єдину галузь знань — криптологію, яка є частиною сучасної математики та має важливі застосування в інформаційних технологіях [3].

Захист конфіденційності та цілісності інформації є критично важливим у сучасному цифровому світі. Зі зростанням кіберзагроз і постійним розвитком

технологій необхідно знаходити ефективні методи захисту даних від несанкціонованого доступу. Одним із найдієвіших способів забезпечення безпеки інформації є криптографічний захист, який використовує шифрування для захисту даних від несанкціонованого доступу.

Серед різноманітних криптографічних методів особливо вирізняється алгоритм подвійної перестановки, який базується на складних математичних операціях і перестановках символів у тексті. Цей алгоритм забезпечує високий рівень захисту, оскільки його реалізація включає послідовне застосування двох перестановок до вхідного тексту, що робить процес розшифрування практично неможливим без знання ключа.

У цьому вступі ми розглянемо принципи роботи алгоритму подвійної перестановки та його застосування для криптографічного захисту інформації. Дослідження цього алгоритму допоможе краще зрозуміти його переваги, недоліки та потенціал у контексті сучасних вимог до кібербезпеки.

1 ОГЛЯД ЛІТЕРАТУРИ І ПОСТАНОВКА ЗАВДАННЯ ПРОЕКТУВАННЯ

1.1 Огляд літератури

Проблема захисту інформації шляхом її перетворення, яке виключає можливість прочитання сторонніми, хвилювала людство з давніх часів. Історія криптографії тісно пов’язана з історією людської мови. Перші системи письма самі по собі були криптографічними, оскільки в стародавніх суспільствах володіння письмом було привілеєм обраних. Прикладом цього є священні книги Стародавнього Єгипту та Стародавньої Індії [1].

Криптографічні методи захисту інформації включають шифрування, кодування або інші способи перетворення даних, завдяки яким їхній зміст стає недоступним без ключа для зворотного перетворення. Криптографічний захист є найнадійнішим методом, оскільки захищається сама інформація, а не лише доступ до неї. Цей метод реалізується у вигляді програм або програмних пакетів.

Основні напрямки використання криптографічних методів включають передачу конфіденційної інформації через канали зв'язку (наприклад, електронна пошта), встановлення автентичності переданих повідомлень, а також зберігання інформації (документів, баз даних) на носіях у зашифрованому вигляді [1].

Процес криптографічного захисту даних може здійснюватися як програмним, так і апаратним шляхом. Хоча апаратна реалізація значно дорожча, вона має такі переваги, як висока продуктивність, простота та надійність. Програмна реалізація є більш практичною та гнучкою у використанні [1].

Під час розробки інформаційно-комунікаційних систем (ІКС) виникає важливе питання захисту інформації. Ця проблема стає все більш актуальною з розвитком інформаційних технологій та широким використанням ІКС і мереж у всіх сферах діяльності.

Нині в галузі захисту інформації сформувалася потужна індустрія, яка об'єднує науку й виробництво та спрямована на вирішення основних питань безпеки. Ці питання можна поділити на три групи: фізичні (об'єктивні фактори), логічні (суб'єктивні фактори) і соціальні.

До фізичної безпеки належать питання захисту від пожеж, затоплень, землетрусів, ураганів, вибухів, впливу промислових хімічних речовин, різних

магнітних полів, збоїв обладнання, гризунів тощо, тобто вплив зовнішнього середовища, яке може створювати перешкоди для наших каналів зв'язку.

Завада – це будь-який випадковий вплив на сигнал, який погіршує точність відтворення переданих повідомлень. Завади можуть бути різноманітними за своїм походженням і фізичними властивостями. У радіоканалах часто зустрічаються атмосферні завади, спричинені електричними процесами в атмосфері, зокрема грозовими розрядами. Енергія цих завад зосереджена переважно в діапазоні довгих і середніх хвиль. Сильні завади також створюються промисловим обладнанням, яке генерує так звані індустріальні завади через різкі зміни струмів в електричних колах різних електропристроїв. Сюди належать завади від електротранспорту, електродвигунів, медичних установок, систем запалювання двигунів тощо. Поширеним видом завад є перешкоди від сторонніх радіостанцій і каналів, спричинені порушенням регламенту розподілу робочих частот, недостатньою стабільністю частот, поганою фільтрацією гармонік сигналу, а також нелінійними процесами в каналах, що призводять до перехресних спотворень [2].

У дротових каналах зв'язку основним видом завад є імпульсні шуми та переривання зв'язку. Імпульсні завади часто виникають через автоматичну комутацію та перехресні наведення. Переривання зв'язку – це явище, при якому сигнал у лінії різко слабшає або зникає.

Практично в будь-якому діапазоні частот присутні внутрішні шуми апаратури, зумовлені хаотичним рухом носіїв заряду в підсилювальних приладах, резисторах та інших компонентах. Ці завади особливо помітні в радіозв'язку на ультракоротких хвилях, де інші види завад мінімальні. В цьому діапазоні також мають значення космічні завади, пов'язані з електромагнітними процесами на Сонці, зірках та інших астрономічних об'єктах. Шум визначає нижню межу сигналів, які можуть бути оброблені електронними засобами. Усунення впливу внутрішніх шумів на точність передачі повідомлень у системах зв'язку є однією з найскладніших задач для розробників. Навіть коли зовнішні завади можуть бути зведені до мінімуму або повністю усунені спеціальними заходами, залишається теоретично мінімальний рівень шумів, обумовлений наявністю внутрішніх джерел шуму.

Логічна безпека стосується захисту від несанкціонованого доступу (НСД), помилок у діях персоналу та програм, які негативно впливають на інформацію.

До соціальної безпеки належать засоби юридичного, організаційного та адміністративного захисту, підготовка кадрів, виховна робота, спрямована на формування дисципліни та етичних норм, обов'язкових для тих, хто працює в інформаційному середовищі. Основні характеристики безпеки інформації включають конфіденційність, цілісність та доступність [2].

Конфіденційність – це характеристика безпеки інформації, яка забезпечує її нерозкритість і доступність лише для осіб з відповідними повноваженнями. Цілісність – це властивість інформації, що дозволяє їй протистояти несанкціонованим змінам. Доступність – це характеристика безпеки інформації, що забезпечує можливість використання відповідних ресурсів у заданий момент часу згідно з наданими повноваженнями. Зараз зосередимо увагу на проблемі конфіденційності інформації.

1.2 Розділи сучасної криптографії

Українське законодавство щодо захисту інформації регулюється Цивільним та Господарським кодексами України, а також Законом України «Про інформацію», який введе поняття «інформація із обмеженим доступом». Згідно з цим законом, така інформація поділяється на конфіденційну та таємну.

Конфіденційна інформація - це дані, що перебувають у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і розповсюджуються за їх бажанням згідно з умовами, визначеними ними. Криптографічні методи виявляються надзвичайно ефективними серед різноманітних засобів захисту від несанкціонованого доступу до захищеної інформації, оскільки вони ґрунтуються на властивостях інформації та уникають слабкостей, пов'язаних із вузлами її обробки, середовищем передачі та адміністративними заходами.

Криптографія вивчає математичні методи забезпечення автентичності та конфіденційності даних. Сучасний її етап характеризується використанням алгоритмів, які передбачають реалізацію за допомогою обчислювальних засобів. Основні вимоги до сучасних методів криптографічного захисту - це забезпечення конфіденційності та цілісності. Сучасна криптографія акцентує увагу на методах захисту з використанням ключа, які поділяються на два типи: симетричні та асиметричні [2].

Симетричні системи шифрування використовують один ключ як для шифрування, так і для дешифрування, або ключ дешифрування може бути обчисленим за ключем шифрування. Вони відрізняються:

1. Великою пропускною здатністю.

2. Використанням відносно коротких ключів.

3. Можливістю використання як основи для створення різних криптографічних механізмів, таких як псевдовипадкові генератори чисел та обчислювально-ефективні схеми.

4. Можливістю їх комбінування для підвищення криптостійкості.

Першою ключовою характеристикою для класифікації шифрів є рівень інформації, невідомий для сторонніх осіб. Якщо алгоритм перетворення повідомлення є повністю невідомим зловмиснику, тоді такий шифр називають тайнописом. Це означає, що інформація закодована або перетворена таким чином, що зловмисник не знає принципу кодування. У криптографії з ключем, навпаки, сам алгоритм шифрування широко відомий, але шифрування відбувається на основі невеликого обсягу інформації – ключа, який відомий лише відправнику та одержувачу повідомлення.

У сучасній криптографії розмір ключа зазвичай коливається від 56 до 4096 біт. Всі криптоалгоритми з ключем поділяються на симетричні та асиметричні. У симетричних криптоалгоритмах ключі, використовувані на обох сторонах комунікації, є ідентичними. Цей ключ містить усю інформацію про процес шифрування повідомлення і тому повинен бути відомий тільки учасникам комунікації. Часто для цього термін "таємний ключ" і "шифр на таємному ключі" використовуються відповідно [4].

Рисунок 1.1 – Загальна схема передачі даних симетричного шифрування

У випадку асиметричного шифрування для кодування повідомлення використовується один ключ, а для розшифрування – інший. Таким чином, доступ до зашифрованого тексту можливий лише за наявності ключа розшифрування. Тому ключ для шифрування може бути відкритим для всіх користувачів мережі і відомим як відкритий ключ. Ключ для розшифрування, навпаки, залишається закритим. Самі асиметричні системи шифрування отримали назву шифру на відкритому ключі. Використання асиметричних шифрів для безпечного зберігання документів не має сенсу. Їх головне призначення – захист повідомлень, електронної пошти і тому подібних.

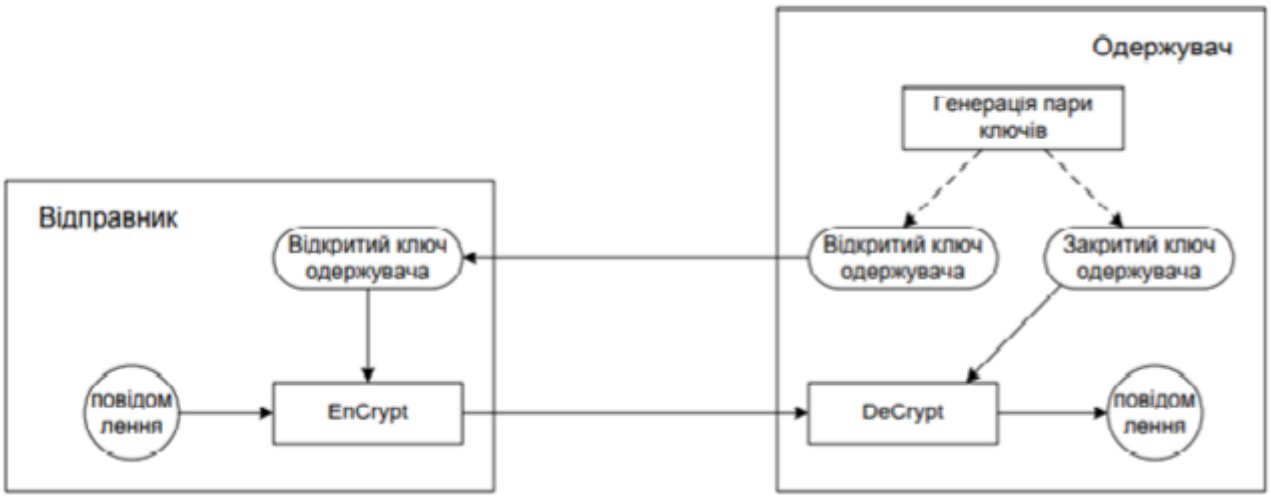


Рисунок 1.2 – Загальна схема передачі даних асиметричного шифрування

1. Симетричні схеми шифрування використовують один і той самий ключ як для шифрування, так і для розшифрування. У цих схемах оригінальний текст, також відомий як відкритий текст, перетворюється на шифрований текст за допомогою ключа, і цей же ключ використовується для розшифрування шифрованого тексту. Шифрування перетворює оригінальний текст у зашифрований, а розшифрування відновлює його до первинного стану за допомогою того ж ключа.

2. Криптосистеми з відкритим ключем використовують два ключі: відкритий і закритий. Інформація зашифровується за допомогою відкритого ключа, який доступний для всіх користувачів, а розшифровується за допомогою закритого ключа, який відомий лише одержувачу повідомлення. Основна

перевага асиметричного шифрування полягає в тому, що воно дозволяє обмінюватися секретними повідомленнями без попередньої домовленості щодо безпеки. Необхідність обміну таємним ключем по захищеному каналу відпадає. Деякі приклади криптосистем з відкритим ключем включають Схему Ель-Гамаля, RSA, Діффі-Гелмана і DSA [1].

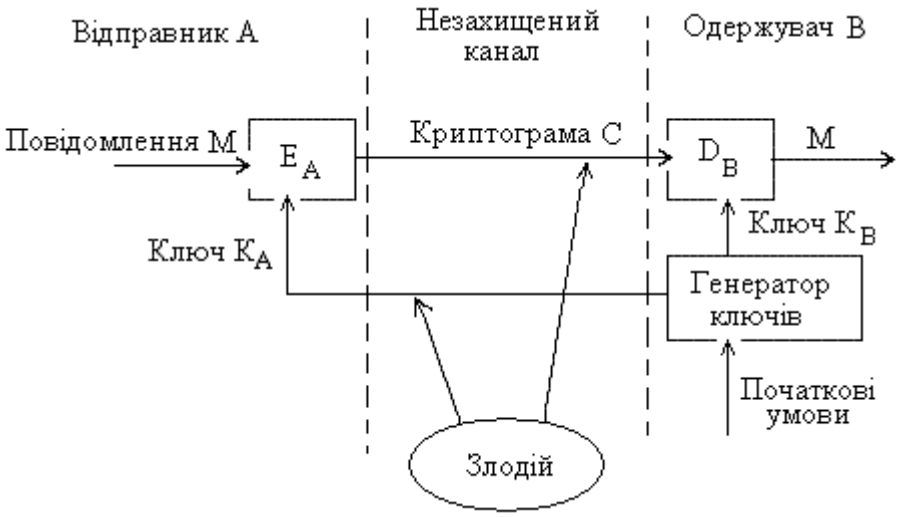


Рисунок 1.3 – Криптосистеми з відкритим ключем

Рисунок 1.4 – Як працює шифрування за RSA

3. Електронні підписи – це криптографічна процедура, що включається до тексту, для підтвердження авторства та цілісності повідомлення при його отриманні іншими користувачами [1].

4. Управління ключами – це процес обробки інформації, який включає у себе створення ключів та їх розподіл серед користувачів [1].

1.3 Симетричні криптосистеми

Симетричні криптографічні алгоритми використовують один і той же ключ для шифрування та розшифрування даних. До появи асиметричної криптографії основним методом була симетрична криптографія. Ключ алгоритму повинен бути таємним для обох сторін.

Алгоритми шифрування та розшифрування широко використовуються в комп'ютерних системах для захисту конфіденційної та комерційної інформації від несанкціонованого доступу. Основним принципом є необхідність, щоб отримувач заздалегідь знав алгоритм шифрування та ключ, без яких інформація залишається незрозумілою. Симетричні криптоалгоритми виконують перетворення невеликого блоку даних (1 біт або 32-128 біт) відповідно до ключа так, що оригінальний текст може бути відновлений лише з використанням цього секретного ключа [5].

Симетричні криптоалгоритми поділяються на:

- Скремблери.
- Блокові шифри.

Скремблери – це програмні або апаратні реалізації алгоритму, які дозволяють шифрувати неперервні потоки інформації біт за бітом. Сам скремблер представляє собою набір бітів, які на кожному кроці змінюються за певним алгоритмом. Після кожного кроку на виході з'являється біт, який «сумішчю» (операцією XOR) додається до поточного біту інформаційного потоку, або 0, або 1. Однак основним недоліком алгоритмів скремблювання є їх вразливість до фальсифікації.

Блокові шифри, у свою чергу, перетворюють блок вхідної інформації фіксованої довжини в результатуючий блок того ж обсягу, нечитабельний для сторонніх осіб, які не мають ключа. Таким чином, схему роботи блокового шифру можна представити як функції EnCrypt(X,Key) і DeCrypt(Z,Key), де Key

– це параметр блокового алгоритму, який представляє собою блок фіксованого розміру. Хоча вихідний (X) і зашифрований (Z) блоки даних мають однакову довжину, вони не обов'язково рівні розміру ключа [5].

1.4 Криптографічні методи

- Заміна – символи в зашифрованому тексті замінюються символами з іншого алфавіту відповідно до попередньо визначених правил;

- Перестановка – символи в зашифрованому тексті переставляються за певними правилами в межах певного блоку тексту, що передається;

- Аналітичне перетворення – зашифрований текст змінюється відповідно до певних аналітичних правил, наприклад, гамування – процес, що включає накладання псевдовипадкової послідовності чисел на вихідний текст, згенерованої на основі ключа;

- Комбіноване перетворення – це послідовність базових методів перетворення, які застосовуються до блоку зашифрованого тексту. На практиці, блокові шифри є більш поширеними, ніж певні класи «чистих» перетворень, через їх вищу криптографічну стійкість. Російські та американські криптографічні стандарти базуються на цьому класі [1].

Системи з відкритим ключем. Незважаючи на складність і надійність криптосистеми, їхньою слабкою точкою у практичному застосуванні є проблема розподілу ключів. Для обміну секретною інформацією між двома об'єктами в інформаційній системі (ІС), один з них має згенерувати ключ і передати його іншому об'єкту якимось секретним способом [1].

Порівняння асиметричних і симетричних криптоалгоритмів:

Асиметричні криптоалгоритми:

- Система шифрування з відкритим ключем;
- При шифруванні повідомлення використовується відкритий ключ, а при дешифруванні – закритий. Це означає, що за наявності ключа шифрування та зашифрованого тексту неможливо відновити вихідне повідомлення;
- При порушенні конфіденційності k-ої робочої станції зловмисник дізнається тільки “закритий” ключ k, що дозволяє йому читати всі повідомлення, що приходять абонентові k, але не дозволяє видавати себе за нього при відправленні листів;

- Кількість ключів у асиметричних системах залежить лінійно від кількості користувачів (у системі з N користувачів використовуються 2*N ключів).

Симетричні криптоалгоритми:

- Система шифрування з секретним ключем;
- Секретний ключ використовується як для шифрування, так і для дешифрування. Це означає, що за наявності ключа шифрування та зашифрованого тексту ви можете дешифрувати повідомлення;
- При порушенні конфіденційності будь-якої робочої станції зловмисник отримує доступ до всіх ключів цього користувача й може відправляти, нібито від його імені, повідомлення всім абонентам, з якими “жертва” вела переписку;
- У симетричних системах кількість ключів зростає квадратично зі збільшенням числа користувачів.

1.5 Системи з відкритим ключем

Асиметричні криптосистеми, також відомі як системи криптографічного захисту даних з відкритим ключем, є ефективними методами забезпечення безпеки інформації. У таких системах для шифрування використовується один ключ, а для розшифрування — інший, що створює асиметричний характер. Перший ключ, який відомий як відкритий, може бути опублікованим для загального використання всіма користувачами, які шифрують дані.

Проте розшифрування зашифрованих даних за допомогою відкритого ключа неможливе. Для цього отримувач зашифрованої інформації використовує другий ключ, що є секретним (закритим). Очевидно, що ключ розшифрування не може бути визначеним на основі ключа шифрування [6].

Незалежно від складності та надійності криптографічної системи, викликом у її практичному використанні є проблема обміну ключами. Для забезпечення обміну секретною інформацією між двома об’єктами в інформаційній системі, один з них повинен створити ключ і передати його іншому об’єкту способом, який залишається конфіденційним. Іншими словами, для передачі ключів часто використовують криптографічні системи. Для вирішення цієї проблеми були розроблені системи з відкритим ключем, які ґрунтуються на результаті класичної та сучасної алгебри. У таких системах кожен IP-адресат генерує два ключі, які мають певні взаємозв’язки. Один з цих ключів є відкритим і доступним для всіх, хто хоче відправити повідомлення адресатові. Другий ключ залишається секретним [1].

1.6 Електронний підпис

Які проблеми виникають у зв'язку з аутентифікацією даних? Зазвичай, у кінці звичайного листа або документа виконавець або відповідальна особа ставлять свій підпис з двома основними метами. По-перше, отримувач може перевірити автентичність листа, порівнявши підпис зі зразком, який він має. По-друге, підпис фізичної особи є юридичною гарантією того, що вона є автором документа. Цей аспект надзвичайно важливий при укладанні різних комерційних угод, довіреностей, договорів тощо. Однак, якщо підробити підпис людини на папері дуже складно, а встановлення авторства підпису за допомогою сучасних криміналістичних методів технічно складне, то з електронними підписами ситуація інша. Будь-який користувач може підробити ланцюжок бітів, просто скопіювавши їх, або непомітно внести несанкціоновані зміни в документ [1].

1.7 Управління ключами

Крім вибору відповідної криптосистеми для конкретної інформаційної системи, важливим аспектом є управління ключами. Незалежно від того,

наскільки складною і надійною є сама криптосистема, її ефективність залежить від правильного використання ключів. Хоча простий обмін ключами може забезпечити конфіденційність між двома користувачами, управління ключами стає складною задачею в інформаційних системах з великою кількістю користувачів. Ключова інформація охоплює всі ключі в системі. Якщо не дотримуватися належного управління ключами, зловмисники можуть мати необмежений доступ до інформації. Управління ключами – це процес, який включає генерацію, зберігання і розподіл ключів [1].

В початкових стадіях дискусій про криптографічні схеми було зазначено, що використання невипадкових ключів для зручності зберігання не рекомендується. В серйозних інформаційних системах використовують спеціальне обладнання або програмне забезпечення для генерації випадкових ключів. Зазвичай для цього використовуються генератори псевдовипадкових чисел.

Управління ключами включає в себе організацію зберігання, ведення обліку та видалення ключів. Зберігання ключів є критичним аспектом, оскільки ключі привертають увагу зловмисників і можуть призвести до розкриття конфіденційної інформації. Закриті ключі не повинні знаходитися у відкритому доступі на носіях, які можуть бути прочитаними або скопійованими. У складних інформаційних системах один користувач може мати справу з великим обсягом ключової інформації і, іноді, управляти невеликими базами даних ключів.

1.8 Узагальнена схема криптографічної системи

Криптографічна система представляє собою впроваджену програмно, апаратно або програмно-апаратно, що виконує криптографічне перетворення інформації з метою захисту. Припустимо, що відправник бажає надіслати повідомлення одержувачу, причому це повідомлення повинно бути передане безпечно: відправник прагне переконатися, що будь-який зловмисник, що перехопив інформацію, не зможе прочитати її зміст. Саме це повідомлення, яке передається, вважається відкритим текстом. Зміна форми повідомлення з метою приховання його змісту називається шифруванням. Зашифроване повідомлення отримує назву зашифрованого тексту (або даних). Процес перетворення зашифрованого тексту у відкритий називається розшифруванням (або

дешифруванням за допомогою криптографічного аналізу). Загальну схему криптографічного перетворення, яка забезпечує шифрування передаваної інформації (повідомлень, текстів, даних) і її подальше розшифрування, можна побачити на рис. 1.5.

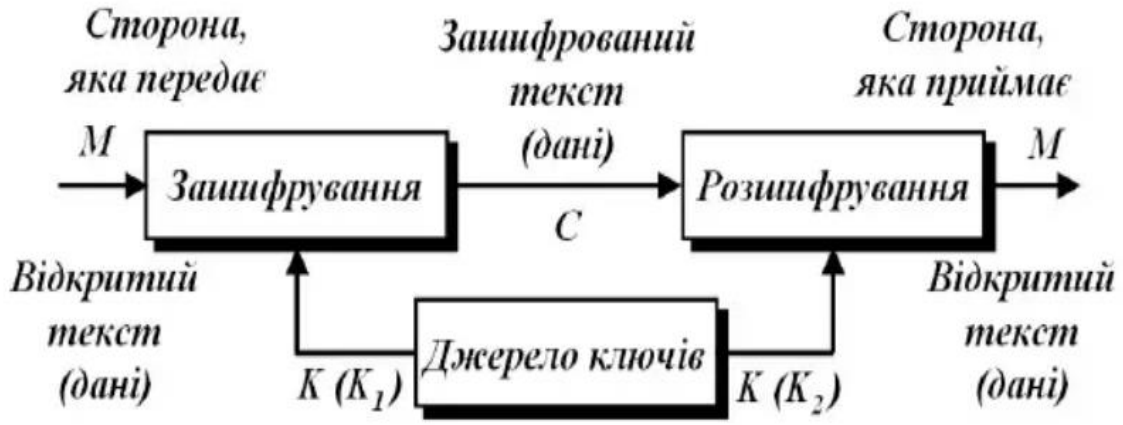


Рисунок 1.5 – Узагальнена схема криптографічного перетворення

Якщо безпека алгоритму базується на таємниці самого алгоритму, це вважається обмеженим підходом. Такі обмежені алгоритми представляють історичний інтерес, але вони абсолютно не відповідають сучасним стандартам. Велика або змінюючася група користувачів не може використовувати такі алгоритми, оскільки при виході хоча б одного користувача з групи, іншим членам потрібно переходити на інший алгоритм. Якщо кимось ззовні випадково виявиться секретний ключ, алгоритм потрібно змінити.

Сучасна криптографія вирішує ці проблеми за допомогою ключів. Ключ – це конкретний секретний набір параметрів алгоритму криптографічного перетворення даних, який дозволяє вибрати лише один варіант з усіх можливих. Множину всіх можливих ключів називають простором ключів.

Безпека алгоритмів, що описуються виразами, повністю базується на ключах, а не на особливостях алгоритму. Це означає, що алгоритм може бути опублікований і проаналізований. Продукти, які використовують цей алгоритм, можуть бути широко використані. Згідно з фундаментальним правилом криптографічного аналізу, вперше сформульованим О. Керкгоффсом у XIX столітті, стійкість шифру (криптографічної системи) повинна залежати лише від

секретності ключа. Іншими словами, правило Керкгоффса передбачає, що весь алгоритм шифрування й розшифрування, крім секретного ключа, відомий криптографічному аналітику противника. Це обумовлено тим, що криптографічна система, яка реалізовує ряд криптографічних перетворень, зазвичай розглядається як відкрита система. Такий підхід відображає дуже важливий принцип технології захисту інформації: захищеність системи не повинна залежати від секретності чогось, що не можна швидко змінити в разі витоку конфіденційної інформації.

Зазвичай криптографічна система складається з апаратних і програмних засобів, які можуть бути змінені лише за значні зусилля, тоді як ключ є елементом, який можна легко змінити. Саме тому стійкість криптографічної системи повинна залежати від ступеня секретності ключа.

1.9 Постановка завдання

Мета: Розробити пристрій для криптографічного захисту інформації на основі алгоритму подвійної перестановки з метою забезпечення конфіденційності та цілісності даних.

Опис задвдання: Необхідно розробити пристрій, який буде використовувати алгоритм подвійної перестановки для шифрування та розшифрування інформації. Пристрій повинен мати наступні функціональні можливості:

1. Здатність приймати вхідний текст та ключ для шифрування.
2. Реалізація алгоритму подвійної перестановки для шифрування вхідного тексту з використанням заданого ключа.
3. Можливість здійснення процедури розшифрування зашифрованого тексту з використанням того самого ключа.
4. Забезпечення безпеки ключа та зашифрованого тексту від несанкціонованого доступу.

Вимоги до пристрою:

1. Ефективна реалізація алгоритму подвійної перестановки з мінімальними обчислювальними витратами.
2. Високий рівень безпеки, що гарантує стійкість до криптоаналізу.

3. Можливість використання на практиці в різних областях, включаючи передачу конфіденційної інформації через відкриті мережі та зберігання даних у зашифрованому вигляді.

Для досягнення цієї мети необхідно виконати наступне:

1. Визначити основні функції та завдання, які повинен виконувати пристрій шифрування інформації.

2. Розробити алгоритм функціонування пристрою.

3. Розробити схему електричну структурну пристрою шифрування.

4. Розробити схему електричну принципову пристрою шифрування інформації на базі алгоритму подвійної перестановки.

Очікуваний результат: Розроблений пристрій має забезпечувати надійний криптографічний захист інформації на основі алгоритму подвійної перестановки, забезпечуючи високий рівень конфіденційності та цілісності даних. Такий пристрій буде використовуватися для захисту конфіденційної інформації в різних сферах, зокрема, у фінансах, медицині, військовій сфері тощо.

2 РОЗРОБЛЕННЯ АЛГОРИТМУ ФУНКЦІОНУВАННЯ ТА СХЕМИ ЕЛЕКТРИЧНОЇ СТРУКТУРНОЇ ПРИСТРОЮ

У ході виконання роботи було створено схему електричну структурну криптосистеми, яка наведена на рисунку 2.1.

Відправник створює відкритий текст вихідного повідомлення «М», призначеного передачі законному одержувачу через незахищений канал. Цей канал схильний до ризику перехоплення, тому перехоплювач намагається отримати доступ до повідомлення, що передається. Для захисту конфіденційності змісту повідомлення «М», відправник застосовує конвертоване перетворення Ек для шифрування. Таким чином, створюється шифртекст (або криптограма) С = Ек (М), який відправляється одержувачу.

Законний одержувач, прийнявши шифртекст «С», розшифровує його за допомогою зворотного перетворення $D=Ек^{-1}$ і отримує вихідне повідомлення у вигляді відкритого тексту М:

$Dk(C) = Ек^{-1}(Ек(M)) = M$.

Криптографічна система – це однопараметричне сімейство $(E_к)_{K\in\overline{K}}$ оборотних перетворень $E_K : \overline{M} \to \overline{C}$ з простору $\overline{M}$ повідомлень відкритого тексту в простір $\overline{C}$ шифровані тексти.

Ключ (К) вибирається з певної множини $\overline{K}$, відомої як простір ключів.

Ця криптосистема складається з таких частин:

- відправник;
- блок прийому інформації;
- шифрування Ек(М);
- канал зв'язку;
- перехоплювач;
- ключ;
- розшифрування Dк(С);
- одержувач.

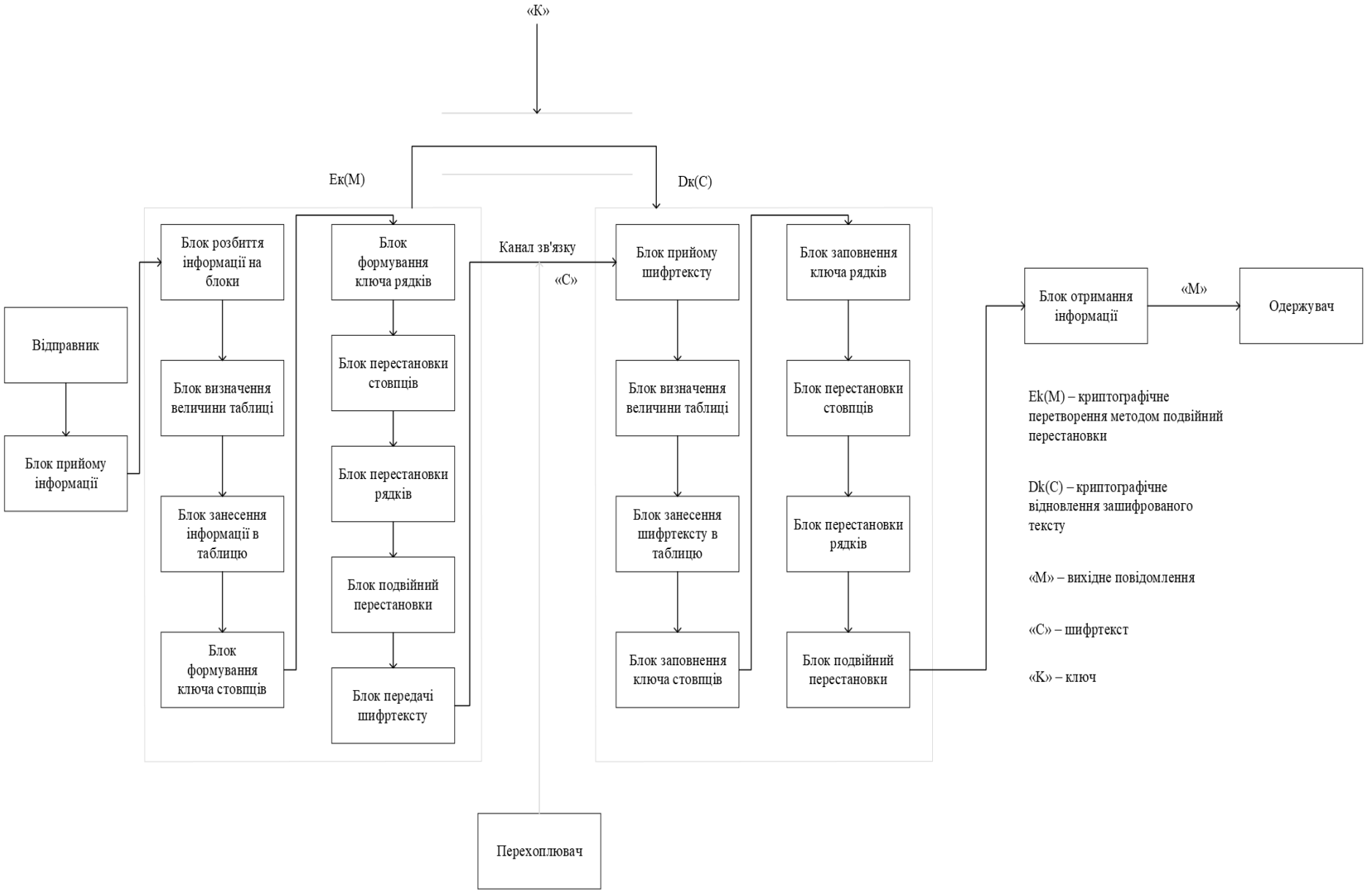


Рисунок 2.1 – Структурна схема криптосистеми

Блок шифрування включає:

- блок розбиття інформації на блоки;
- блок визначення величини таблиці;
- блок занесення інформації в таблицю;
- блок формування ключа стовпців;
- блок формування ключа рядків;
- блок перестановки стовпців;
- блок перестановки рядків;
- блок передачі шифртексту.

Блок розшифрування включає:

- блок прийому шифртексту;
- блок визначення величини таблиці;
- блок занесення шифртексту в таблицю;
- блок заповнення ключа стовпців;
- блок заповнення ключа рядків;
- блок перестановки стовпців;
- блок перестановки рядків.

Відправник – передає вихідний текст «М», який потрібно зашифрувати.

Блок прийому інформації отримує повідомлення від відправника та направляє його до блоку шифрування Ек(М).

Блок розбиття інформації поділяє повідомлення окремі інформаційні блоки для подальшого заповнення таблиці по блокам. Передача отриманої інформації з блоку прийому блок розбиття дозволяє здійснити цей поділ.

Блок визначення величини таблиці визначає необхідний розмір коректного розміщення інформації. Після цього визначення таблиця утворюється відповідним чином. Якщо створення таблиці відбувається успішно, процес переходить до блоку занесення інформації. У разі невдачі створення таблиці відбувається повторний запит на створення.

Блок занесення інформації в таблицю заповнює її даними, необхідні наступної перестановки.

Блок формування ключа стовпців запитує ключ «К» і вставляє його в спеціально відведене для ключа стовпців місце. Аналогічно, блок формування ключа рядків виконує аналогічну операцію.

Блок перестановки рядків здійснює переміщення рядків у довільному порядку, здійснюючи першу перестановку. Аналогічно, блок перестановки стовпців виконує переміщення стовпців у таблиці.

Блок передачі шифртексту здійснює передачу інформації з таблиці, в якій була виконана подвійна перестановка, канал зв'язку для доставки одержувачу.

У блоці розшифрування Dk(C) здійснюються зворотні операції порівняно з блоком шифрування Ек(М), що дозволяє відновити вихідне повідомлення із зашифрованого шифртексту.

Блок прийому шифртексту призначений для отримання зашифрованого повідомлення «С» з каналу зв'язку та його подальшої передачі. Після отримання повідомлення блок передає управління блоку визначення розміру таблиці, який визначає необхідний розмір для подальшої обробки даних.

Блок визначення величини таблиці використовується встановлення необхідних розмірів таблиці перед її створенням, щоб забезпечити правильну організацію даних у межах криптографічної системи.

Блок занесення шифртексту до таблиці виконує внесення зашифрованого повідомлення «С» до таблиці з раніше встановленим розміром, забезпечуючи таким чином правильне розміщення зашифрованих даних для подальшої обробки.

Блок запиту ключа стовпців запитує ключ шпальт, після чого цей ключ заноситься у відповідне поле. Подібні дії виконуються і блоком запиту ключа рядків, де також запитується та заноситься ключ.

Блок перестановки стовпців здійснює переміщення стовпців у таблиці відповідно до отриманого ключа, що дозволяє забезпечити необхідну криптографічну перестановку даних для забезпечення безпеки.

Блок перестановки рядків здійснює переміщення рядків у таблиці відповідно до отриманого ключа, забезпечуючи необхідну перестановку даних для подальшої обробки.

Блок подвійної перестановки вказує на завершення процесу дешифрування з використанням алгоритму подвійної перестановки та передає управління блоку передачі інформації, готуючись до наступного етапу передачі даних.

Блок передачі інформації передає вихідне повідомлення «М» одержувачу, завершуючи процес шифрування та передачі даних через канал зв'язку.

Відправник передає інформацію, яку приймач приймає за допомогою блоку прийому інформації. Щоб зашифрувати повідомлення, його необхідно розбити на окремі блоки і це завдання виконує блок розбиття інформації на блоки, що дозволяє ефективно обробляти дані в криптографічній системі.

Потім визначається розмір таблиці, яку буде внесено повідомлення, у відповідному блоці. Після цього повідомлення міститься в таблицю заздалегідь заданого розміру, щоб згодом здійснити перестановки таблиці. Перестановка виконується двічі: спочатку відбувається перестановка стовпців, потім рядків. Для здійснення перестановки необхідно створити ключі «К» – ключі рядків та стовпців. Цей процес виконується у відповідних блоках, зображених на структурній схемі.

На наступному етапі виконується перша перестановка – перестановка стовпців у таблиці. Після завершення перестановки стовпців проводиться перестановка рядків, що здійснюється у блоці перестановки рядків. Процес шифрування вважається завершеним, після чого потрібно передати зашифроване повідомлення. Передача зашифрованого повідомлення через зв'язок виконується в блоці передачі шифртексту, завершуючи процес передачі даних.

Щоб перехоплювач міг прочитати повідомлення, необхідно знати ключ «К». Цей ключ передається одержувачу окремим захищеним каналом зв'язку, забезпечуючи конфіденційність ключової інформації та захист від несанкціонованого доступу.

На стороні одержувача знаходиться блок розшифрування шифртексту Dk(C). Прийом зашифрованого тексту відбувається у блоці прийому інформації. Потім, у відповідному блоці визначається розмір таблиці. Після цього шифроване повідомлення вводиться в таблицю заздалегідь заданого розміру в блоці внесення шифртексту, де воно буде піддано подальшій обробці для відновлення вихідного повідомлення.

Для розшифрування повідомлення «С», отриманого захищеним каналом, ключ «К» додається до таблиці. Спочатку додається ключ стовпців, а потім ключ рядків. За наявності ключа можна виконати дві відповідні дії: перестановку стовпців та перестановку рядків. Ці операції реалізуються в окремих блоках. Потім розшифроване повідомлення передається в блок передачі інформації, а потім вихідне повідомлення передається одержувачу, завершуючи процес передачі та дешифрування даних.

Щоб краще зрозуміти, як працює пристрій, на рисунку 2.2 представлений алгоритм його функціонування.

Алгоритм функціонування описує послідовність наступних дій.

Спочатку відбувається прийом інформації від відправника та її поділ на інформаційні блоки. Потім визначається розмір таблиці. Якщо вихідна таблиця вже існує, інформація вноситься до неї; якщо ж вона ще не створена, процес повертається до прийому інформації для подальшої обробки.

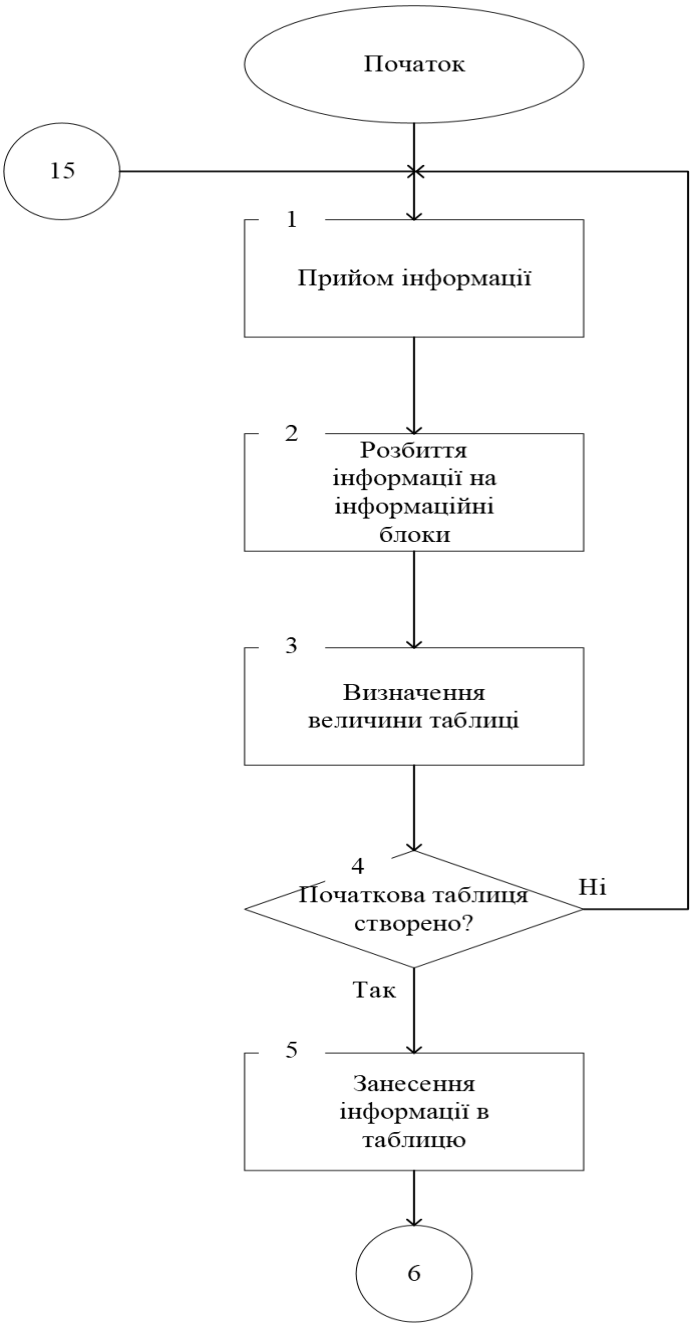
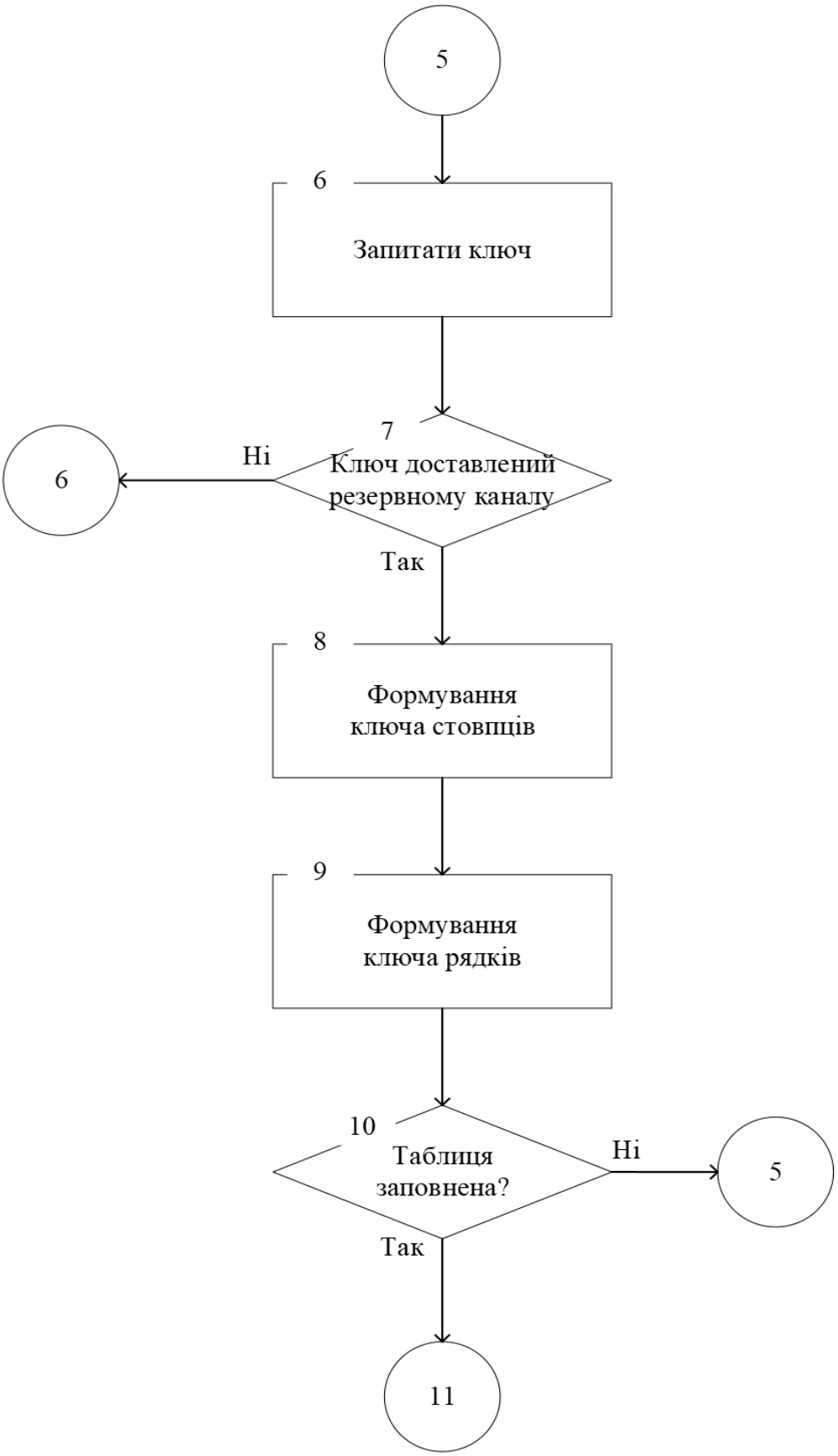


Рисунок 2.2 – Схема алгоритму функціонування пристрою



Продовження рисунку 2.2

Продовження рисунку 2.2

Після того, як інформація занесена в таблицю, запитується ключ «К». Якщо ключ було доставлено через резервний канал, відбувається формування ключів шпальт і рядків. У разі відсутності ключа «К» відбувається повернення запиту ключа. Потім відбувається перехід до умовного блоку: якщо таблицю не заповнено, відбувається повернення до блоку «Занесення інформації до таблиці». Після заповнення таблиці стовпці упорядковуються за зростанням, а рядки також упорядковуються за зростанням, гарантуючи структуроване представлення даних.

У наступному блоці демонструється шифрування через подвійну перестановку. Відбувається два етапи перестановки: спочатку проводиться перестановка рядків, та був перестановка стовпців. Останнім блоком у блок-схемі алгоритму є блок передачі інформації, де здійснюється передача зашифрованої інформації «С» через канал зв'язку, завершуючи процес обробки та передачі даних.

Останній блок перевіряє, чи є ще текст, який потребує шифрування. Якщо є, алгоритм повертається до початку і процес повторюється. Якщо ж немає, алгоритм завершується. Таким чином, весь текст буде зашифровано.

3 РОЗРОБЛЕННЯ СХЕМИ ЕЛЕКТРИЧНОЇ ПРИНЦИПОВОЇ ПРИСТРОЮ

3.1 Вибір елементної бази

Центральний процесорний модуль є центральним блоком контролера. Він забезпечує управління та синхронізацію роботи всього пристрою, забезпечує прийом, видачу, зберігання та обробку даних.

До складу центрального процесорного модуля (ЦПМ) входять процесор КР1821ВМ85А (DD1), два буферних регістра КР580ІР82 (DD2, DD3), двонаправлений шинний формувач КР580ВА86 (DD4), мультиплексор К555КП11 (DD5) (R1, C2, S).

Процесор КР1821ВМ85А має вбудований генератор тактових імпульсів та системний контролер, живиться від одного джерела +5 В. Він програмно повністю сумісний з процесором КР580ВМ80А. Процесор КР1821ВМ85А має суміщені шину даних та шину адреси. Для поділу сигналів цих шин використовуються буферні регістри. По 8-розрядній внутрішній шині вхідні та вихідні дані вводяться всередину пристрою. Вони можуть надходити з внутрішньої шини даних у наступні частини МП:

- 8-розрядний акумудятор;
- Регістр тимчасового зберігання;
- індикатори;
- Регістр команд;
- пристрій керування;
- якийсь із регістрів загального призначення (B, C, D, E, H, L);
- 16-розрядний покажчик стека;
- 16-розрядний лічильник команд;
- 8-розрядний буфер адреси/даних.

Арифметико-логічний пристрій завантажується двома 8-розрядними регістрами (акумулятором та регістром тимчасового зберігання), як у типовому МП.

Регістр станів містить п'ять індикаторів стану замість двох, як це було у типовому МП.

Регістр команд пов'язаний з дешифратором, який визначає поточну команду, необхідну мікропрограму або наступний машинний цикл, а потім інформує схему керування та синхронізацію про послідовність дій. Ця схема координує дії МП та периферії.

Поява у першому такті машинного циклу на шині A15-A8 старшого байта адреси, але в шині AD7-AD0 – молодшого, стробується сигналом процесора ALE, що використовується дозволу записи в регістри. Під час передачі по шині AD7-AD0 даних цей сигнал відсутній. Таким чином, у регістрах буде записано адресу, а дані будуть передаватися через формувач шини. До того ж, регістри та шинний формувач виконують функцію збільшення здатності навантаження ЦПМ (32 мА/висновок).

Мультиплексор два на один перетворює сигнали процесора на сигнали читання/запису пам'яті та зовнішніх пристроїв – MEMR, MEMW, I/OR, I/OW.

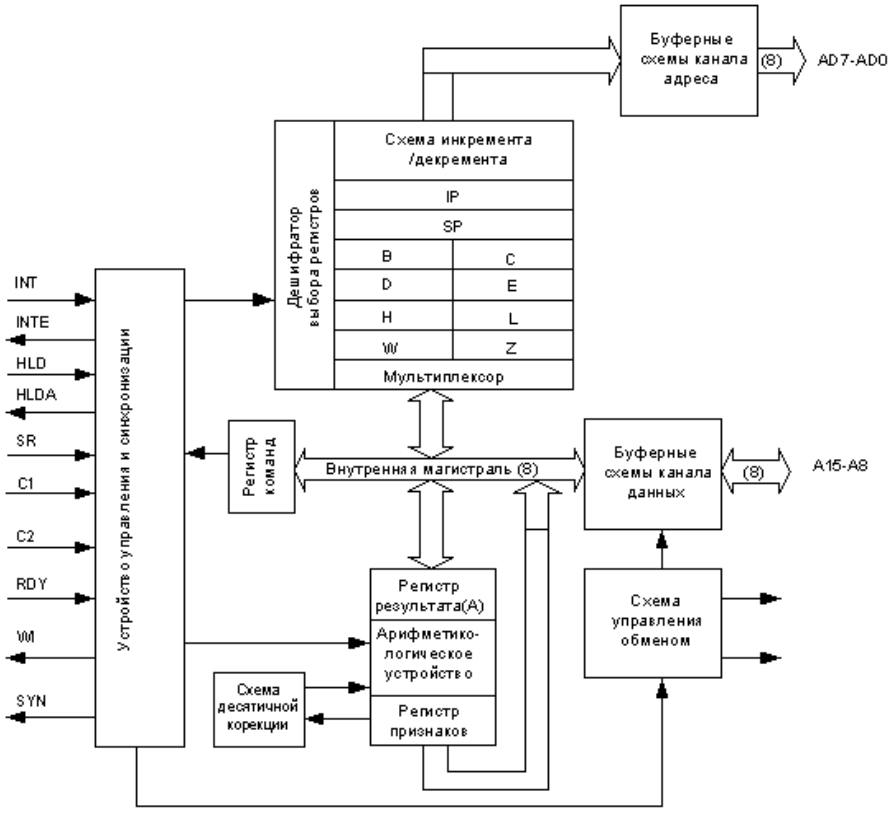


Рисунок 3.1 – Структурна схема КР1821ВМ85А

Для стабілізації частоти системного генератора висновків X1 і X2 МП БІС підключають кварцовий резонатор з номінальною частотою 6 МГц. Тривалість машинного такту при цьому дорівнюватиме 4 мкс. Підстроювальний конденсатор C1 використовується регулювання частоти системного генератора в невеликих межах.

Ланцюжок R1C2 служить для короткочасного формування імпульсу з негативним фронтом переднім з тривалістю мінімум 1,5 мкс. Приймемо постійну часу ланцюжка τ R1C1 за 10мкс. У цьому R1 = 10 кОм, а C1 = 1000 пФ. Принцип роботи схеми формування імпульсу скидання ось у чому. У нормальному стані конденсатор C2 заряджений і вхід МП БІС $\overline{RESI}$ через резистор R1 з'єднаний з джерелом +5В, що зумовлює логічну одиницю. При замиканні контактів перемикача S конденсатор C2 розряджається на корпус, а після розмикання контактів починається його розрядка, вхід МП БІС $\overline{RESI}$ виявляється замкненим на корпус, що відповідає стану логічного нуля. Після закінчення зарядки на вході $\overline{RESI}$ знову встановлюється рівень, що відповідає логічній одиниці. Подібні процеси відбуваються після подачі харчування на мікроконтролер.

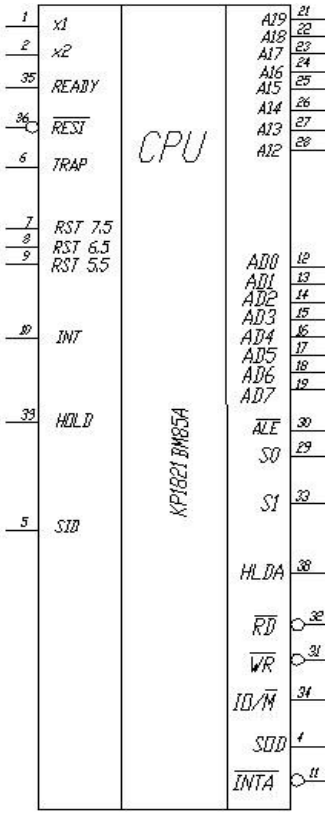


Рисунок 3.2 – Мікропроцесор КР1821ВМ85А

Восьмирозрядний арифметико-логічний пристрій мікропроцесора забезпечує виконання арифметичних та логічних операцій над двійковими даними, представлені в додатковому коді, а також обробку двійково-десяткових упакованих чисел.

До складу блоку регістрів входять 16-розрядний регістр адреси команди (IP), 16-розрядний регістр покажчика стека (SP), 16-розрядний регістр тимчасового зберігання (WZ), 16-розрядна схема інкременту декременту та шість 8-розрядних регістрів загального призначення (B, C, D, E, H, L), які можуть використовуватися і як три 16-розрядні регістри (BC, DE, HL).

МП КР1821ВМ85А використовує п'ять способів адресації:

- неявна - команда STC (відновити індикатор перенесення) відноситься виключно до вказаного індикатора і ні до чого більше;

- Регістрова - операція та джерело операнда точно визначені, команди дуже ефективні, тому що використовують тільки один байт пам'яті, і швидко здійсненні, тому що не використовують операцію вилучення даних з пам'яті;

- безпосередня – використовує команди, якими дані йдуть безпосередньо за КОП;

- Пряма - описується трибайтовим форматом команд: Перший - КОП, другий;

- МБ (молодший байт), третій - СБ (старший байт);

- Непряма реєстрова - команди звертаються на згадку, використовуючи пару регістрів для вказівки на адресу операнда.

Додатково є комбінований спосіб, який використовує поєднання різних способів адресації.

Таблиця 3.1 - Основні електричні параметри мікропроцесора

Параметр	Позначення	Значення параметрів [макс (хв)]
Напруга живлення, В	Ucc	5,25 (4,75)
Вхідна напруга низького рівня, В	Uii	0,8
Вхідна напруга високого рівня, В	Uiн	(2,0)
Вихідна напруга низького рівня, В	Uoi	0,45
Вихідна напруга високого рівня, В	Uoн	(2,4)

Продовження таблиці 3.1

Вихідний струм низького рівня, мА	Ioi	2,2
Вихідний струм високого рівня, мА	Ioн	-0,4
Струм витоку на входах, мкА	Iii	±10
Струм витоку на входах/виходах, мкА	Ioz	±10
Ємність навантаження, пФ	Ci	100
Місткість на входах, пФ	Ci	10
Місткість на входах/виходах, пФ	Co	20

Мікропроцесор виконує команди по машинним циклам. Число циклів необхідне виконання команди залежить від її типу і може бути від одного до п'яти.

Машинні цикли виконуються за машинними тактами. Число тактів у циклі визначається кодом виконуваної команди і може бути від трьох до п'яти. Тривалість такту дорівнює періоду тактової частоти і за частоті 20 МГц становить 500нс.

Таблиця 3.2 – Призначення виводів мікропроцесора

Вивід	Позначення	Тип виводу	Функціональне призначення виводів
1, 25-27, 29-40	A10, A0-A2, A3-A9, A15, A12-A14, A11	Виходи	Канал адреси
2	GND	-	Загальний
3-10	D4-D7, D3-D0,	Входи / виходи	Канал даних
11	Uio		Напруга джерела зміщення – 5В
12	SR	Вхід	Встановлення у вихідний стан
13	HLD	Вхід	Захоплення
14	INT	Вхід	Запит переривання
15, 22	C2, C1	Входи	Тактові сигнали

Продовження таблиці 3.2

16	INTE	Вихід	Дозвіл переривання
17	RC	Вихід	Прийом інформації
18	TR	Вихід	Видача інформації
19	SYN	Вихід	Сигнал синхронізації
20	Ucc1	-	Напруга живлення +5В
21	HLDA	Вихід	Підтвердження захоплення
23	RDY	Вхід	Сигнал "Готовність"
24	WI	Вихід	Сигнал "Чекання"
28	Ucc2	-	Напруга живлення +12В

МП КР1821ВМ85А має наступні групи команд:

- група передачі – призначена передачі даних між регістрами чи пам'яттю і регістрами;

- група арифметична – виконує операції складання, віднімання, інкременту, декременту над даними у регістрах чи пам'яті;

- група логічна - виконує операції І, АБО, АБО ВИКЛЮЧНЕ, порівняння, переміщення та інвертування даних у регістрах або між даними в пам'яті та регістрі;

- група розгалуження – викликає розгалуження (переходи) умовні чи безумовні, виклики, повернення та повторні запуски;

- група стека, ВР та машинного управління – розуміє команди операцій зі стеком, зчитування в портах введення, записи в порти виведення, ініціалізації та зчитування маскованих переривань та встановлення та скидання індикаторів.

Мікросхема КР580ВА86 - двонаправлений 8-розрядний шинний формувач, призначений для обміну даними між мікропроцесором та системною шиною; має підвищену здатність навантаження.

Мікросхема КР580ВА86 - формується без інверсії та з трьома станами на виході.

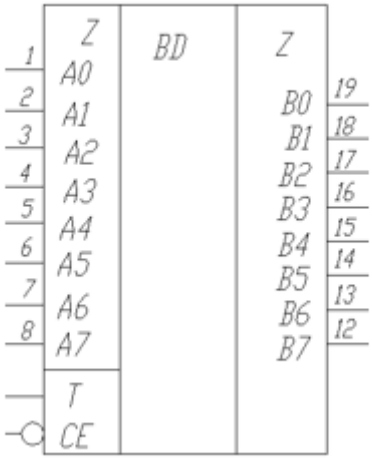


Рисунок 3.3 – Шинний формувач КР580ВА86

Для 16-розрядної шини даних слід підключати дві мікросхеми КР580ВА86 або КР580ВА87.

Кожна мікросхема складається з восьми однакових функціональних блоків та схеми управління.

Блок містить підсилювача – формувача. За допомогою схеми управління виробляється дозвіл передачі (керування 3-м станом виходу) та вибір напряму передачі даних.

Залежно стану керуючих сигналів ОЕ і Т мікросхеми можуть працювати у режимі передачі А->В, В; В, В ->А або в режимі вимкнено:

при ОЕ = 0, Т = 1 - напрямок передачі А-> В, В;

при ОЕ = 0, Т = 0 - напрямок передачі В, В ->А;

при ОЕ = 0, Т = Х - на виході А, В, В - третій стан, де Х - байдужий стан.

Таблиця 3.3 – Призначення виводів КР580ВА86

Вивід	Позначення	Виводи	Функціональне призначення виводів
1-8	А0-А7	Вхід / вихід	Інформаційна шина
9	ОЕ	Вхід	Дозвіл передачі (управління 3-м станом)
10	GND	-	Загальний

Продовження таблиці 3.3

11	T	Вхід	Вибір напряму передачі
12-19	B7-B0	Вихід / вхід	Інформаційна шина
20	Ucc	-	Напруга живлення +5В

Для зберігання констант, проміжних даних, коду програми, що управляє, результатів обчислень необхідна пам'ять. До складу блоку пам'яті в проектованому пристрої входить постійне запам'ятовуючий пристрій (ПЗП) і оперативний пристрій (ОЗУ). У ПЗП (DD6) зберігатиметься код програми, в ОЗП (DD7) – вхідні змінні, проміжні дані, результат обчислень. Для поставленого завдання підійде ПЗУ КР573РФ5 об'ємом 2 кбайт та статичне ОЗУ КР537РУ10 об'ємом 2 кбайт. Застосування ОЗУ статичного типу дозволяє вирішити завдання збереження даних у пам'яті – на відміну динамічного ОЗУ статичне вимагає циклів регенерації пам'яті. Це дозволяє значно спростити апаратну частину контролера.

Для розділення області ПЗП та ОЗП необхідно дешифрувати верхні розряди адреси. Після подачі сигналу скидання на процесор лічильник команд приймає значення 0, тобто виконання програми починається з адреси 0. Отже область ПЗП, в якому зберігається код програми, повинна починатися з адреси 0. Тоді верхня адреса ПЗП 2 кбайт буде дорівнює 2047 (7ffH) що відповідає двійковому 00000111111111111. Область ОЗУ слід відразу ж за ПЗП. Нижня адреса ОЗУ в цьому випадку 2048 (0800H), тобто 0000100000000000. Верхня межа в 2 кбайт відповідає адресою 4095 (0fffH), тобто 0000111111111111. Як видно, для адресації до 1А1 тільки02. При цьому біти А15-А12 приймають значення 0 як ПЗП, так і для ОЗУ, а біт А11 приймає значення 0 для ПЗП і 1 для ОЗУ. Цю обставину і застосовуємо для побудови селектора, що розділяє області ПЗП та ОЗП. Також слід врахувати, що при зверненні до пам'яті ЦПМ встановлює 0 сигнали MEMW або MEMR, а для звернення до ПЗП можливо тільки при читанні даних, але не при їх запису. Сигнали з селектора мають активний рівень 0 і підключені до входів вибірки кристала CS та переведення виходів у Z-стан ОЕ мікросхем ОЗУ та ПЗП. Висновки мікросхем об'єднані у загальну шину даних відповідними розрядами та підключаються до ЦПМ.

Таблиця 3.4 - Карта пам'яті

			Розряди шини адреси															
			15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
ПЗУ (2 кбайт)	min	0H	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	max	7ffH	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1
ОЗУ (2 кбайт)	min	800H	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
	max	0fffH	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1

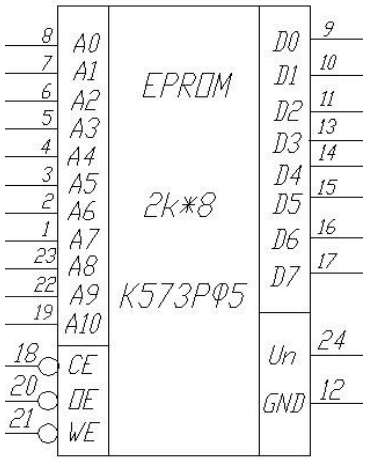


Рисунок 3.4 - Позначення мікросхеми К573РФ5

Таблиця 3.5 – Призначення сигналів ROM

Номер виводу	Позначення	Тип виводу	Призначення виводу
1-7, 15-17	A0-A9	Вхід	адресні входи
11-14	D0-D3	Виходи	дані (підключаються до ШД0-ШД7)
18	Uживл	Вхід	живлення +5В
9	GND	Виходи	загальний
8	CS	Вхід	вибір мікросхеми
10	WR	Вхід	запис/читання

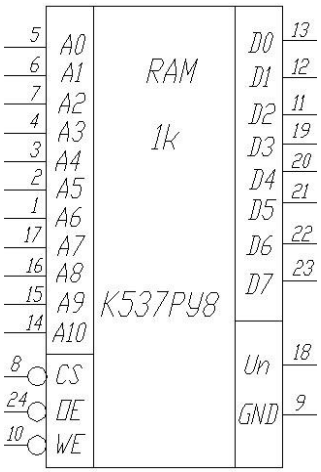


Рисунок 3.5 - Позначення мікросхеми К537РУ8

Таблиця 3.6 – Призначення сигналів RAM

Номер виводу	Позначення	Тип виводу	Призначення виводу
1-8,23, 33,19	A0-A9	Вхід	Адресні входи
9-16	D0-D3	Виходи	Дані (підключаються до ШД0-ШД7)
4	Uживл	Вхід	Живлення +5В
17	CS	Вхід	Вибір мікросхеми
18	WR	Виходи	Запис/читання

Для управління зовнішніми пристроями та введення/виведення інформації необхідна мікросхема інтерфейсу КР580ВВ55 (DD8). Ця мікросхема складається з 3-х 8-ми розрядних портів введення/виводу РА, РВ, РС, причому порт РС може працювати в режимі 2-х незалежних 4-х розрядних портів. Призначення висновків:

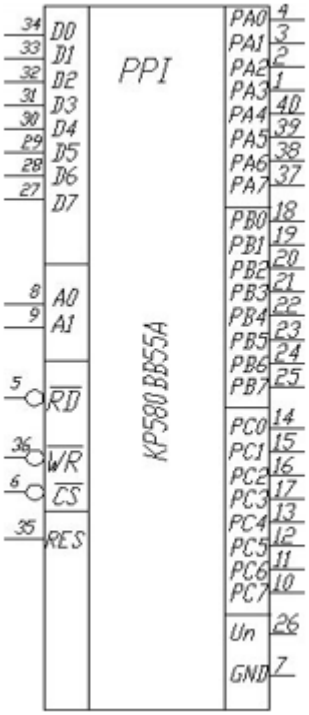


Рисунок 3.6 - Програмований пристрій введення/виводу КР580ВВ55А

Обмін інформацією між магістраллю даних здійснюється через 8-розрядний двонаправлений тристабільний канал даних (D).

Для зв'язку з периферійними пристроями використовується 24 лінії введення/виводу, згруповані в три 8-розрядних канали ВА, ВР, ВС, напрямок передачі визначаються програмним способом.

Режим 0: забезпечується можливість синхронної програмно керованої передачі даних через два незалежні 8-розрядні канали ВА і ВР і два 4-розрядні канали ВС.

Режим 1: забезпечується можливість введення або виведення інформації з периферійного пристрою через два незалежні 8-розрядні канали ВА та ВР за сигналом квитування.

Режим 2: забезпечується можливість обміну інформації з периферійними пристроями через двонаправлений 8-розрядний канал ВА сигналом квитування.

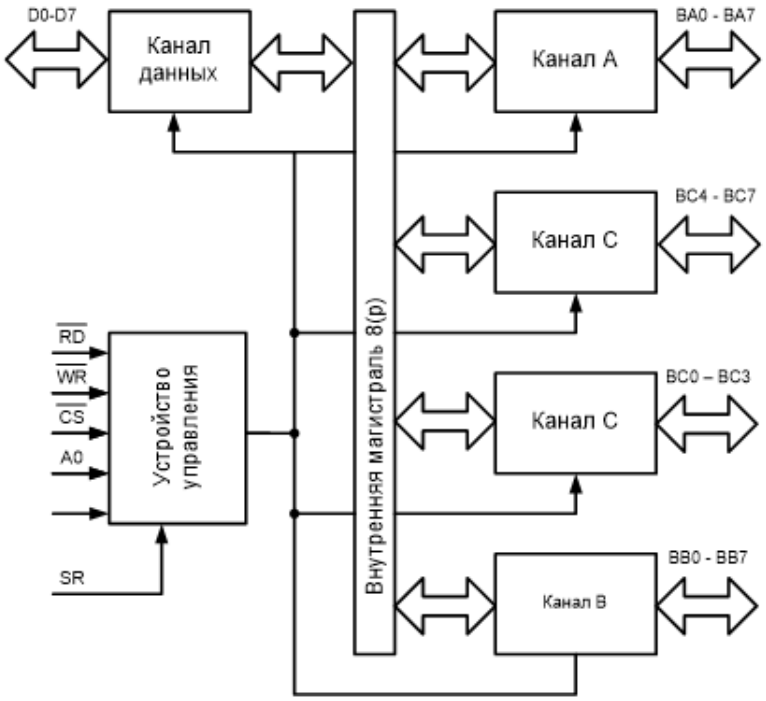


Рисунок 3.7 – Структурна схема КР580ВВ55А

Таблиця 3.7 – Призначення виводів КР580ВВ55А

Вивід	Позначення	Тип виводу	Функціональне призначення виводів
1-4, 37-40	ВА3-ВА0, ВА7-ВА4	Входи / виходи	Інформаційний канал А
5	RD	Вхід	Читання інформації
6	CS	Вхід	Вибір мікросхеми
7	GND	-	Загальний
8,9	A1, A0	Вхід	Молодші розряди адреси
10-17	ВС7-ВС4, ВС0-ВС3	Входи / виходи	Інформаційний канал В
18-25	ВВ0-ВВ7	Входи / виходи	Інформаційний канал С
26	Ucc	-	Напруга живлення +5В
27-34	D7-D0	Входи / виходи	Канал даних
35	SR	Вхід	Встановлення у вихідний стан
36	WR	Вхід	Запис інформації

Для введення інформації використовується послідовний інтерфейс КР580ВВ51. Мікросхема КР580ВВ51А - універсально - асинхронний приймач (УСАПП), призначений для апаратної реалізації послідовного протоколу обміну між мікропроцесором КР580ВМ80А (КМ1810ВМ86) або іншим пристроєм, здатні запрограмувати дану мікросхему на необхідний режим.

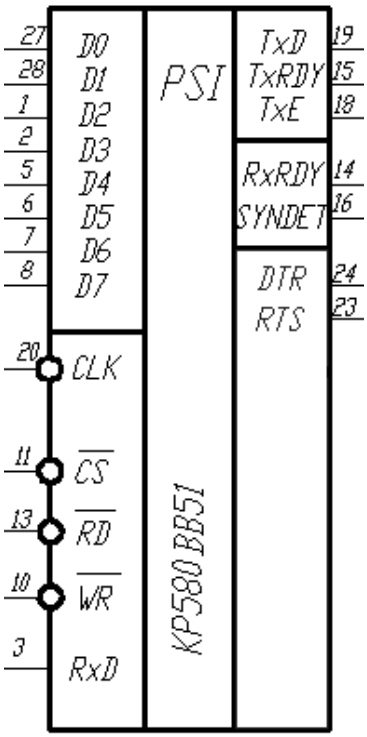


Рисунок 3.8 – Мікросхема КР580ВВ51

Мікросхема УСАПП перетворює паралельний код, що отримується від центрального процесора, у послідовний потік символів зі службовими бітами і видає цей потік у послідовний канал зв'язку з різною швидкістю, а також виконує зворотне перетворення: послідовний потік символів у паралельний 8-розрядне слово.

Максимальна швидкість передачі/прийому інформації послідовним каналом 64К бод, мінімальна не обмежена і визначається зовнішніми пристроями (ВУ).

Мікросхема може працювати в синхронному та асинхронному режимах.

Синхронний режим характеризується безперервним потоком інформації, що передається (приймається). Для встановлення синхронізації між передавачем

(передавачем) мікросхеми КР580ВВ51А та приймачем (передавачем) зовнішнього пристрою та виділення з послідовного потоку символів корисної інформації вводиться кодуючі слова (синхросимволи). Інформаційна (5-8 біт) та тимчасова довжина синхросимволу та слова даних рівні.

Асинхронний режим характеризується одиночними посилками інформації, ініціалізація яких визначається або процесором системи, або зовнішнім пристроєм.

Таблиця 3.8 - Призначення виводів КР580ВВ51

Вивід	Позначення	Тип виводу	Функціональне призначення виводу
1, 2, 5-8, 27, 28	D2-D7, D0, D1	Входи / виходи	Канал даних - обмін інформацією між мікропроцесором та мікросхемою
3	RxD	Вхід	Приймач мікросхеми
4	GND	-	Загальний
9	TxC	Вхід	Синхронізація передачі
10	WR	Вхід	Запис інформації
11	CS	Вхід	Вибір мікросхеми
12	CO/D	Вхід	Управління (дані)
13	RD	Вхід	Читання інформації
14	RxRDY	Вихід	Готовність приймача
15	TxRDY	Вихід	Готовність передавача
16	SYNDET/BD	Вхід / Вихід	Двонаправлений трьох - стабільне програмоване введення/виведення
17	CTS	Вхід	Готовність зовнішнього пристрою прийняти дані
18	TxEND	Вихід	Кінець передачі
19	TxD	Вихід	Передавач мікросхеми
20	C	Вхід	Синхронізація
21	SR	Вхід	Встановлення вихідного стану
22	DSR	Вхід	Готовність зовнішнього пристрою передати дані

Продовження таблиці 3.8

23	RTS	Вихід	Запит приймача зовнішнього пристрою на прийом даних
24	DTR	Вихід	Запит передавача зовнішнього пристрою на прийом даних
25	RxC	Вхід	Синхронізація прийому
26	Ucc	-	Напруга живлення +5В

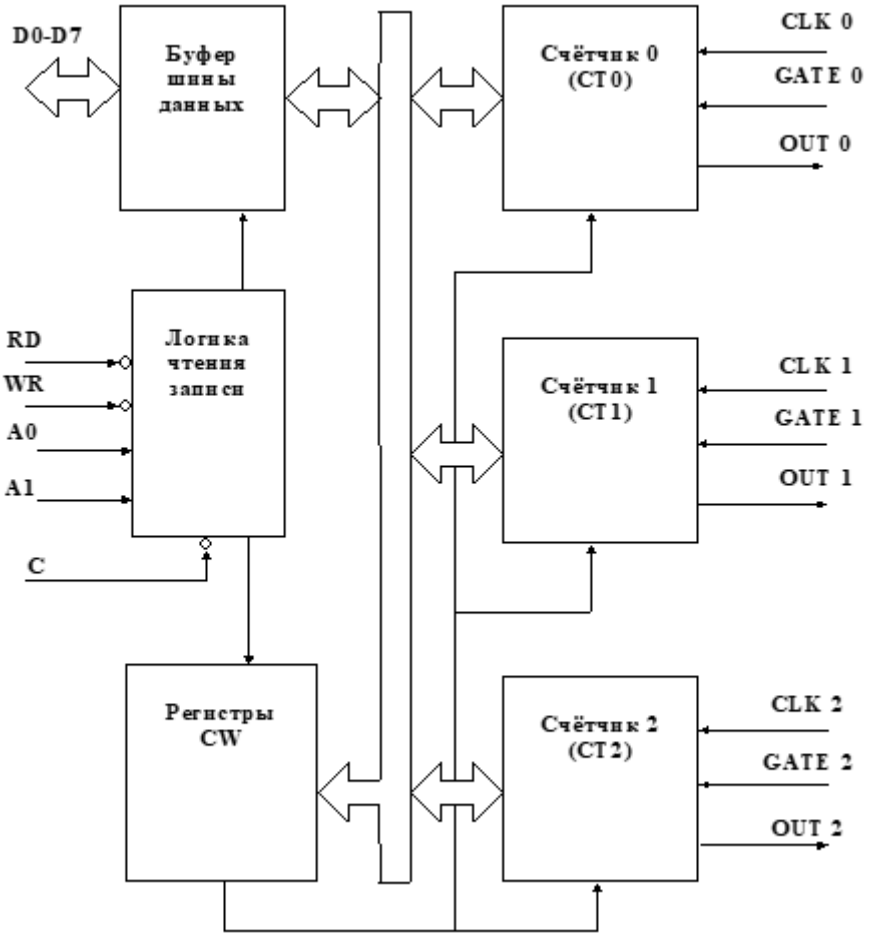


Рисунок 3.9 – Структурна схема КР580ВІ53

Програмований інтервальний таймер КР580ВІ53 є функціонально закінченим однокристальним периферійним пристроєм типу, що вбудовується, і вирішує одну з найбільш важливих проблем будь-якої мікропроцесорної системи - генерацію точних часових інтервалів під програмним контролем.

Структурну схему таймера КР580ВІ53 наведено на рис. 3.9. До складу БІС входять три канали, основу яких складають 16-розрядні лічильники, що віднімають (СТ0, СТ1 і СТ2) з частотою рахунку по входу CLK до 2 МГц. Кожен канал ПІТ може працювати незалежно від інших в одному із шести програмно заданих режимів. Лічильники каналів програмно доступні для запису та читання і можуть працювати як у двійковому, так і в двійково-десятковому коді. Управління режимами здійснюється за допомогою керуючих слів CW, які визначають режим роботи таймера, код рахунку (двійковий або двійково-десятковий) та формат обміну даними з МП під час операцій з лічильниками.

Зв'язок таймера з МПС здійснюється через двонаправлену восьмирозрядну шину даних D0-D7 під керуванням п'яти сигналів A0, A1, CS, RD та WR. При двобайтовому форматі даних операція з лічильниками виконується двічі: спочатку записується (зчитується) молодший байт, потім старший. Обслуговування СТ виконується паралельно незалежно один від одного. При подачі живлення на БІС стану регістрів лічильників та режими роботи не визначені, тому перед початком роботи кожен канал таймера має бути ініціалізований індивідуально посилкою відповідного слова стану CW.

Мікросхема КР580ІР82 – 8-розрядні адресні регістри, призначені для зв'язку мікропроцесора з системною шиною; мають підвищену навантажувальну здатність. Мікросхеми КР580ІР82 8-розрядний D-реєстр засувка без інверсії та з трьома станами на виході.

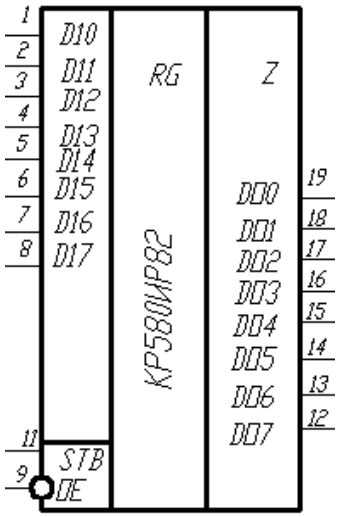


Рисунок 3.10 – Адресний регістр КР580ІР82

Кожна мікросхема складається з восьми однакових функціональних блоків та схеми управління. Блок містить D-регістр засувку та потужний вихідний вентиль без інверсії або з інверсією. За допомогою схеми управління проводиться стробування інформації, що записується, і управління третім станом потужних вихідних вентилів.

Залежно від стану стробуючого сигналу мікросхеми можуть працювати у двох режимах: у режимі шинного формувача та в режимі зберігання.

Таблиця 3.9 – Призначення виводів мікросхеми КР580ІР82

Вивід	Позначення	Тип виводу	Функціональне призначення виводів
1-8	D0-D7	Вхід	Інформаційна шина
9	OE	Вхід	Дозвіл передачі (управління 3-м станом)
10	GND	-	Загальний
11	STB	Вхід	Стробуючий сигнал
12-19	Q7-Q0	Вихід	Інформаційна шина
20	Ucc	-	Напруга живлення +5В

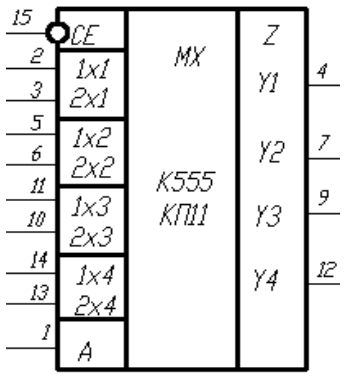


Рисунок 3.11 – Мультиплекс К555КП11

Мікросхема К555КП11 - чотири двовхідні мультиплексори із загальним управлінням і можливістю переведення виходів у високоімпедансний стан. При балку. 0 на адресному вході на вихід кожного мультиплексора проходить сигнал

зі входу D0, при лог. 1-з входу D1. Виходи мікросхеми активні за лог. 0 на вході ЕО. Подача лог 1 на вхід ЕО переводить виходи у високоімпедансний стан.

Таблиця 3.10 – Електричні параметри мікросхеми К555КП11

Uжив., ном., В	5
U0вих., не більше, В	0.48
U1вих., не більше, В	2.5
I0вх., не більше, мА	-0.76
I1вх., не більше, мА	0.02
I0пот., не більше, мА	13.6
I1пот., не більше, мА	9.7
t1.0зд.р., не більше, нс	21
t0.1зд.р., не більше, нс	18

Таблиця 3.11 - Призначення виводів мікросхеми К555КП11

1	Вхід адреси даних S
2	Вхід даних I 1a
3	Вхід даних I2a
4	Вихід даних Ya
5	Вхід даних I1b
6	Вхід даних I2b
7	Вихід даних Yb
8	GND
9	Вихід даних Yc
10	Вхід даних I1c
11	Вхід даних I2c
12	Вихід даних Yd
13	Вхід даних I1d
14	Вхід даних I2d
15	Вхід дозволу трансляції даних на виходи /E0
16	“+” живлення

Мікросхема КР580ВН59-програмований контролер переривань, обслуговує до восьми запитів на переривання мікропроцесора, що надходять від зовнішніх пристроїв.

Мікропроцесор дозволяє скоротити засоби програмного забезпечення та реальні витрати часу за пріоритетів переривань у системах з пріоритетами багатьох рівнів. Алгоритм завдання пріоритету встановлюється програмним шляхом. Пріоритети, що закріплені за зовнішніми пристроями, можуть бути змінені в процесі виконання програм.

У мікросхемі передбачено можливість розширення числа каскадного з'єднання мікросхем ПКП.

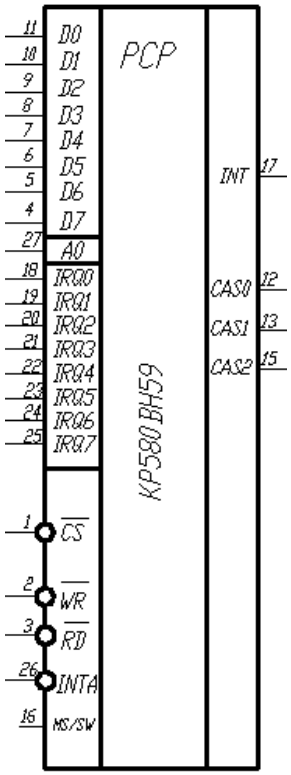


Рисунок 3.12 – Програмований контролер переривань КР580ВН59

Таблиця 3.12 - Призначення виводів мікросхеми КР580ВН59

Вивід	Позначення	Тип виводу	Функціональне призначення виводів
1	CS	Вхід	Вибір мікросхеми
2	WR	Вхід	Запис інформації

Продовження таблиці 3.12

3	RD	Вхід	Читання інформації
4-11	D7-D0	Входи / виходи	Канал даних
12, 13, 15	CFS2-CAS0	Входи / виходи	Шина каскадування
14	GND	-	Загальний
17	INT	Вихід	Переривання
18-25	IRQ7-IRQ0	Вхід	Запит переривання
26	INTA	Вхід	Підтвердження переривання
27	A0	Вхід	Адреса 0-го розряду
28	Ucc	-	Напруга живлення

Для з'єднання з індикаторами використовуємо буферний регістр К555ІР22. Мікросхема є восьмирозрядним регістром з умощенними виходами для управління великим ємнісним або низькоомним навантаженням і може бути використана як магістральний формувач. Базовий елемент мікросхеми - D-тригтер спроектований за типом прохідної клямки, що дозволяє при високому рівні на вході стробування проходити вхідному сигналу на вихід минаючи тригер.

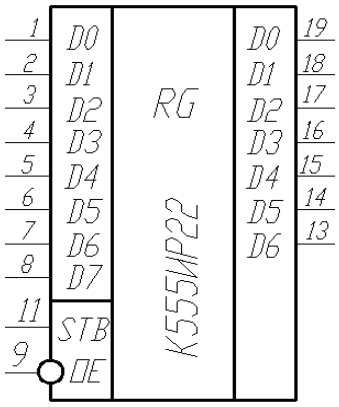


Рисунок 3.13 – Реєстр К555ІР2

Для виведення ключа використовуватиметься індикатор КІПЦ01. Він являє собою інтегральну мікросхему зі світлодіодних структур та необхідних електричних з'єднань. Це однорозрядний семисегментний цифро-літерний індикатор.

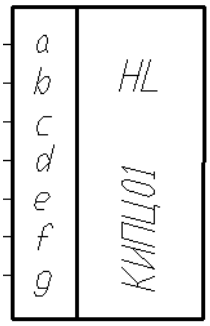


Рисунок 3.14 – Індикатор КІПЦ01

Колір свічення – червоний.

Сила світла – 1 мкд.

Постійний прямий струм – 20 мА.

Розкид сили світла між елементами – 3.

Максимально допустимий прямий струм – 25 мА.

Потужність розсіювання – 700 мВт.

Корпус – пластмасовий.

Для забезпечення повноцінної роботи пристрою необхідно використовувати 14 програм.

Наведемо розрахунок для максимальної кількості команд Командна система буде містити 75 команд, з яких:

- 25 однобайтних команд;
- 30 двобайтних команд;
- 20 трьох байтних команд.

Відомо, що однобайтні команди виконуються за 2 машинні цикли (МЦ), тоді:

$$25x2 = 50 \text{ МЦ}; \quad (3.1)$$

Відомо, що двобайтні команди виконуються за 3 машинні цикли (МЦ), тоді:

$$60x3 = 180 \text{ МЦ}; \quad (3.2)$$

Відомо, що трибайтні команди виконуються за 4 машинні цикли (МЦ), тоді:

$$60x4 = 240 \text{ МЦ}; \quad (3.3)$$

Розрахуємо загальну кількість машинних циклів (МЦ):

$$50 + 180 + 240 = 470 \text{ МЦ}; \quad (3.4)$$

Розрахуємо кількість машинних тактів (МТ):

$$N_{МТ} = 470 \times 4 = 1880 \text{ МТ}; \quad (3.5)$$

З умови відомо, що час виконання підпрограм дорівнює 1 мс.

Тому розрахуємо час машинних тактів:

$$t_{МТ} = \frac{1мс}{\text{N}_{\text{МТ}}} = \frac{1мс}{1880МТ} = 5{,}32 \text{ x } 10^{-7}; \quad (3.6)$$

Загальна пам'ять, яка потрібна для реалізації всіх команд, дорівнює:

$$(1x25) + (2x30) + (3x20) = 145 \text{ байт}; \quad (3.7)$$

Оскільки всіх програм 14 , то загальна ємність пам'яті, яка необхідна реалізації цих програм дорівнюватиме:

$$145x14 = 2030 \text{ байт} = 2 \text{ кБ}; \quad (3.8)$$

Розрядність адресної шини розрахуємо за такою формулою:

$$|A| = \log_2 2030 = 3,3 \quad (3.9)$$

Частоту мікропроцесора визначаємо за такою формулою:

$$f = 1/5,32 \times 10^{-7} = 1,88 \text{ МГц}; \quad (3.10)$$

Наведемо розрахунок для мінімальної кількості використовуваних команд

Командна система буде містити 45 команд, з яких:

- 10 однобайтних команд;
- 20 двобайтних команд;
- 15 трьох байтних команд.

Відомо, що однобайтні команди виконуються за 2 машинні цикли (МЦ), тоді:

$$10x2 = 20 \text{ МЦ}; \quad (3.11)$$

Відомо, що двобайтні команди виконуються за 3 машинні цикли (МЦ), тоді:

$$40x3 = 120 \text{ МЦ}; \quad (3.12)$$

Відомо, що трибайтні команди виконуються за 4 машинні цикли (МЦ), тоді:

$$45x4 = 180 \text{ МЦ}; \quad (3.13)$$

Розрахуємо загальну кількість машинних циклів (МЦ):

$$20 + 120 + 180 = 320 \text{ МЦ}; \quad (3.14)$$

Розрахуємо кількість машинних тактів (МТ):

$$N_{MT} = 320 \times 4 = 1280 \text{ МТ; (3.15)}$$

З умови відомо, що час виконання підпрограм дорівнює 1 мс.

Тому розрахуємо час машинних тактів:

$$t_{MT} = \frac{1мс}{\text{N}_{\text{МТ}}} = \frac{1мс}{1280MT} = 0{,}78 \text{ x } 10^{-6}\text{; (3.16)}$$

Загальна пам'ять, яка потрібна для реалізації всіх команд, дорівнює:

$$(1\text{x}10) + (2\text{x}20) + (3\text{x}15) = 85 \text{ байт; (3.17)}$$

Оскільки всіх програм 14 , то загальна ємність пам'яті, яка потрібна для реалізації цих програм дорівнюватиме:

$$85\text{x}14 = 1190 \text{ байт} = 1{,}2 \text{ кБ; (3.18)}$$

Розрядність адресної шини розрахуємо за такою формулою:

$$|A| = \log_2 1190 = 3{,}1\text{; (3.19)}$$

Частоту мікропроцесора визначаємо за такою формулою:

$$f = 1/0{,}78 \text{ x}10^{-6} = 1{,}3 \text{ МГц; (3.20)}$$

Зробивши розрахунки таких параметрів як пам'ять, частота процесора та адресної шини, можна зробити висновок, що наш мікропроцесор повинен мати частоту не менше 1.9 МГц. Адресна шина має мінімальну розрядність 4. Пам'ять, яка необхідна для реалізації всіх програм у нашому пристрої повинна бути не менше 2 кБ.

Розрахунок генератора імпульсу двох інверторах. Схема генератора наведено на рис. 3.15.

Резистор R4 є обмежувальним, і його опір не повинен бути меншим за 1 кОм, а щоб він не впливав на розрахункову частоту, номінал резистора R5 вибираємо значно більше R4

На програмований таймер ВІ53 необхідно подати частоту 19200 Гц.

$$T = \frac{1}{f} = \frac{1}{19200} = 5{,}2 * 10^{-5}\,\text{с}; \quad (3.21)$$

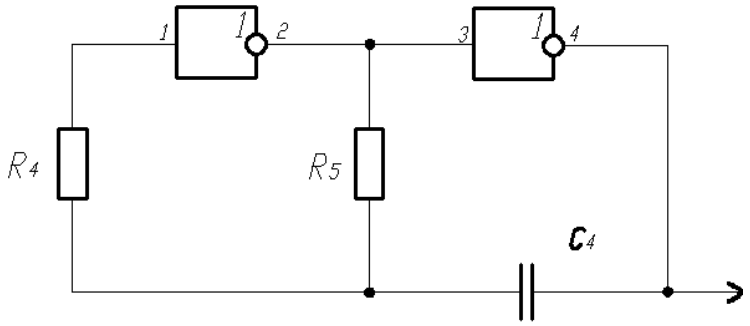


Рисунок 3.15 – Тактовий генератор

Повний період складає $T = 1{,}4 R_5 C_4$. Резистор R_5 та конденсатор C_4 можуть бути в діапазоні 20 кОм…10МОм, 300 пф…100 мкФ.

Вибираємо резистор R_5 типу МЛТ-0,25-20кОм± 10%, тоді:

$$C_4 = \frac{T}{R_5 * 1{,}4} = \frac{5{,}2 * 10^{-5}}{20 * 10^3 * 1{,}4} = 20 n\Phi; \quad (3.22)$$

Вибираємо конденсатор C типу К10-17-1б-2,2пФ± 10%.

Номінал резистора R_4 визначимо за такою формулою:

$$R_4 = 0{,}005 * R_5 = 100 Ом; \quad (3.23)$$

Вибираємо резистор R_4 типу МЛТ-0,25-100 Ом± 10%.

3.2 Розроблення програмного забезпечення пристрою

Мікропроцесор КР1821ВМ85А, розроблений у Радянському Союзі, є аналогом американського мікропроцесора Intel 8085. Це 8-бітний процесор з набором команд, орієнтованим на обробку даних та управління зовнішніми пристроями.

Програма на мікропроцесорі КР1821ВМ85А буде написана на асемблері, і вона буде виконувати просте завдання — миготіти світлодіодом, підключеним до одного з портів вводу-виводу. Ця програма демонструє основні операції з регістрами, порушеннями і командами управління.

Програма

```
; Програма для мікропроцесора КР1821ВМ85А (Intel 8085)
; Миготіння світлодіодом, підключеним до порту вводу-виводу

ORG 0000H        ; Початкова адреса програми
START:  MVI A, 55H    ; Завантажуємо значення 55H у регістр A
        OUT 01H     ; Виводимо значення A у порт 01H (запалюємо світлодіод)
        CALL DELAY   ; Викликаємо процедуру затримки
        MVI A, 00H   ; Завантажуємо значення 00H у регістр A
        OUT 01H      ; Виводимо значення A у порт 01H (гасимо світлодіод)
        CALL DELAY   ; Викликаємо процедуру затримки
        JMP START    ; Повертаємося до початку програми

DELAY:  LXI D, 0FFFFH ; Завантажуємо в регістр D пару значень FFFFH
DELAY_LOOP: DCX D     ; Зменшуємо значення в регістрі DE
        MOV A, D      ; Перевіряємо, чи D стало 0
        ORA E         ; або E стало 0
        JNZ DELAY_LOOP; Якщо ні, повторюємо цикл
```

```
        RET         ; Повертаємося з підпрограми
```

Пояснення

1. ORG 0000H: Вказує на початкову адресу програми.
2. MVI A, 55H: Завантажує значення 55H (яке еквівалентне 01010101 в двійковій системі) у регістр A.
3. OUT 01H: Виводить значення з регістру A в порт 01H, до якого підключений світлодіод.
4. CALL DELAY: Викликає підпрограму затримки, щоб створити видимий ефект миготіння.
5. MVI A, 00H: Завантажує значення 00H у регістр A для вимкнення світлодіода.
6. OUT 01H: Виводить значення з регістру A в порт 01H для вимкнення світлодіода.
7. JMP START: Повертається до початку програми, щоб повторити цикл.
8. DELAY: Підпрограма затримки, яка зменшує значення в регістрі DE до нуля і створює паузу.

Ця проста програма демонструє базові принципи роботи з мікропроцесором КР1821ВМ85А: використання регістрів, команд вводу-виводу та створення затримок.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було розроблено пристрій криптографічного захисту інформації на базі алгоритму подвійної перестановки.

Створено структурну схему пристрою, яка включає основні компоненти для реалізації алгоритму. Розроблено алгоритми обробки даних для забезпечення надійного криптографічного захисту.

Причиною розробки даного приладу стала необхідність забезпечення високого рівня захисту конфіденційної інформації в умовах зростаючих загроз кібербезпеки. З розвитком технологій та збільшенням обсягів даних, що передаються та зберігаються в електронному вигляді, виникла потреба у створенні більш надійних і ефективних методів захисту інформації. Алгоритм подвійної перестановки було обрано як основу для розробки пристрою завдяки його стійкості до криптографічних атак та можливості реалізації на апаратному рівні, що дозволяє досягти високої швидкості обробки даних.

Для вирішення даного завдання були виконані наступні кроки: осліджено різні криптографічні алгоритми, їх особливості та області застосування. Визначено, що алгоритм подвійної перестановки володіє високою стійкістю до атак та може бути ефективно реалізований на апаратному рівні.

При виборі апаратної бази враховувалися наступні критерії: низька собівартість, доступність, універсальність і зручність у використанні. Був вибраний мікропроцесор КР1821ВМ85А.

В результаті виконаної роботи було доведено, що пристрій криптографічного захисту інформації на базі алгоритму подвійної перестановки є ефективним інструментом для захисту конфіденційної інформації. Запропоновані методи та підходи можуть бути використані для створення надійних систем захисту даних в різних галузях, включаючи фінансову, медичну та державну сфери.

СПИСОК ЛІТЕРАТУРИ

1. Криптографічні методи захисту інформації. Контроль цілісності програмних і інформаційних ресурсів. [Електронний ресурс]. Режим доступу: https://naurok.com.ua/tema-kriptografichni-metodi-zahistu-informaci-kontrol-cilisnosti-programnih-i-informaciynih-resursiv-210574.html
2. Основи сучасної криптографії. Традиційні симетричні криптосистеми. https://studfile.net/preview/5118185/page:46/
3. Безпека програм та даних [Електронний ресурс] : навч. Посіб. До лаб. Практикуму / В. А. Дем'яненко, Ю. А. Кузнецова. – Харків : Нац. Аерокосм. Ун-т ім. М. Є. Жуковського «Харків. Авіац. Ін-т», 2021. – 95 с.
4. Захист інформації https://w.wiki/AHRZ
5. Основні визначення криптографії і захисту інформації. Криптографія з відкритим ключем та цифрові конверти, різновидності алгоритмів, порівняння алгоритмів https://sites.google.com/view/blog-ua/
6. Асиметричні алгоритми шифрування https://w.wiki/AHRG
7. КР1821ВМ85А – Однокристальні восьмирозрядні та шістнадцятирозрядні мікропроцесори. https://studfile.net/preview/8805453/page:4/
8. Мікропроцесори http://surl.li/uixmp
9. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. :ДУТ, 2014.– 448 с.:іл.
10. Бивалін Р.А. Захист інформації з допомогою перестановок / Борисенко О.А., Горішняк А.О., Бивалін Р.А. // Фізика, електроніка, електротехніка (ФЕЕ-2023). Матеріали та програма науково-технічної конференції. – Суми: СумДу, 2023. – С. 80.
11. Бивалін Р.А. Пристрій криптографічного захисту інформації на базі алгоритму подвійної перестановки / Бережна О.В., Товстогуз Б.О., Бивалін Р.А. // Фізика, електроніка, електротехніка (ФЕЕ-2024). Матеріали та програма науково-технічної конференції. – Суми: СумДу, 2024. – С. 67.

Додаток А

Захист інформації з допомогою перестановок

Борисенко О.А., *професор*; Горішняк А. А., *аспірант*; Бивалін Р. А, *студент*
Сумський державний унівеситет, м. Суми, Україна

Перестановки це математичний об'єкт, який широко розповсюджений в математиці. Їх використовують при рішенні задач комбінаторної оптимізації, в абстрактній алгебрі, а також при захисту інформації від несанкціонованого доступу. Також вони дозволяють знаходити помилки при передачі повідомлень.

Це можливо тому що перестановки це об'єкти, які складаються з елементів, що не повторюються. Наприклад, якщо перестановки складаються з 3 елементів а б с, то можна скласти 6 перестановок: абс, асб, бас, бса, саб, сба. Відповідно ними можна закодувати 6 повідомлень.

Якщо при передачі якоїсь перестановки з'являться комбінації, які не є перестановками, наприклад ааб або саа, то це буде ознакою помилки. Помилки в перестановках можна не тільки знаходити, а й виправляти.

Також перестановки, якщо їх буде достатня кількість, захищають інформацію від несанкціонованого доступу, і чим більше буде елементів в перестановках, тим надійніший буде захист. Перестановкам ставляться у відповідність повідомлення, що передаються.

Кількість перестановок знаходиться як факторіал від кількості їх елементів. Так, якщо кількість елементів дорівнює 6, то кількість перестановок буде дорівнювати 720.

З подальшим збільшенням кількості елементів перестановок їх кількість збільшується за експонентою. Тому декодувати без знання ключів шифру ці перестановки досить складно і відповідно вони мають високу стійкість. Наряду з закритістю від дешифрування перестановки ще й завадостійкі.

Таким чином, перестановки можуть ефективно використовуватися в задачах зв'язку одночасно для боротьби з завадами і несанкціонованим доступом до інформації.

Додаток Б

Пристрій криптографічного захисту інформації на базі алгоритму подвійної перестановки

Бережна О.В., *доцент*, Бивалін Р.А., *студент*,
Товстогуз Б.О., *студент*
Сумський державний університет, м. Суми, Україна

Розвиток Інтернету речей значно збільшує кількість об'єктів автоматизації та каналів передачі даних. Значно збільшується кількість каналів витоку інформації та зростає потреба у застосуванні оптимальних методів захисту інформації відповідно до рівня кіберзагроз. Актуальним завдання є пошук напрямків розвитку та застосування таких криптографічних методів, як алгоритм подвійної перестановки.

На сьогоднішній день алгоритми криптографічного захисту, зокрема алгоритм подвійної перестановки, можуть широко використовуватись в різних сферах, таких як інформаційна безпека, електронна комунікація, банківська справа тощо. Вони дозволяють ефективно захищати дані від несанкціонованого доступу та забезпечують конфіденційність інформації.

Однак існують певні недоліки у сучасних рішеннях, пов'язаних з алгоритмом подвійної перестановки. Деякі з них включають обмежену довжину ключа, можливість атак методом перебору ключів та обмежену стійкість до криптоаналітичних атак.

Дослідження показали, що для подолання недоліків алгоритму подвійної перестановки можна використовувати додаткові методи шифрування або покращені версії алгоритму, наприклад:

- застосування додаткових шифрувальних методів: комбінування алгоритму подвійної перестановки з іншими криптографічними методами може підвищити рівень безпеки;
- використання більш складних ключів: використання довших і складніших ключів може зробити атаки зламу складнішими та менш ймовірними.

Запропоновані рішення можуть допомогти подолати недоліки і підвищити ефективність алгоритму подвійної перестановки. Здійснення таких заходів сприятиме підвищенню рівня безпеки конфіденційної інформації, що передається та зберігається в інфокомунікаційних системах.

Поз. позн.	Назва	Кіл.	Примітка
	Конденсатори		
$C_1 – C_4$	К10-9-15В-1500 пФ ОЖО.460.172ТУ	4	
C_5	К10-17-1б-2,2пФ± 10% ОЖО.461.104ТУ	1	
C_5-С6	К10-17-25В-0,1 мкФ ОЖО.461.104ТУ	2	
C_7-С22	К50-6-25В-10 мкФ ОЖО.460.172ТУ	16	
	Мікросхеми		
DD1	КР1821ВМ85А	1	
DD2	КР580ВВ51	1	
DD3	КР580ВИ53	1	
DD4…5	КР580ИР82	2	
DD6	К555КП11	1	
DD7	КР1533ИД3	1	
DD8	КР580ВА86	1	
DD9	КР580ВН59	1	
DD10	К573РФ5	1	
DD11	К537РУ8	1	
DD12	КР580ВВ55А	1	
DD13…15	КР555ИР22	3	
DD16	1533ЛН1	2	
DD17	К564ЛН2	2	
DD18	К1533ЛЕ4	1	
DD19…20	К1533ЛИ1	3	
DD21	КИПЦ01	3	

Зм.	Лист	№ докум.	Підпис	Дата	ЕлІТ 6.171.00.10.025 ПЕ			
Розроб.		Бивалін Р.А.			Пристрій криптографічного захисту інформації на базі алгоритму подвійної перестановки	Літ.	Лист	Листів
Перевір.		Бережна О.В.					1	2
Нач.лаб.								
Н. Контр.		Бережна О.В..				ЕС-01		
Затверд.		Опанасюк А.С.			Перелік елементів			

Поз. обозн.	Назва	Кіл.	Примітка
	Резистори		
R_1 - R_3	С2-29В-0,125-220 Ом+10% ОЖО.467.180 ТУ	1	
R_4	CF14JT100R-100 Ом ± 10%,	1	
R_5	CF1/4W-203J-20кОм ± 10%,	1	