МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет

Факультет електроніки та інформаційних технологій
Кафедра електроніки і комп'ютерної техніки

«До захисту допущено»
Завідувач кафедри

_____ _____
_____ 2023р.

КВАЛІФІКАЦІЙНА РОБОТА
На здобуття освітнього ступеня бакалавр
зі спеціальності 6.171.00.10 "Електроніка",
освітньо-професійної програми «Електронні системи та компоненти»
на тему: «Пристрій криптографічного перетворення даних згідно ДСТУ ГОСТ 28147:2009»

Здобувача групи ЕС-91 Орлов Владислав Віталійович

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

_____ _____

Керівник_____ _____

Суми – 2023

Сумський Державний Університет

Факультет ЕлІТ
Кафедра електроніки і комп'ютерної
техніки Напрямок підготовки:
6.171.00.10 "Електроніка"

ЗАТВЕРДЖУЮ:
Зав. кафедри Опанасюк А.С.
« » 20 р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

студенту **Орлову Владиславу Віталійовичу**

1. Тема проекту «Пристрій криптографічного перетворення даних згідно ДСТУ ГОСТ 28147:2009» затверджено наказом по кафедрі від «30» березня 2023р №0310-6

2.Термін здачі студентом закінченого проекту _____

3.Вихідні дані до проекту Розробити пристрій криптографічного перетворення даних згідно ДСТУ ГОСТ 28147:2009. Синтез пристрою виконати на базі мікропроцесорної системи

4.Зміст розрахунково-пояснювальної записки(перелік питань, які підлягають розробці) 1.Огляд літератури; 2.Розробка алгоритму функціонування та структурної схеми проектованого пристрою; 3.Розробка схеми електричної принципової пристрою; 4.Розроблення програмного забезпечення пристрою;

5.Перелік графічного матеріалу(з точним зазначенням обов'язкових креслень)

1 Схема алгоритму.
2 Схема електрична структурна.
3 Схема електрична принципова.

КАЛЕНДАРНЫЙ ПЛАН

№ п/п	Назва етапів дипломного проекту(роботи)	Термін виконання етапів дипломного проекту (роботи)	Примітка
1	Огляд технічної літератури	21.04.23	
2	Розробка алгоритму функціонування та структрурної схеми пристрою	05.05.23	
3	Розрахунок вузлів та блоків пристрою та розробка схеми принципової пристрою	13.05.23	
4	Оформлення графічної частини	17.05.23	
5	Оформлення пояснювальної записки	26.05.23	
6	Рецензування та підготовка до захисту	02.06.23	

Студент-дипломник Орлов В.В.

Керівник проекту Бережна О.В.

«____»_____2023 р.

ЗМІСТ

АНОТАЦІЯ

Пояснювальна записка містить: 45 аркушів, 16 рисунків, 4 таблиці

Графічна частина моєї роботи включає в себе: блок-схему алгоритму роботи пристрою, структурну та принципову електричну схему.

Пояснювальна записка містить чотири розділи

У першому розділі йдеться про актуальність теми, постанови задачі та аналізі відповідної літератури для її вирішення

Другий розділ присвячений розробці та побудові алгоритму криптографічного перетворення з подальшим створенням структурної схеми.

У третьому розділі була проведена робота над пошуком підходящих елементів та розробку принципової схеми пристрою шифрування.

Четвертий розділ описує розробку програмного забезпечення пристрою.

ВСТУП

На теперішній час, час Інформаційної ери більшість населення користуються персональними копм'ютерами, ЕОМ чи іншими електронними пристроями. Об'єми створюваної інформації важко уявити – за деякими даними [1] 100 зетабайтів за рік , якщо конкретніше 10^{21} байтів або зебібайт - 2^{70}.

Над цими даними постійно проводяться процеси обробки, передачі чи зберігання. Дивлячись на обсяги цієї інформації, виникає питання щодо її доступності: невже будь яку інформацію можна отримати з будь-якого закутка?? Фільми, навчальні підручники, наукові роботи, художні книжки, газети чи інші щоденні новини – данні, що мають загальний доступ не потребують важкого захисту. Тобто, потрібно захистити інформацію більше від зовнішніх завад - від часткового або повного спотворення даних. Бажано, щоб деякі з таких даних не вкрали, але це вирішують законами та показанням за «піратство».

З іншої сторони – є те, що не хотілось би висвітлювати. Для звичайних буднів більшості населення цими секретами можуть бути звичайні діалоги з людьми, як робочі, так і особисті. Така інформація підлягає захисту від сторонніх очей, але її викрадення та розшифрування не вплине більше ніж на декількох осіб. Розглядаючи документы, рахунки та дані на рівні держави – розумним буде передавати та зберігати їх в захищеному стані.

Для обох випадків створені органи державної влади, що спостерігають та ловлять інформаційних зловмисників. Та для обох ситуацій створені методи криптографічних перетворень: від простих зсувів літер алфавіту, що використовували тисячі років назад, до багаторівневих шифрувань, яких людина, без гаджетів, дешифрувала б роками.

Мета даної роботи у розгляді методу криптографічного перетворення даних, та розробки пристрою для його використання.

1.ОГЛЯД ЛІТЕРАТУРИ

1.1 Система передачі даних

Система передачі даних (далі СПД) – це сукупність каналів зв’язку та апаратів передачі даних (далі АПД). АПД в свою чергу можна представити як кодер/декодер та модулятор/демодулятор. Виходячи з цього загальна модель СПД має такий вигляд:

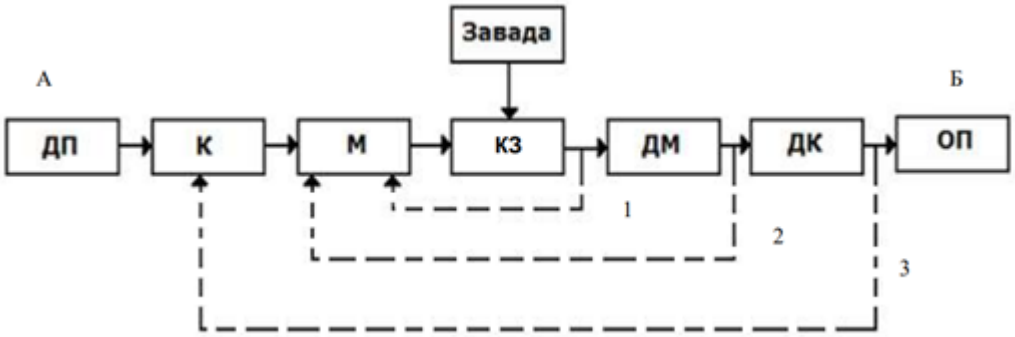

Рис. 1.1 Модель СПД

Кодер – пристрій кодування сигналу у двійковій системі числення

Модулятор – пристрій підготовки сигналів для придатності до передачі (наприклад: накладання високих частот)

Джерело інформації або її споживач (одержувач), або тим і іншим одночасно називають – кінцевий термінальний пристрій (далі КТП). Часто для визначення КТП застосовують міжнародний термін DTE (date terminal equipment.

Безпосередня передача даних відбувається за допомогою АПД -апаратури передачі даних, за міжнародним позначенням DCE (date communications equipment). Функція DCE полягає в тому щоб забезпечити можливість обміну інформацією між двома (або більше) DTE по каналу певного типу, наприклад, телефонному каналу загального користування (ТКЗК). DCE може являти собою аналоговий модем, якщо використовується аналоговий канал зв'язку або бути пристроєм обслуговування цифрового каналу типу E1/T1, або ISDN.

У більшості випадків модем - це пристрій, який виконує функції модулятора-демодулятора, кодера-декодера та інші при обміні інформацією між персональними комп'ютерами як безпосередньо, так і в складі інформаційно-обчислювальних мереж (BBS, FIDONET, Internet, Novell і т.д.). Для такого пристрою вхідний сигнал, це, як правило, цифрова послідовність даних, що надходить від DTE, а вихідний сигнал – це аналоговий сигнал, що подається в аналоговий телефонний канал. Однак це вірно для випадку, коли модем працює як модулятор. Якщо ж він працює як демодулятор, то все навпаки: вхідний сигнал має аналогову форму, а вихідний сигнал - це потік цифрових даних. Важливу роль для взаємодії DTE і DCE відіграє їх інтерфейс, що складається з вхідних/вихідних кіл DTE, DCE, рознімачів та з'єднувальних кабелів.

За використовуємою моделлю системи передачі даних можна розділити на дві групи: системи без зворотного зв'язку і системи зі зворотним зв'язком.

До першої групи відносяться СПД, що використовують для передачі інформації прості (ненадлишкові) коди, і СПД, що використовують надлишкові коди, що виявляють і виправляють помилки. СПД 3 застосуванням простих кодів не можуть забезпечити високої достовірності переданої інформації через низьку завадостійкість прийому повідомлень в умовах дії завад.

Такі системи знаходять застосування головним чином при передачі інформації на короткі відстані при низькому рівні завад у каналі зв'язку

Ускладнення кодів (збільшення надмірності) покращує ефективність проте вимагає значних ресурсів пропускної здатності. У той же час навіть прості коди завжди мають кращі властивості щодо виявлення помилок аніж їх виправлення.

Тому до другої групи СПД (зі зворотним зв'язком) відносяться системи, у яких якість передачі інформації контролюється і керується за допомогою використання каналу зворотного зв'язку. Як правило, у таких системах застосовують коди, що виявляють помилки. Перевагою СПД зі зворотним зв'язком є можливість підвищення правильності переданої інформації без ускладнення коду, використовуваного в системі, простою зміною функцій зворотного каналу. У таких системах по прямому каналу передають повідомлення від станції «А» до станції «Б». Зворотний же канал у СПД може бути використаний для посилки передавальному пристрою «А» відомостей про фактичний прийом повідомлень на станції Б. В залежності від охоплення певного обладнання СПД її зворотний зв'язок розрізняють за трьома типами:

тип 1 - фіксує факт надходження сигналу (наявності необхідного рівня) з лінії зв'язку на вхід приймача чи після проходження сигналом перших каскадів приймача;

тип 2 фіксує правильність розпізнавання одиничних елементів сигналу демодулятором (охоплює модем);

тип 3 — фіксує правильність прийому кодових комбінації (охоплює - всю систему).

В життевих реаліях загальна структура СПД має такий вигляд:

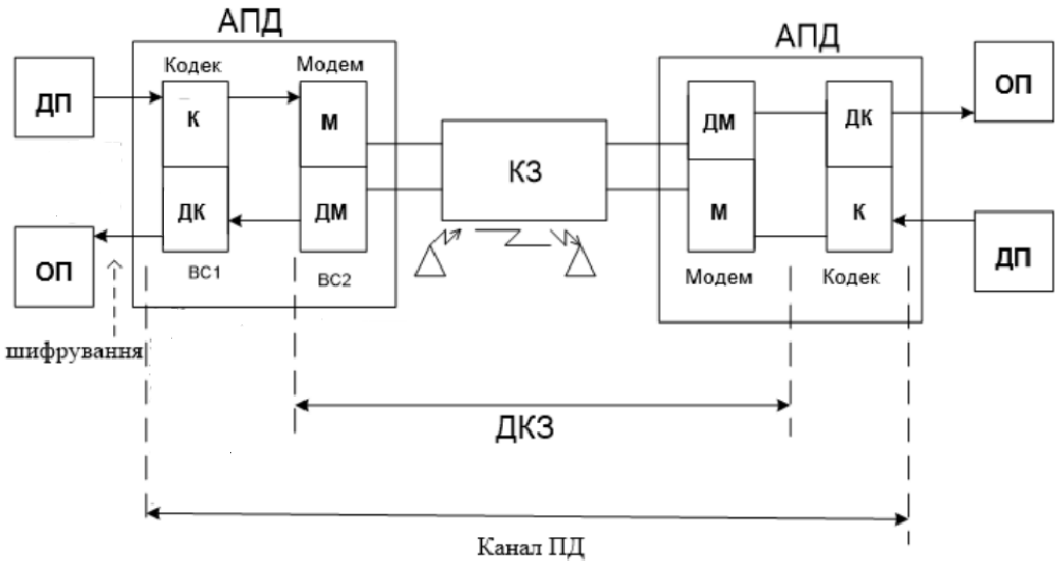

Рис. 1.2. Загальна структура СПД [5]

Кодек виконує функції кодування сигналів завадостійким кодом та реалізує алгоритми підвищення достовірності передачі.

Модем виконує функцію узгодження сигналу передачі даних параметрами каналу передачі, в ньому відбувається модуляція (демодуляція) сигналу, а також забезпечення параметрів стандартного стику з каналом передачі (кількість ланцюгів, електричні параметри сигналу і ін.).

Варіант 1 зворотного зв'язку фактично контролює якість прямого каналу, і в залежності від його стану передавач може змінювати умови передачі сигналів (метод кодування, вид модуляції, швидкість передачі, потужність сигналу і т.д.).

Варіант 2 - зворотні зв'язки контролюють роботу модему, правильність демодуляції сигналів.

Варіант 3 зворотні зв'язки - контролюють роботу декодера. Таким чином, у варіантах 2 і 3 зворотний зв'язок контролює рішення, прийняті приймачем.

У залежності від використання зворотного зв'язку СПД кожного з трьох типів поділяють на системи з інформаційним зворотним зв'язком (133) і з вирішальним зворотним зв'язком (ВЗЗ).

ВЗЗ (вирішальний зворотний зв'язок) — рішення про правильність прийнятої інформації виноситься приймачем і у зворотному каналі видається підтвердження правильності прийому або запит на повторення неприйнятої інформації. При цьому використовуються прості коди, а у зворотному каналі кількість передаваємої інформації незначна.

133 (інформаційний зворотний зв'язок) — рішення про правильність прийнятої інформації видає передавач на основі переданої і прийнятої зі зворотного зв'язку інформації. Процес повторюється доти поки інформація не збігається. З 133 можна передавати без кодів, але у зворотному каналі здійснюється повна передача всього обсягу інформації.

1.2 Захист інформації

Під час розробки таких каналів або інших інформаційно-комунікаційних систем (далі ІКС), з’являється важливе питання захисту інформації. Ця проблема поступово загострюється в міру розвитку інформаційних технологій і тотального використання ІКС і мереж у всіх областях.

На сьогодні в сфері захисту сформувалася досить потужна індустрія (яка об'єднала в собі науку й виробництво), орієнтована на рішення основних питань безпеки, які можна розділити на три групи: фізичні (зв'язані здебільшого з об'єктивними факторами); логічні (пов'язані із суб'єктивними факторами); соціальні.

З фізичною безпекою зв'язані питання захисту від пожеж, затоплень, землетрусів, ураганів, вибухів, промислових хімічних речовин, різних магнітних полів, збоїв устаткування, гризунів і т.п. Тобто вплив зовнішнього середовища, яке створює завади для нашого каналу зв’язку.

Завада - будь-який випадковий вплив на сигнал, який погіршує вірність відтворення переданих повідомлень. Завади досить різноманітні як по своєму походженню, так і по фізичних властивостях. У радіоканалах часто зустрічаються атмосферні завади, обумовлені електричними процесами в атмосфері й, насамперед, грозовими розрядами. Енергія цих завад зосереджена, головним чином, в області довгих і середніх хвиль. Сильні завади створюються також промисловим обладнанням. Це так називані індустріальні завади, що виникають через різкі зміни токів в електричних колах усіляких електропристроїв. Сюди також відносяться завади від електротранспорту, електричних двигунів, медичних установок, систем запалювання двигунів тощо. Розповсюдженим видом завад є завади від сторонніх радіостанцій і каналів. Вони обумовлені порушенням регламенту розподілу робочих частот, недостатньою стабільністю частот і поганою фільтрацією гармонік сигналу, а також нелінійними процесами в каналах, що призводять до перехресних спотворювань.

У дротових каналах зв'язку основним видом завад є імпульсні шуми й переривання зв'язку. Поява імпульсних завад часто пов'язана із автоматичною комутацією й перехресними наведеннями. Переривання зв'язку – це явище, при якому сигнал у лінії різко загасає або зникає. Практично в будь-якому діапазоні частот мають місце внутрішні шуми апаратури, обумовлені хаотичним рухом носіїв заряду в підсилювальних приладах, опорах і інших елементах апаратури.

Ці завади особливо позначаються при радіозв'язку в діапазоні ультракоротких хвиль, де інші завади невеликі. У цьому діапазоні мають значення й космічні завади, пов'язані із електромагнітними процесами, що відбуваються на Сонці, зірках й інших неземних об'єктах. Шум визначає нижню межу сигналів, які можуть бути оброблені електронними засобами. Усунення впливу внутрішніх шумів на вірність повідомлень у системах зв'язку – одна з найбільш складних завдань, що стоять перед розроблювачами таких систем. Навіть коли вплив зовнішніх завад спеціальними заходами може бути зведений до мінімуму або повністю усунутий, залишається теоретично мінімальний рівень шумів, обумовлений наявністю деяких джерел власних, або внутрішніх шумів.

Логічна безпека відображає питання захисту від несанкціонованого доступу (НСД), помилок у діях персоналу й програм, які негативно впливають на інформацію й т.п.

До соціальної безпеки належать засоби юридичного, організаційного й адміністративного захисту, питання підготовки кадрів, виховної роботи, спрямованої на формування певної дисципліни й етичних норм, обов'язкових для тих, хто взаємодіє в інформаційному контурі й т.п

До базових характеристик безпеки інформації відносять конфіденційність (Confidential), цілісність (Integrity) і доступність (Accessibility).

Конфіденційність - характеристика безпеки інформації, що відображає її властивість нерозкритості й доступності без відповідних повноважень.

Цілісність - характеристика безпеки інформації (даних), що відображає її властивість протистояти несанкціонованій модифікації/

Доступність - характеристика безпеки інформації, яка відображає її властивість, що складається в можливості використання відповідних ресурсів у заданий момент часу відповідно до пред'явлених повноважень.

На даний момент розглянемо проблему конфедеційності інформації

1.3 Криптографія

В Україні питання захисту інформації регулюються Цивільним, Господарським кодексами України. Закон України «Про інформацію» ввів поняття « інформація із обмеженим доступом». Ця інформація відповідно до закону поділяється на конфіденційну та таємну. Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб та розповсюджуються за їх бажанням відповідно з передбаченими ними умовами.

Чільне місце серед всього різноманіття засобів попередження несанкціонованого доступу до захищеної інформації посідають криптографічні методи, оскільки вони ґрунтуються на властивостях інформації і не мають слабкостей, що виникають при використанні особливостей вузлів її обробки,середовища передачі, адміністративних засобів.

Криптографія - це наука, що вивчає математичні методи забезпечення автентичності і конфіденційності даних. Для сучасного етапу її розвитку характерним є використання алгоритмів, що припускають реалізацію за допомогою обчислювальних засобів.

Основними вимогами до сучасних методів криптографічного захисту є: конфіденційність, й цілісність . В сучасній криптографії практичне значення мають лише методи захисту з використанням ключа. Їх поділяють на два види: симетричні та асиметричні

Симетричні системи шифрування базуються на одному ключі,що використовується і для шифрування, і для дешифрування або ключ дешифрування можливо обчислити за ключем шифрування. Їх перевагами є:

1. Велика пропускна здатність.

2. Відносно короткі ключі.

3. Їх можна використати як основу для створення різних криптографічних механізмів псевдовипадкові генератори чисел та обчислювально-ефективні схеми.

4. Можливість їх комбінування для підвищення криптостійкості.

Першою принциповою ознакою, яка дозволяє провести класифікацію шифрів, є обсяг інформації, який невідомий третій стороні. Якщо зловмиснику повністю не відомий алгоритм виконаного над повідомленням перетворення. Шифр називають тайнописом. Тобто тайнопис є звичайним кодуванням інформації, або представленням її у іншому вигляді. При цьому третій стороні невідомий сам принцип кодування.

У противагу тайнопису криптографією з ключем називають сьогодні алгоритми шифрування, в яких сам алгоритм перетворень широко відомий та доступний кожному, але шифрування виконується на основі невеликого обсягу інформації – ключа, який відомий тільки відправнику та одержувачу повідомлення. В сучасній криптографії розмір ключа складає від 56 до 4096 біт.

Всі криптоалгоритми з ключем поділяються на симетричні та асиметричні. У симетричних криптоалгоритмах ключі, які використовуються на передавальній та приймальній стороні повністю ідентичні. Такий ключ несе в собі всю інформацію щодо процесу утаємнення повідомлення і тому не повинен бути відомий нікому, окрім учасників переговорів. Тому тут часто застосовують термін таємний ключ. А самі системи називають шифрами на таємному ключі.

Загальна схема процесу передачі повідомлення приведена на рис.6.1.

Рис 1.3 Загальна схема передачі даних симетричного шифрування

У асиметричному шифруванні (рис.6.2.) для шифрування повідомлення використовуються один ключ, а для дешифрування – інший. Таким чином, прочитати зашифрований текст можливо, тільки при наявності ключа дешифрування. Тому ключ шифрування може бути відомий всім користувачам мережі та носить назву відкритого ключа. А ключ дешифрування називають закритим. Самі ж асиметричні системи отримали назву шифру на відкритому ключі. Асиметричні шифри немає сенсу використовувати для захищеного зберігання документів. Їх призначення – захист повідомлень, електронна пошта, тощо.

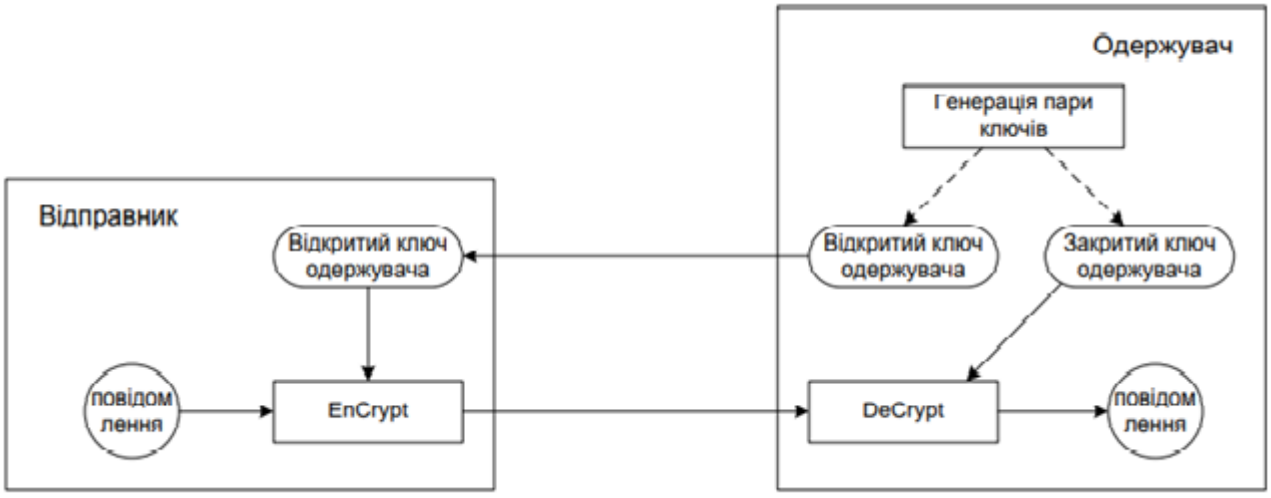

Рис.1.4 Загальна схема передачі даних асиметричного шифрування

1.4 Приклади криптографічних методів

Простими прикладами симетричного шифрування можна представити такі методи як: методи простої заміни, простої перестановки, подвійної перестановки, перестановки «Магічний квадратат».Шифр простої заміни (він же простої підстановки,моноалфавітний шифр) - клас методів шифрування, які зводяться до створення таблиці шифрування за певним алгоритмом, в якому для кожної букви відкритого тексту є одна відповідна їй буква шифротексту. Саме шифрування полягає в заміні букв відповідно до таблиці. Для розшифровки досить мати таку ж таблицю, або знати алгоритм, за яким вона генерується.

Шифри простої заміни включають багато шифрів, що виникли в давнину або середньовіччі, такі як шифр Атбаш (також читається як Етбаш) або шифр Цезаря

Шифр Цезаря є окремим випадком шифру простої заміни (одноалфавітної підстановки). Назву цей шифр отримав по імені римського імператора Гая Юлія Цезаря, який використовував цей шифр при листуванні з Цицероном (близько 50 р. до н.е.).

При шифруванні вихідного тексту кожна літера змінювалася на іншу літеру того самого алфавіту за таким правилом. Літера, на яку замінювали вихідну літеру, визначалася шляхом зсуву за алфавітом від вихідної літери на К літер. При досягненні кінця алфавіту виконували циклічний перехід до його початку. Цезар використовував шифр заміни при параметрі зсуву К = 3. Він змінював у повідомленні першу літеру латинського алфавіту на четверту, другу – на п’яту і так далі, а останню літеру на третю.

Метод простої перестановки

Це метод симетричного шифрування, при якому елементи вихідного відкритого тексту міняються місцями. Елементами тексту можуть бути окремі символи (найпоширеніший випадок), пари букв, трійки букв, поєднання цих відмінків і так далі. Типовими прикладами перестановки є анаграми

Широкого поширення набула різновид маршрутної перестановки - вертикальна. У цьому шифрі також використовується прямокутна таблиця, в якій повідомлення записується рядок за рядком зліва направо. Шифрограма виписується вертикально, а колонки вибираються в порядку, визначеному ключем.

Таблиця 1.1.

2	4	1	5	3
О	с	ь	п	р
и	к	л	а	д
д	л	я	ш	и
ф	р	у	в	а
н	н	я		

Текст: Ось приклад для шифрування

Шифрекст: ьляуяОидфнрдиасклрнпашв

Шифр подвійної перестановки

При шифруванні шифром з подвійною перестановкою текст записується в таблицю за певним маршрутом, потім стовпці і рядки переставляються. Далі шифрограма виписується за певним маршрутом.

Ключем до шифру є розмір таблиці, маршрути написання і оформлення замовлення, порядок перестановки стовпців і рядків. Якщо маршрути мають фіксовані значення, то кількість клавіш - "n!m!", де "n" і "m" - кількість рядків і стовпців в таблиці.

Таблиця 1.2

	2	4	1	5	3
2	О	с	ь	п	р
1	и	к	л	а	д
4	д	л	я	ш	и
3	ф	р	у	в	а
5	н	н	я		

	1	2	3	4	5
1	л	и	д	к	а
2	ь	О	р	с	п
3	у	ф	а	р	в
4	я	д	и	л	ш
5	я	н		н	

Текст: Ось приклад для шифрування

Шифртекст читається в обраній послідовності зазделегідь. Наприклад: зверху-вниз, зліва-направо

Шифртекст: льуяяиОфдндраиксрлнапвш

Перестановка Магічний квадратат

Магічні квадрати - це квадратні таблиці з послідовними натуральними числами від 1, вписаними в їх осередки, які складаються в однакове число для кожного стовпця, кожного рядка і кожної діагоналі. Такі квадрати широко використовувалися для введення шифротексту відповідно до наведеної в них нумерації. Якщо потім виписати вміст таблиці рядками, то вийде шифрування, переставляючи букви. На перший погляд здається, що Ніби магічних квадратів дуже мало. Однак їх кількість дуже швидко збільшується зі збільшенням розмірів квадрата. Так, існує тільки один магічний квадрат розміром 3 х 3, якщо не брати до уваги його обороти. Існує вже 880 магічних квадратів 4 х 4, а кількість магічних квадратів 5 х 5 становить близько 250 000. Тому великі магічні квадрати могли стати хорошою основою для надійної системи шифрування того часу, адже ручне перерахування всіх ключових варіантів цього шифру було немислимо.

У квадрат розміром 4 на 4 помістяться числа від 1 до 16. Його магія полягала в тому, що сума чисел в рядках, стовпцях і повних діагоналях дорівнювала одному і тому ж числу - 34. Вперше ці квадрати з'явилися в Китаї, де їм приписували якусь «магічну силу».

Відомим, але складнішим, методом симетричного шифрування є «гамування».

Під гамуванням розуміють процес накладення за певним законом гами шифру на відкриті дані.

Гама шифру - це псевдовипадкова послідовність, що вироблена за заданим алгоритмом для шифрування відкритих даних і розшифрування зашифрованих даних.

Псевдовипадкові послідовності формуються алгоритмічно, тому є не суто випадковими. Зазвичай приймають, що отримана послідовність має властивості, що є типовими для випадкової послідовності.

Процес шифрування полягає в генерації гами шифру і накладення отриманої гами на вихідний відкритий текст оборотним чином, наприклад, з використанням операції додавання за модулем 2.

Слід зазначити, що перед шифруванням відкриті дані розбивають на блоки однакової довжини, зазвичай по 64 біти. Гама шифру виробляється у вигляді послідовності блоків аналогічної довжини.

Гамма шифру повинна змінюватися випадковим чином для кожного блоку, що шифрується. Якщо період гами перевищує довжину всього тексту, що шифрується, й зловмиснику невідома ніяка частина вихідного тексту, то такий шифр можна розкрити тільки прямим перебором всіх варіантів ключа. В цьому випадку криптостійкість шифру визначається довжиною ключа (періодом неповторюваної частини гами шифру). Оскільки за допомогою комп'ютера можна згенерувати практично нескінченну гаму шифру, то даний спосіб є одним з основних для шифрування інформації в автоматизованих системах.

Рис 1.5 Схема одноразового гамування

Популярний на даний час приклад асиметричного шифрування є електроний підпис

Це реквізит електронного документа, отриманого в результаті криптографічного перетворення інформації з використанням закритого ключа підпису і дозволяє перевірити відсутність спотворення відомостей в електронному документі з моменту формування підпису (цілісність), належність підпису власнику сертифіката ключа підпису (авторство), і в разі успішної перевірки підтвердити факт підписання електронного документа.

Було б незручно шифрувати весь документ, тому шифрується тільки його хеш - невеликий обсяг даних, жорстко прив'язаний до документа за допомогою математичних перетворень і його ідентифікації. Зашифрований хеш - це електронний підпис.

Хеш-функція (англ. hash - «перетворення в фарш», «мішанина»), або функція згортки, - це функція, яка перетворює масив вхідних даних довільної довжини в рядок вихідного біта заданої довжини, що виконується за певним алгоритмом.

Наступним критерієм класифікації шифрів є схема обробки ними потоку інформації. Згідно йому симетричні криптоалагоритми поділяються на: поточні та блочні шифри. Поточний шифр здатний обробляти інформацію побітно. Така схема дуже зручна в каналах послідовного зв’язку, де сам процес передачі інформації може обриватися в будь який момент а потім продовжуватся далі.

Така обробка інформації є досить повільною і тому, враховуючи можливості сучасних процесорів здійснювати паралельну обробку, застосовують інші принципи криптографічних перетворень, які носять назву блочних шифрів. Основним законом блочного шифрування є „або блок, або нічого”. Тобто перетворення можуть здійснюватися тільки над інформацією строго визначеного обсягу. Розмір блоку на сьогоднішній день дорівнює 64, 128 або 256 бітам. Часткове шифрування (наприклад намагання обробити 177 біт) неможливе. Блочне шифрування отримало значно ширше розповсюдження завдяку розвитку обчислювальної техніки. Отже, якщо поточні шифри однаково часто реалізуються як програмно, так і апаратно, то блочні шифри в своїй більшості мають програмну реалізацію.

Одним з таких криптографічних перетвореннь блочного типу є радянський стандарт симетричного шифрування, повна назва якого «ГОСТ 28147-89 Системи обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення».

Основа алгоритму шифру — Мережа Фейстеля (різновид блочного шифру з певною ітеративною структурою). Базовим режимом шифрування за ГОСТ 28147-89 є режим простої заміни (визначені також складніші режими гамування, гамування зі зворотним зв'язком і режим імітовставки).

З моменту опублікування ГОСТу на ньому стояв обмежувальний гриф «Для службового користування», і формально шифр був оголошений «повністю відкритим» тільки в травні 1994 року. Історія створення шифру і критерії розробників станом на 2010 рік не опубліковані.

У 2009 році ГОСТ 28147-89 перевиданий в Україні під назвою ДСТУ ГОСТ 28147:2009.

1.5 Постановка завдання даної роботи

Метою роботи є розробка пристрою криптографічного перетворення даних згідно ДСТУ ГОСТ 28147:2009.

Для досягнення цієї мети необхідно виконати наступне:

1. Визначити основні функції та завдання, які повинен виконувати пристрій криптографічного перетворення даних.

2. Розробити алгоритм функціонування пристрою.

3. Розробити схему електричну структурну пристрою криптографічного перетворення.

4. Розробити схему електричну принципову пристрою

2. РОЗРОБЛЕННЯ АЛГОРИТМУ РОБОТИ ТА СТРУКТУРНОЇ СХЕМИ ПРИСТРОЮ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ДАНИХ ЗГІДНО ДСТУ ГОСТ 28147:2009

2.1 Розгляд алгоритму шифрування

Алгоритм шифрування даних, який визначається ГОСТ 28147-89, являє собою 64-бітовий блочний алгоритм з 256-бітовим ключем.

Дані, що підлягають шифруванню, розбивають на 64-розрядні блоки

Ці блоки розбиваються на два субблока N1 і N2 по 32 біт

Субблок N1 обробляється певним чином:

Вміст субблока N1, складається за модулем 232 з частиною ключа Кх (логічна операція XOR)

Субблок N1 розбивається на 8 частин по 4 біт, значення кожної з яких замінюється відповідно до таблиці заміни для даної частини субблока

Виконується побітовий циклічний зсув субблока вліво на 11 біт

Результат субблока N1 складається зі значенням субблока N2 застосовується логічна операція XOR - додавання виконується по модулю 2.

Наступним кроком буде зміна субблоків місцями. N1, в первичному вигляді, першого циклу становиться N2 для наступного, N1 після обробки – N1 для наступного циклу. Дане перетворення виконується певне число раз («раундів») - 16 або 32, в залежності від режиму роботи алгоритму.

Загальна схема алгоритму перетворення демонстрована на рис.2.1

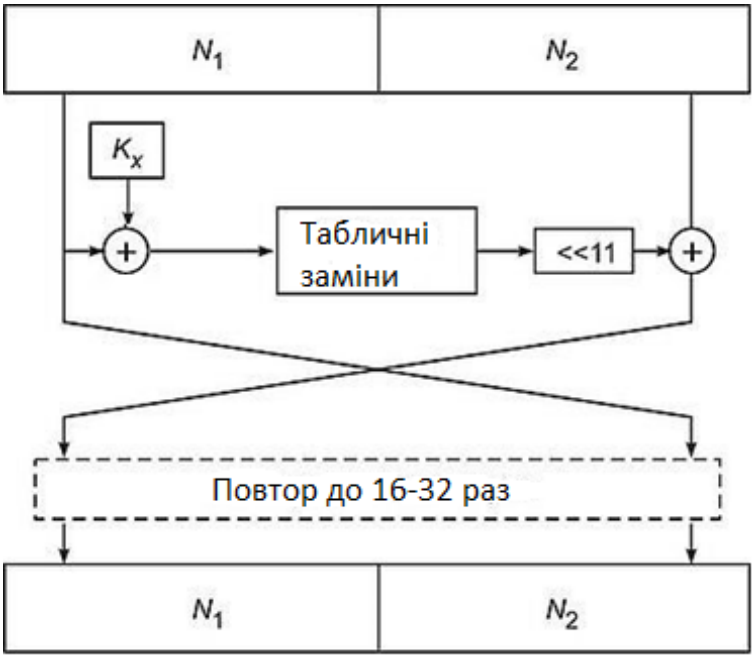

Рис. 2.1 Схема алгоритму ГОСТ 28147—89

Ключ та таблиці заміни також проходять деякі зміни.

Ключ генерується або вводиться розміром 256 біт. Перед використанням ключ розділяється на 8 частин по 32 біти. Для кожного циклу шифрування частина ключа Кх змінюється. Наприклад, для режиму простої заміни (докладніше на наступній сторінці), ключ змінюється таким чином:

К0, К1, К2, К3, К4, К5, К6, К7, К0, К1, і т. д. - в раундах з 1-го по 24-й;

К7, К6, К5, К4, К3, К2, К1, К0 - в раундах з 25-го по 32-й.

Таблиці заміни збираються в блок підстановки. Він з восьми вузлів заміни (S-блоків заміни) S1, S2, ..., S8 з пам'яттю, 64 біт кожен. Субблок N1, який поступає на блок підстановки S, розбивають на вісім 4-бітових послідовних векторів. Кожен з них перетворюється в 4-бітовий вектор відповідним вузлом заміни. Кожен вузол заміни можна представити у вигляді таблиці-підстановки 16-ти 4-бітових двійкових чисел в діапазоні 0000 ... 1111. Вхідний вектор вказує адресу рядка в таблиці, а число в цьому рядку є вихідним вектором. Потім 4-бітові вихідні вектори послідовно об'єднують в 32-бітовий вектор.

Приклад таблиці заміни:

Таблиця 2.1

Вхідний	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Вихідний	**14**	**4**	**2**	**11**	**7**	**10**	**12**	**13**	**3**	**15**	**1**	**8**	**5**	**0**	**6**	**9**

Якщо на вхід прийшов 4-бітний блок «1010», тобто значення 10, то, згідно таблиці, вихідне значення буде дорівнювати 1, тобто «0001», значення 3 замінюється на 11, 1 – на 4 і т.п.

Алгоритм, який визначається ГОСТ 28147-89, передбачає чотири режими роботи:

простої заміни;

гамування;

гамування зі зворотним зв'язком;

генерації імітовставок.

Режим простої заміни

У режимі простої заміни для шифрування кожного 64-бітового блоку інформації виконуються 32 описаних вище раунда. При цьому 32-бітові підключи використовуються в наступній послідовності:

К0, К1, К2, К3, К4, К5, К6, К7, К0, К1, і т. д. - в раундах з 1-го по 24-й; К7, К6, К5, К4, К3, К2, К1, К0 - в раундах з 25-го по 32-й.

Всі блоки шифруються незалежно один від одного, тобто результат шифрування кожного блоку залежить тільки від його вмісту (відповідного блоку вихідного тексту).

даний режим застосовується в основному для шифрування самих ключів шифрування

Для шифрування власне інформації призначені два інших режими роботи - гамування та гамування зі зворотним зв'язком.

У режимі гамування кожен блок відкритого тексту побітно складається за модулем 2 з блоком гами шифру розміром 64 біт. Гама шифру - це спеціальна послідовність, яка формується в результаті певних операцій з регістрами N1 і N2

1. У регістри N1 і N2 записується їх початкове заповнення - 64-бітова величина, яка носить назву синхропосилки.

2. Виконується шифрування вмісту регістрів N1 і N2 (в даному випадку - синхропосилки) в режимі простої заміни.

3. Вміст регістра N1 складається за модулем $(2^{32} - 1)$ з константою

$C1 = 2^{24} + 2^{16} + 2^8 + 4$, а результат додавання записується в регістр N1.

4. Вміст регістра N2 складається за модулем 2^{32} з константою

$C2 = 2^{24} + 2^{16} + 2^8 + 1$, а результат додавання записується в регістр N2.

5. Вміст регістрів N1 і N2 подається на вихід в якості 64-бітового блоку гами шифру (в даному випадку N1 і N2 утворять перший блок гами).

При необхідності продовжувати шифрування, залишився відкритий текст, виконується повернення до операції 2.

Режим гамування зі зворотним зв'язком

У режимі гамування зі зворотним зв'язком для заповнення регістрів N1 і N2, починаючи з 2-го блоку, використовується не попередній блок гами, а результат шифрування попереднього блоку відкритого тексту (рис. 2.2). Перший же блок в даному режимі генерується повністю аналогічно попередньому.

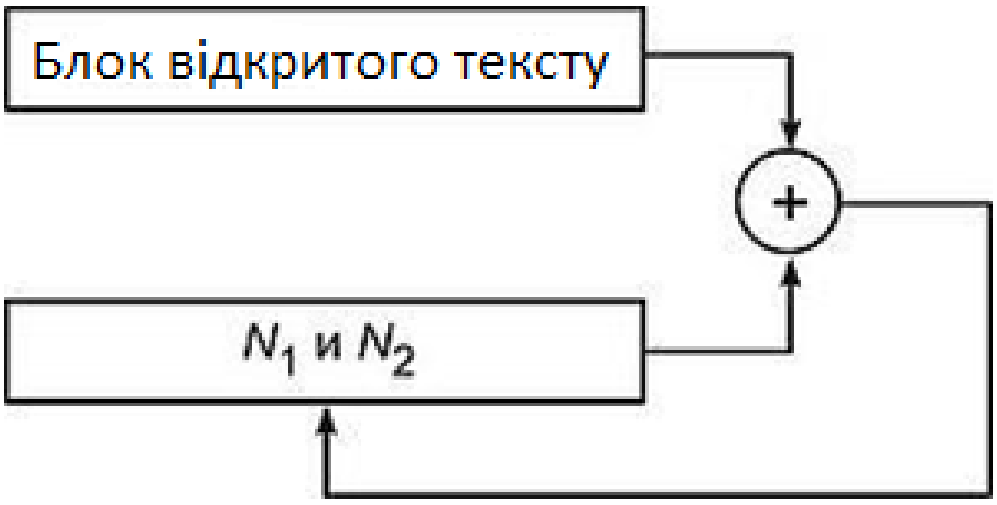

Рис. 2.2 Основа алгоритму гамування зі зворотним зв'язком

Режим генерації імітоприставки

Імітоприставка - це криптографічна контрольна сума, яка обчислюється з використанням ключа шифрування й призначена для перевірки цілісності повідомлень.

Отриманий в результаті цих перетворень 64-бітовий вміст регістрів N1 і N2 або його частина і називається імітоприставкою. Розмір імітоприставки вибирається, виходячи з необхідної достовірності повідомлень: при довжині імітопріставкі в n біт, ймовірність, що зміна повідомлення залишиться непоміченою, дорівнює 2-n.

Імітоприставка використовується наступним чином:

Вона обчислюється для відкритого тексту при зашифровуванні будь-якої інформації та надсилається разом з шифртекстом.

Після розшифрування обчислюється нове значення імітоприставки, яке порівнюється з надісланою.

Якщо значення не збігаються, значить шифртекст був спотворений при передачі або при розшифруванні використовувалися невірні ключі.

На основі першого режиму роботи, а саме, простої заміни, створена схема алгоритму, рис.2.3:

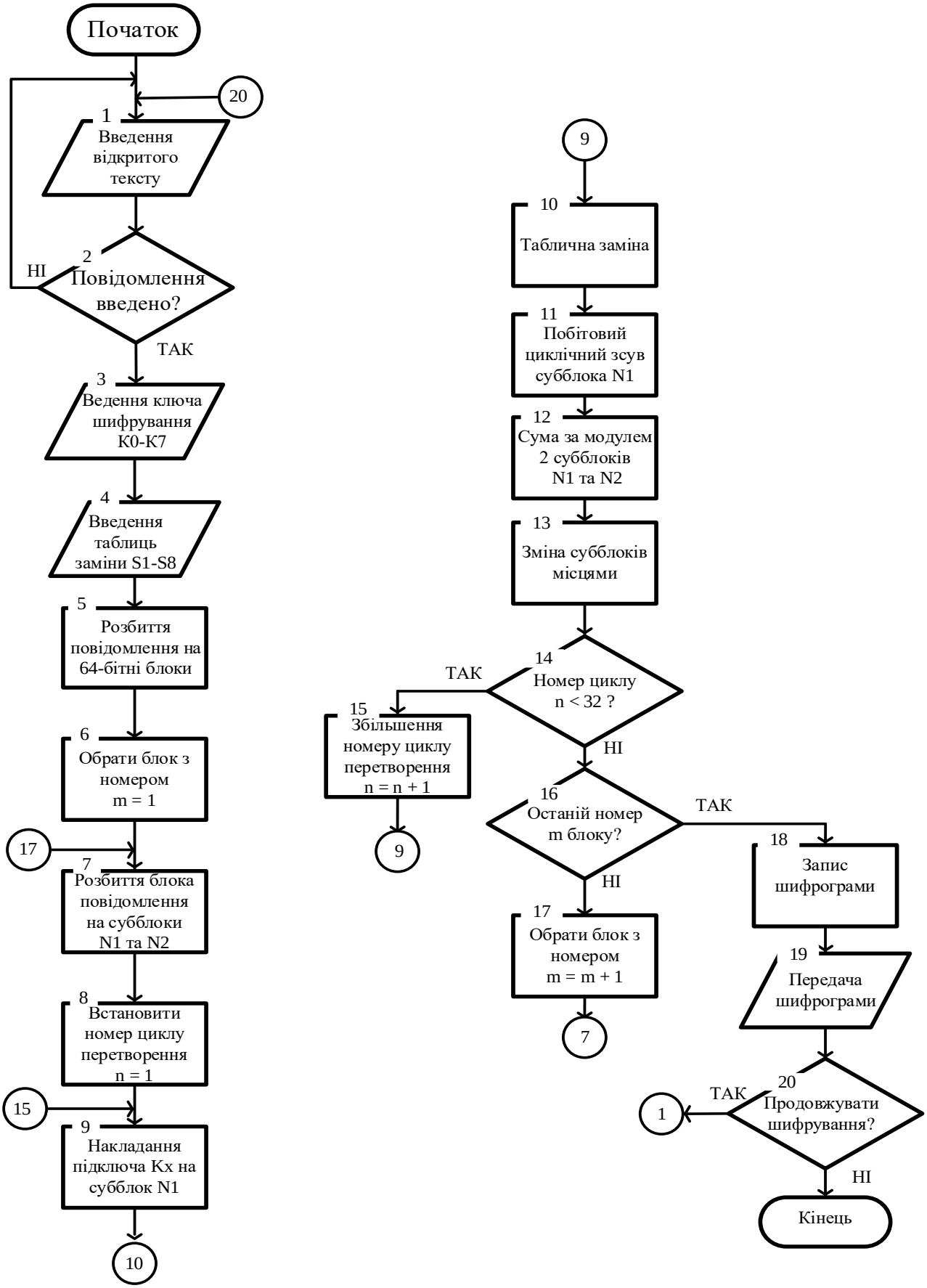

Рис.2.3 Схема алгоритму шифрування

2.2 Розробка структурної схеми пристрою криптографічного перетворення

На основі приведеного алгоритму роботи пристрою та схеми адгоритму, розроблена структурна схема. Складові структурної схеми це сукупність блоків, які мають виконувати певні функції. Схема представлена на рис. 2.4

Розгляд функцій блоків:

Блок введення повідомлення – блок відповідає за отримання/генерації чи введені повідомлення для шифрування.

Блок розбиття повідомлення на 64-розрядні блоки – розділяє кодову комбінацію вхідного повідомлення на блоки по 64 біти.

Блок розділення 64-розрядного блоку на 32-розрядні субблоки – блок відповідає за розділення окремого (надалі кожного) блоку з 64 біт на два рівні субблоки по 32 біти, які мають назву N1 та N2

Суматор по модулю 232 вмісту субблока N1 з підключем Кх – блок відповідає за арифметико-логічну операцію додавання за модулем два між 32-бітним субблоком N1 на 32-бітною частиною ключа, яка обирається відповідно циклу.

Блок введення ключа шифрування – блок відповідає за створення/введення 256-бітного ключа шифрування, та його розділення на вісім 32-бітних частин К0-К7, для подальшого їх вибіркового використання

Блок введення таблиць заміни – блок відповідає за створення/введення таблиць заміни, у к-сті 8 штук S1-S8.

Блок табличної заміни 4-бітових частин проміжної шифрограми – блок, який пропускає через таблицю заміни вхідний субблок.

Регістр побітового циклічного зсуву субблока N1 – блок відповідає за циклічний побітовий зсув субблока на 11 бітів вліво.

Суматор блоків N1 та N2 за модулем 2 – блок виконує арифметико-логічну операцію додавання за модулем два двух субблоків N1 та N2

Блок тимчасового запам’ятовування – блок тимчасової пам’яті (ОЗУ, регістри, аккумулятор), який зберігає проміжні результати, для подальшого використання в межах циклу.

Блок керування циклами перетворень – блок, який контролює процеси запуску/зупинки циклів, веде їх нумерацію та обирає потрібні змінні відповідно циклу.

Блок зміни субблоків місцями- блок, який перезаписує значення субблоків, змінюючи їх дані місцями (N1 стає N2, N2 стає N1), для використання у наступному циклі.

Блок запису шифрограми – блок, який об'єднує зашифрований код в шифрограму

Передача шифрограми – блок відповідає за відправку готової шифрограми до наступного пристрою.

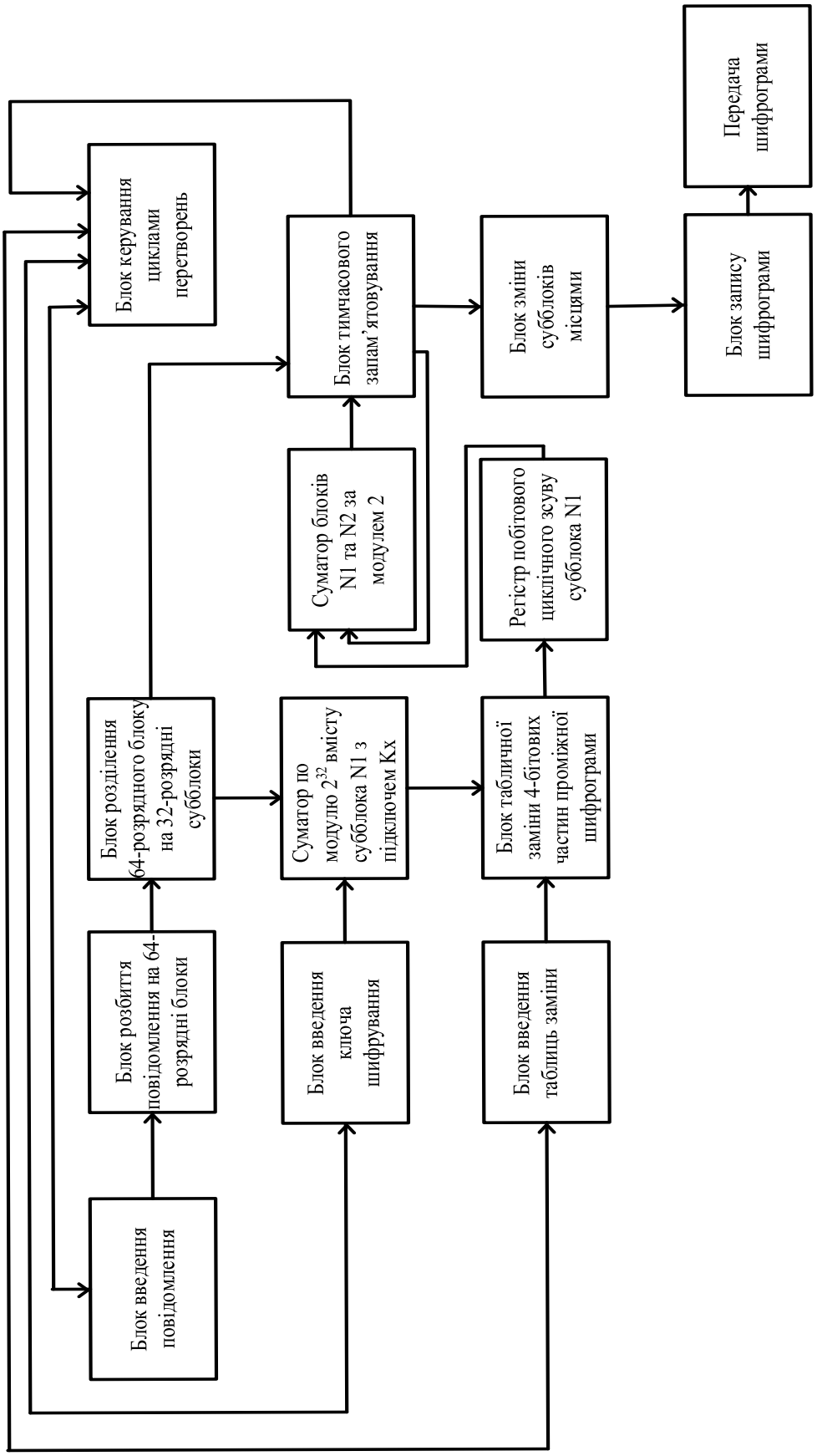

Рис. 2.4 Схема електрична структурна

3.РОЗРОБЛЕННЯ ЕЛЕКТРИЧНОЇ ПРИНЦИПОВОЇ СХЕМИ ПРИСТРОЮ

Для виконання шифрування методом по ГОСТу 28147-89 була розроблена принципова схема. Для реалізації алгоритму криптографічних перетворень орані наступні елементи:

КР1821ВМ85 – мікропроцесор

КР580ІР82 – буферний регістр, в кількості двох штук

КР580ВА86 – шинний формувач

К555КП11 – мультиплексор

КР580ВВ55А – мікросхема вводу/виводу паралельної інформації.

К537РФ2 – ПЗП

К537РУ8 – ОЗП

Розглянем кожен елемент окремо

Мікросхема КМ1821ВМ85 в корпусі продемонстрована на рис. 4.1

Мікросхема є однокристальним статичним 8-розрядним паралельним центральним процесорним пристроєм (мікропроцесором), що виготовляється за технологією КМОН, і призначена для побудови мікро-ЕОМ, що використовуються в системах передачі і обробки інформації.

Виводи:

1,2 - x1, x2 – виводи для підключення зовнішнього кварцового резонатора (або іншого генератора).

35 – RA – вхід «Готовність».

36 - - вхід «Встановлення процесора у початковий стан»,

6, 7, 8, 9, 10 – входи переривань

39 - HOLD - вхід «захоплення шин», вхід сигналу запиту зовнішніх адресної шини та шини даних

5 - SID - вхід «отримання послідовних даних»/послідовний вхід

21-28 – адресні виводи (виводи шини адреси)

12-19 – введення/виведення шини адреси/даних

30 – ALE – вивід стробування адреси

29, 33 – S0,S1 – виводи стану циклів читання та запису відповідно

38 – HLDA - вивід підтвердження захоплення шини

32 – RD - вивід зчитування

31 - WR – вивід запису

34 - IO/M– вивід вибору пам’яті

4 - SOD – вивід послідовних даних

11 - INTA – вивід підтвердження переривань

RES OUT – вивід скидання, «встановлення процесора у початковий стан»

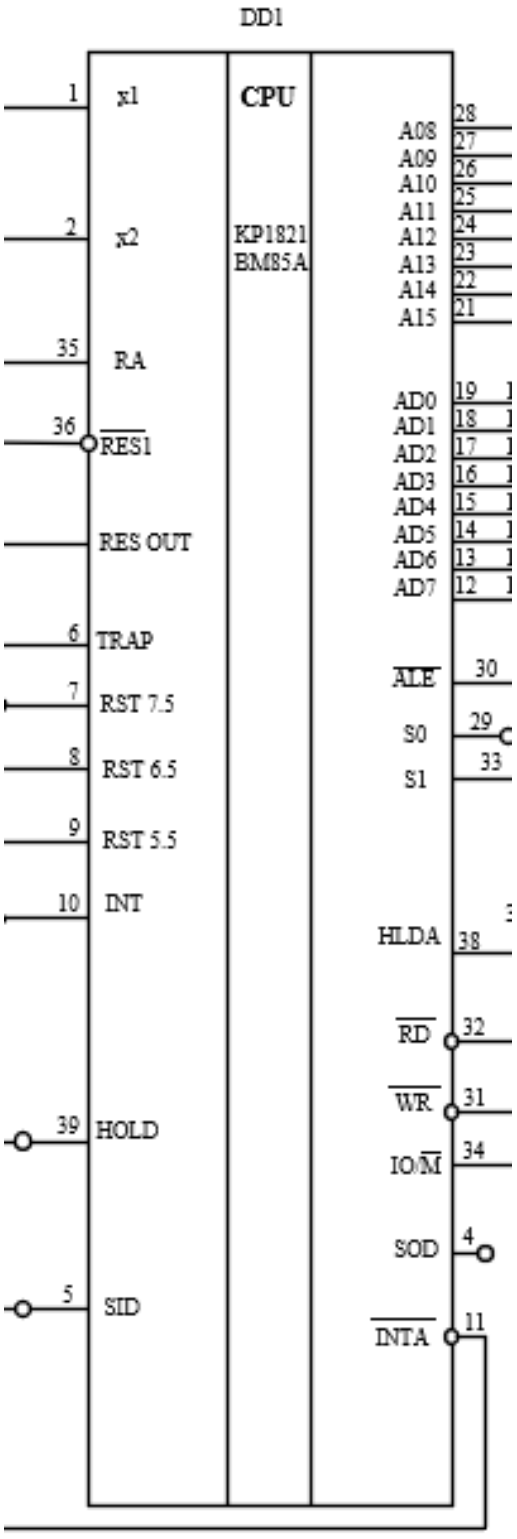

Рис.4.1 КМ1821ВМ85

Регістр КР580ІР82 в корпусі продемонстрована на рис. 4.2

Мікросхема являє собою 8-розрядний буферний регістр, що не інвертує (D-регістр "заскочка" з трьома станами на виході). Призначена для введення-виведення інформації зі стробуванням у мікропроцесорних системах, на ІС серії КР580. Може бути використана як буферний регістр у обчислювальних системах та пристроях дискретної автоматики. Складається з 8 функціональних блоків (D-тригер та потужний вихідний вентиль без інверсії) та схеми управління. Має підвищену здатність навантаження. Залежно від стану стробуючого сигналу може працювати в режимах шинного формувача або зберігання. Містить 520 інтегральних елементів. Корпус типу 2140ю.20-2, маса не більше 4 г

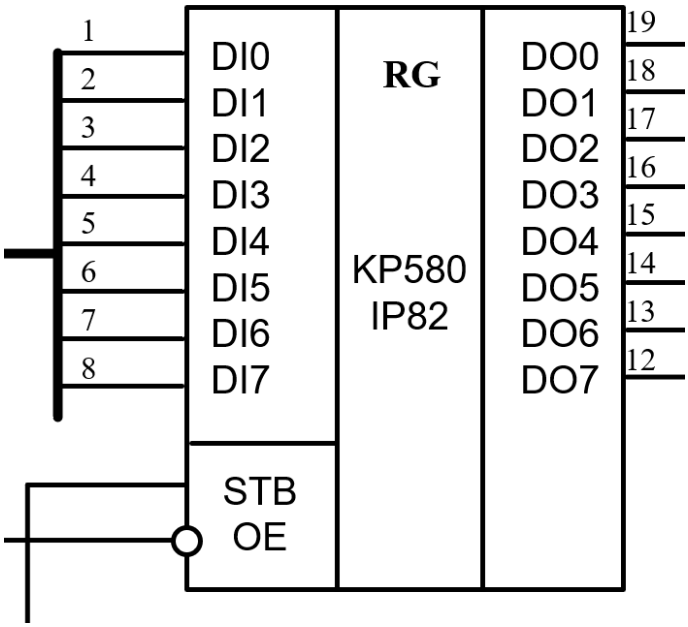

Рис. 4.2 Регістр КР580ІР82

Призначення виводів:

1-8 - інформаційні входи DIO-DI7;

9 - OE - вхід дозволу виходу;

11 - STB – стробуючий вхід;

12-19 - інформаційні виходи DO7-DO0

Шинний формувач КР580ВА86 в корпусі продемонстрована на рис. 4.3

Мікросхеми являє собою двонаправлений 8-розрядний неінвертуючий шинний формувач з трьома станами на виході. ІС служать буферним пристроєм у схемах мікропроцесорних систем серії КР560, КМ580 та здійснюють зв'язок мікропроцесора з периферійними пристроями введення виведення інформації. Наявність стану із високим вихідним імпедансом дозволяє навантажити групу таких мікросхем однією навантаження. Мають підвищену здатність навантаження. Містять 567 інтегральних елементів. Корпус типу 2140.20-1, маса трохи більше 4 р

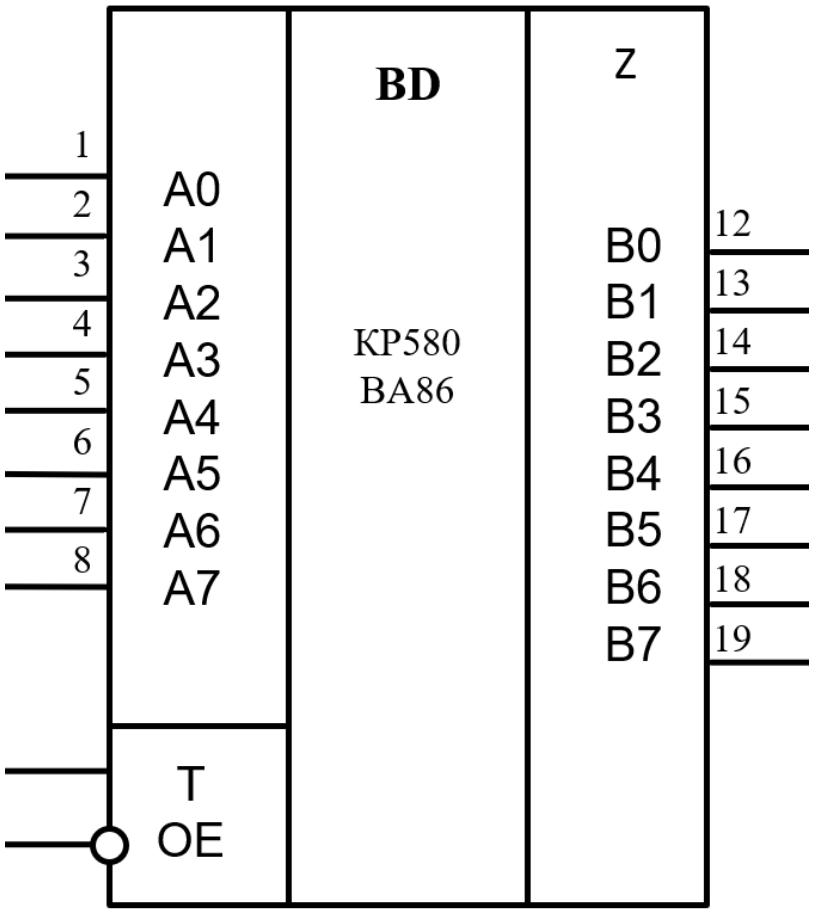

Рис. 4.3 шинний формувач КР580ВА86

Призначення виводів:

A0 – A7 –вивід введення/виведення

OE вхід дозволу виходу;

T - вхідний сигнал керування напрямком передачі;

B0 – B7 –вивід введення/виведення

Мультиплексор К555КП11 в корпусі продемонстрована на рис. 4.4

Мікросхема авляє собою чотирирозрядний селектор 2-1 без інверсії з трьома стійкими станами. Містять 133 інтегральні елементи. Корпус типу 238.16-2, маса трохи більше 1,2 р

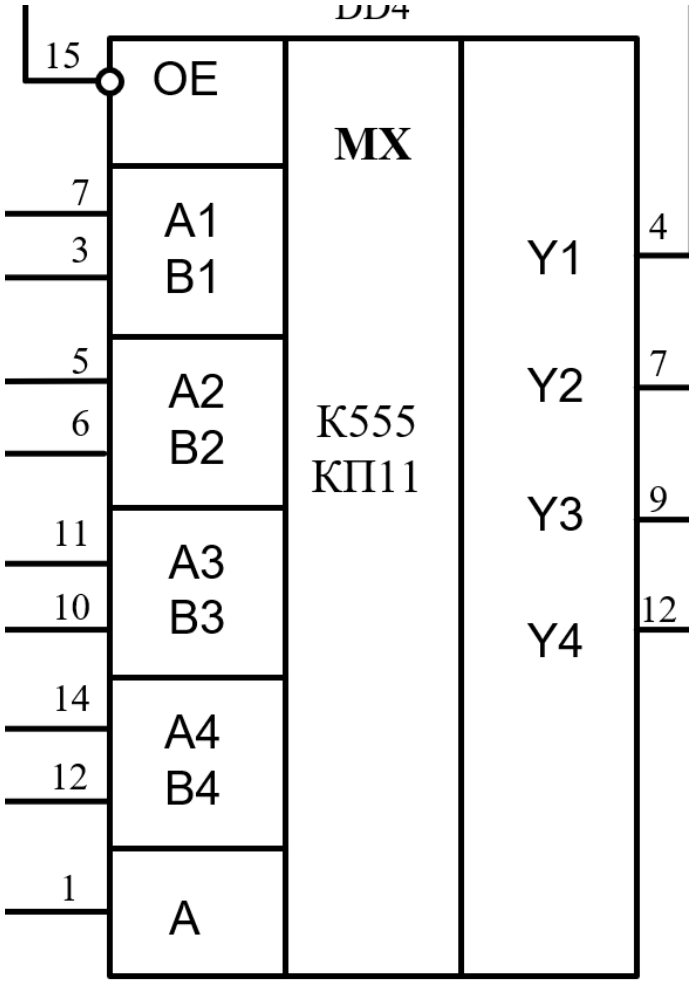

Рис. 4.4 К555КП11 – мультиплексор

Призначення виводів:

A1-A4, B1-B4 – виходи введення

Y1-Y4 – виходи виведення

OE - вхід дозволу виходу

A – вхід вибору каналу

Мікросхема КР580ВВ55А в корпусі продемонстрована на рис. 4.5

Мікросхема КР580ВВ55А програмований пристрій обміну паралельною інформацією застосовується як елемент введення/виведення загального призначення, що сполучає різні типи периферійних пристроїв з магістраллю даних систем обробки інформації.

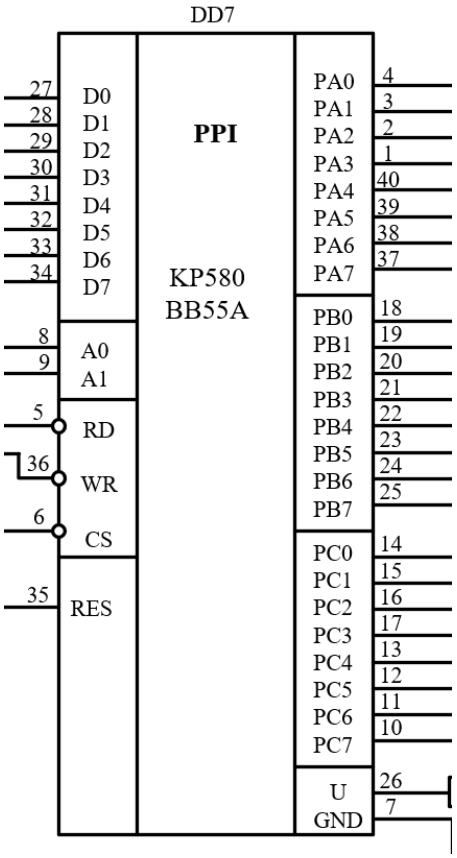

Рис. 4.5 Мікросхема КР580ВВ55А

Обмін інформацією між магістраллю даних МП системи та мікросхеми КР580ВВ55 здійснюється через 8-розрядний двонаправлений тристабільний канал даних (DB). Для зв'язку з периферійними пристроями використовуються 24 лінії введення/виводу в три 8-розрядних канали A.B.C. Напрямок передачі інформації та режими роботи каналів визначається програмним способом. Мікросхема може функціонувати у трьох основних режимах. У режимі 0 забезпечується можливість синхронної програмно керованої передачі даних через два незалежні 8-25 розрядні канали А і В і два 4-розрядні канали С.

У режимі 1 забезпечується можливість введення або виведення інформації або з периферійного пристрою через незалежних 8-розрядних каналу за сигналами квитування. При цьому лінії каналу використовуються для прийому та видачі сигналів керування обміну.

У режимі 2 забезпечується можливість обміну інформацією з периферійними пристроями через двонаправлений 8-розрядний канал по сигналах квитування. Для передачі та прийому сигналів управління обміном використовується 5 ліній каналу С. Вибір відповідного каналу та 12 напрямок передачі інформації через канал визначається сигналами А0, А1 (що з'єднуються зазвичай з молодшими розрядами каналу адреси системи) та сигналами RD, WR, RESET

Значення виводів:

1-4, 37-40 – виводи введення/виведення інформації каналу А

18-25 - виводи введення/виведення інформації каналу В

10-17 - виводи введення/виведення інформації каналу С

27-34 - виводи введення/виведення даних

8,9 – вводи вибору каналу

5 – віід зчитування інформації

36 – вивід запису інформації

6 – ввід вибору мікросхеми

35 – ввід скидання, встановлення у початковий стан

7 – загальний, 26 – живлення

Пвм’ять К537РФ2 в корпусі продемонстрована на рис. 4.6

Пристрій для постійного збереження даних

Значення виводів:

1-8, 19, 22, 23 – вводи адреси

9-17 – виводи введення/виведення

18 - – ввід вибору мікросхеми

20 – ввід дозволу на використання

21 – ввід дозволу на запис

24 – ввід живлення

12 – загальний ввід

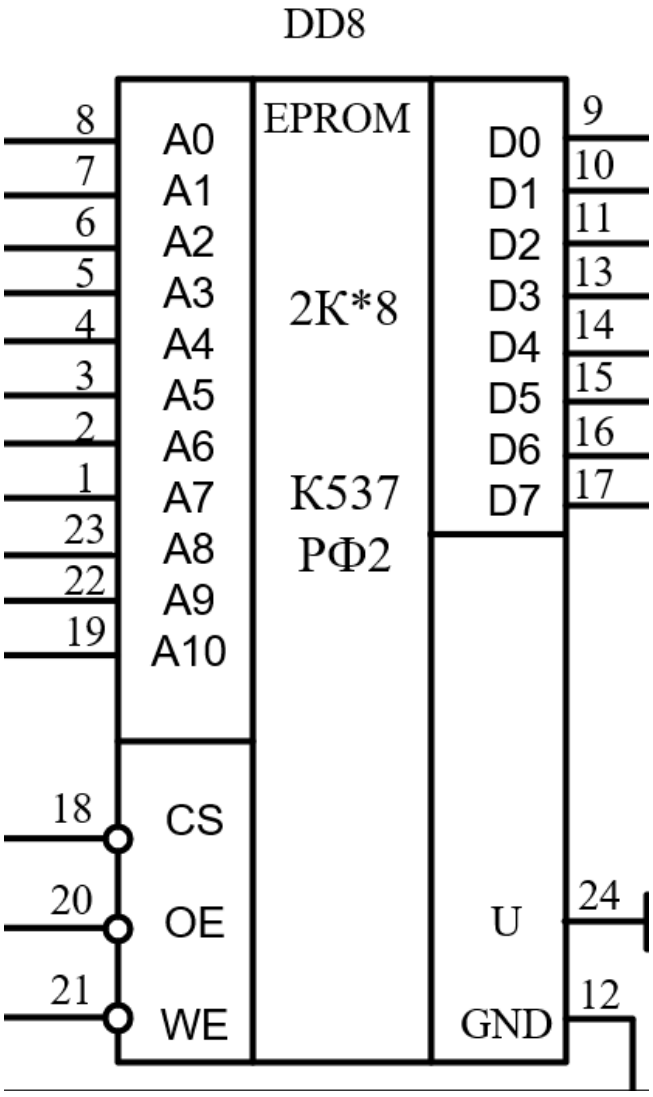

Рис. 4.6 EPROM, постійна пам’ять К537РФ2

Пам’ять К537РУ8 в корпусі продемонстрована на рис. 4.6

Пристрій для оперативного (тимчасового) зберігання даних

Значення виводів:

1-5,14-17 – вводи адреси

13-23 – виводи введення/виведення

8 - – ввід вибору каскаду

24– ввід дозволу на використання

10 – ввід дозволу на запис

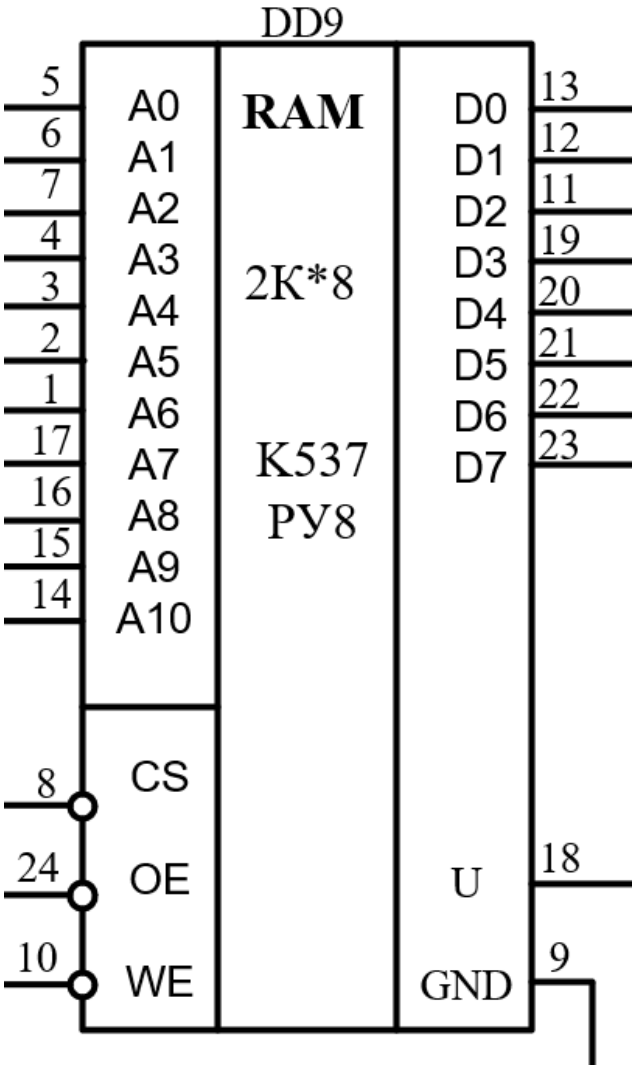
DD9
RAM
2K*8
K537
РУ8
A0
A1
A2
A3
A4
A5
A6
A7
A8
A9
A10
CS
OE
WE
D0
D1
D2
D3
D4
D5
D6
D7
U
GND
5
6
7
4
3
2
1
17
16
15
14
8
24
10
13
12
11
19
20
21
22
23
18
9

Рис. 4.6 RAM

4. РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРИСТРОЮ

Для запуску та налаштування процесора використаємо мову асемблера. Мова асемблера — мова програмування низького рівня для програмованої обчислювальної системи (мікропроцесора, мікроконтролера, комп'ютера або іншого програмованого пристрою), в якій існує сувора відповідність між операторами мови та машинними командами.

Розглянемо приклад вигляду коду на основі використаного процесора:

Приклад програми на мові асемблера для КР1821ВМ85А

```
; Ініціалізація порту B та порту C як виводів
    LDI A, 0xFF      ; Завантажити 0xFF в регістр A
    OUT DDRB, A      ; Записати значення регістра A в регістр DDRB
    OUT DDRC, A      ; Записати значення регістра A в регістр DDRC

; Налаштування таймера
    LDI A, 0x0A      ; Завантажити 0x0A в регістр A (значення для дільника таймера)
    OUT TCCR, A      ; Записати значення регістра A в регістр TCCR (регістр управління таймером)
    LDI A, 0xFF      ; Завантажити 0xFF в регістр A (значення для регістра порівняння таймера)
    OUT OCR, A       ; Записати значення регістра A в регістр OCR (регістр порівняння таймера)

; Увімкнення переривань
    SEI              ; Встановити прапорець глобального дозволу переривань

; Нескінченний цикл
loop:  RJMP loop     ; Нескінчений перехід на мітку loop
```

```
; Обробник переривання від таймера
TIMER_ISR:
    IN A, SREG      ; Зберегти поточне значення регістра стану в регістр A
    PUSH A          ; Покласти значення регістра A в стек

    ; Код обробки переривання

    POP A           ; Завантажити значення з вершини стеку в регістр A
    OUT SREG, A     ; Відновити значення регістра стану з регістра A
    RETI            ; Завершити обробку переривання та повернутися до основної програми
```

Цей код демонструє ініціалізацію портів, налаштування таймера та обробку переривань від таймера, а саме:

1. Ініціалізація портів B і C:

- Завантаження значення 0xFF у регістр A.

- Запис цього значення у регістр DDRB для налаштування порту B як виводу.

- Запис цього значення у регістр DDRC для налаштування порту C як виводу.

2. Налаштування таймера:

- Завантаження значення 0x0A у регістр A, що відповідає значенню дільника таймера.

- Запис цього значення у регістр TCCR (регістр управління таймером).

- Завантаження значення 0xFF у регістр A, що відповідає значенню регістра порівняння таймера.

- Запис цього значення у регістр OCR (регістр порівняння таймера).

3. Увімкнення переривань:

- Установка прапорця глобального дозволу переривань (SEI), що дозволяє обробляти переривання.

4. Бескінечний цикл (безкінечна петля):

- Безкінечний перехід (RJMP) на мітку "loop", що забезпечує постійне повторення коду всередині циклу.

5. Обробник переривання від таймера:

- Збереження поточного значення регістра стану (SREG) у регістр A.

- Положення значення регістра A на стек.

- Код обробки переривання, який виконується при спрацюванні таймера.

- Завантаження значення з вершини стеку в регістр A.

- Відновлення значення регістра стану із регістра A.

- Повернення з обробки переривання до основної програми за допомогою команди RETI

ВИСНОВКИ

Протягом даної роботи розроблено пристрій криптографічного перетворення інформації згідно ГОСТ 28147 : 2009.

Для виконання мети розглянули науковий матеріал та наведений принцип криптографічного методу перетворення даних. На його основі розробили алгоритм роботи, виконаний у вигляді блок-схеми.

Використовуючи знайдену інформацію побудована схема електрична структурна. Вона складається з блоків та зв’язками між ними, функції яких пов’язані з елементами алгоритму та детально описані.

Принципова схема розроблялася виходячи з поставлених задач, сформованих у структурній схемі. Додатково, розглядалось питання простоти компонентів пристрою. Через це використані схеми місцевого виробництва.

СПИСОК ЛІТЕРАТУРИ

1. «175 Zettabytes By 2025» 2018 https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/?sh=4b329d3b5459

2. Ю. С. Грищук: МІКРОКОНТРОЛЕРИ: АРХІТЕКТУРА, ПРОГРАМУВАННЯ ТА ЗАСТОСУВАННЯ В ЕЛЕКТРОМЕХАНІЦІ Харків НТУ «ХПІ» 2019 https://repository.kpi.kharkov.ua/server/api/core/bitstreams/fd62cd97-3ae1-4bf7-b213-2f37c6f4e72c/content

3. «Даташит КМ1821ВМ85» http://datasheets.chipdb.org/Soviet/8085/im1821vm85a_rus.pdf

4. «Теорія електричного зв'язку» https://tks.nau.edu.ua/wp-content/uploads/2016/10/TEORIYA-ELEKTRYCHNOGO-ZVYAZKU.pdf

5. Голь В. Д., Ірха М. С. СИСТЕМИ ПЕРЕДАЧІ ДАНИХ Київ 2021 https://ela.kpi.ua/bitstream/123456789/45443/3/SPD_konspekt.pdf

6. Даташит https://studfile.net/preview/4252765/

7. Статті про криптографію https://esu.com.ua/article-1576

8. Захист інформації в телекомунікаційних системах https://tks.nau.edu.ua/wp-content/uploads/2016/05/Zahyst-informatsiyi-v-telekomunikatsijnyh-systemah.pdf

9. Введение в криптографию / под ред. Ященко. — Litres, 2017

10. Даташит https://www.alldatasheet.com

11. Технологія блокчейн як інструмент побудови розподіленої системи довіри в системах моніторингу громадського транспорту\ студ. Мазуркевич О.А., студ. Орлов В.В., асп. Сердюк В.В. Керівник: доц. Бережна О.В директор Арбузов В.В., \Фізика, електроніка, електротехніка (ФЕЕ-2022). Матеріали та програма науково-технічної конференції. – Суми: СумДу, 2023. – С.82

Поз..	Ім'я	К-сть.	Примітка
	Мікросхеми		
DD1	КР1821ВМ85А	1	
DD2-3	КР580ІР82	2	
DD4	КР580ВА86	1	
DD5	К555КП11	1	
DD6	АБО на 2 входи	1	
DD7	АБО на 4 входи	1	
DD8	КР580ВВ55А	1	
DD9	К537РФ2	1	
DD10-11	НЕ-І з двома входами	2	
DD12	К537РУ8	1	
	Резистори		
R1-R5	*1 Мега ОМ*	5	
	Конденсатори		
C1-C3	*1 пікофрадні*	3	
	Резонатори		
ZQ	*КХО-97 20MHz*	1	

Изм.	Лист	№ докум.	Подпись	Дата	ЕлІТ 6.171.00.10.239 ПЗ		
Разраб.		Орлов В.В.			Пристрій криптографічного перетворення даних згідно ДСТУ ГОСТ 28147:2009 Перелік елементів	Лит.	Лист 1 / Листов 1
Провер.		Бережна О.В.					
Реценз.						СумДУ, гр. ЕС-91	
Н. Контр.		Бережна О.В.					
Утверд.		Опанасюк А.С.					