МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Комп'ютерна графіка і Web-дизайн»

Група: 4ФКГ-06

Дипломний проект

здобувача освіти денної форми навчання
ФКГ.06.05.000.ДП

КУДРЯВЦЕВА
ОЛЕКСАНДРА ІГОРОВИЧА

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: «**Комп'ютерна графіка і Web-дизайн»**

Група: **4ФКГ-06**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи) на тему:

Розробка пристрою крипто-захисту каналу конфіденційного електрозв'язку

Проектний матеріал складається з пояснювальної записки на 68 сторінках та графічного (презентаційного) матеріалу на 16 аркушах (слайдах).

Дипломник _____ (Кудрявцев О.І.)

Керівник _____ (Кірєєв І.А.)

Консультанти:

з економічної частини _____ (Кухарук А.А.)

з охорони праці _____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Кривченко А.А.)

До захисту допущений

Голова циклової комісії _____ (Кривченко Ю.В.)

Завідувач відділення _____ (Скорнякова О.В.)

Захист «27» червня 2023 р. Протокол ДКК № 7

Оцінка ДКК 4 (добре)

Секретар ДКК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення **комп'ютерних систем** Комісія **КТ та ПІ**

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **«Комп'ютерна графіка і Web-дизайн»**

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР _____

Беркань І.В.

"_____" _____ 2023 р.

ЗАВДАННЯ

на дипломний проект (роботу)

здобувачеві (здобувачці) освіти Кудрявцева Олександра Ігоровича

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Розробка пристрою крипто-захисту каналу конфіденційного електрозв'язку

затверджена наказом по коледжу від "17" жовтня 202 2 р. № 235-А2-ОД

2. Термін здачі закінченого проекту (роботи) 12.06.2023

3. Вихідні данні до проекту (роботи) 1. Вимоги конфіденційного електрозв'язку при передачі мовних повідомлень; 2. Специфікації стандарту шифрування DES (Data Encryption System); 3. Передбачити роботу пристрою в режимах відкритої та закритої передачі; 4. Застосувати мікроконтролер для виконання функцій шифрування та дешифрування; 5. Передбачити роботу не менш ніш з 64 ключами, їх зберігання та вибір

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Побудова пристроїв конфіденційного зв'язку; Організація алгоритму засекречування даних DES; Розробка технічних вимог до пристрою крипто-захисту; Розробка функціональної схеми пристрою крипто-захисту; Розробка та опис принципової електричної схеми пристрою крипто-захисту; Розробка алгоритмічного забезпечення пристрою; Розробка програмного забезпечення для мікроконтролера пристрою крипто-захисту

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Структурна схема крипто-захисту каналу передачі конфіденційної інформації; Блок-схема алгоритму шифрування DES та обчислення ключових блоків; Принципова електрична схема пристрою крипто-захисту; Алгоритм роботи пристрою крипто-захисту каналу передачі конфіденційної інформації; Підпрограми обробки переривань від INT1 (низький пріоритет) та від INT0 (низький пріоритет); Підпрограми обробки переривань від T/C0 (високий пріоритет) та від УАПП (високий пріоритет); Кроки моделювання алгоритму DES при шифруванні даних

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1.Технологічний	Кірєєв І.А.		
розділ			
2.Екон. частина	Кухарук А.А.		
3.Охорона праці	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		

7. Дата видачі завдання 01.05.2023

Керівник Кірєєв І.А. _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1.	Вступ. Постановка задачі проектування	22.05.2023	виконано
2.	Побудова пристроїв конфіденційного зв'язку	24.05.2023	виконано
3.	Модель криптографічної системи та методи шифрування	25.05.2023	виконано
4.	Організація алгоритму засекречування даних DES	26.05.2023	виконано
5.	Вимоги до системи крипто-захисту у стандарті DES	29.05.2023	виконано
6.	Розробка технічних вимог до пристрою крипто-захисту	30.05.2023	виконано
7.	Розробка функціональної схеми пристрою крипто-	1.06.2023	виконано
	захисту		
8.	Розробка та опис принципової електричної схеми	2.06.2023	виконано
	пристрою крипто-захисту		
9.	Розробка алгоритмічного забезпечення пристрою	5.06.2023	виконано
	крипто-захисту		
10.	Розробка програмного забезпечення для	7.06.2023	виконано
	мікроконтролера пристрою крипто-захисту		
11.	Економічні розрахунки та аналіз питань техніки безпеки	10.06.2023	виконано
12.	Оформлення креслеників та ПЗ проекту	11.06.2023	виконано

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			ФКГ 06. 05 000. 00 ДП	Дипломний проект		
А4			ФКГ 06. 05 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	ФКГ 06. 05 000. 00 ДП		
Розробив		Кудрявцев О.І.			Розробка пристрою крипто-захисту каналу конфіденційного електрозв'язку	Літ.	Аркуш 4 / Аркушів 68
Перевірив		Кірєєв І.А.				Н Д П	
Н. Контр.		Петрашова В.І.				ВСП "ОТФК ОНТУ" гр.4ФКГ-06	
Затверд.		Кривченко Ю.В.					

ЗМІСТ

ВСТУП

Аналіз різних способів отримання інформації про конкурентів дозволив встановити, що підслуховування телефонних переговорів у ряді випадків може бути одним з ефективних способів несанкціонованого доступу до конфіденційної інформації.

Найефективнішим способом захисту телефонних повідомлень від несанкціонованого доступу є криптографічне перетворення. Дійсно, для того, щоб приховати від зловмисників смисловий зміст телефонного повідомлення, його необхідно певним чином змінити. При цьому змінити його так, щоб відновлення початкового повідомлення санкціонованим абонентом здійснювалося дуже просто, а відновлення повідомлення зловмисником було б неможливим або вимагало б істотних часових або матеріальних витрат, що робило б сам процес відновлення неефективним.

Саме такими властивостями і володіють криптографічні перетворювачі, завданням яких є забезпечення математичними методами захисту конфіденційних телефонних повідомлень. Навіть у разі їх перехоплення зловмисниками і обробки будь-якими способами з використанням самих швидкодіючих суперкомп’ютерів і останніх досягнень науки і техніки смисловий зміст повідомлень може бути розкритий тільки в перебігу заданого часу, наприклад протягом декількох десятків років [1].

Єдиний спосіб запобігання перехопленню інформації і розкриття її змісту стороннім – шифрування або скремблювання (перемішування).

Метою дипломної роботи є проектування і опис простої системи, що дозволяє шифрувати передавані дані і дешифрувати отримані по дротяному каналу електрозв'язку для забезпечення їх захисту від несанкціонованого доступу. У якості приймачів і джерел даних виступають комп’ютери і периферійні пристрої, наприклад факсимільні апарати.

Таким чином, у даному дипломному проекті буде розроблено пристрій крипто-захисту каналу конфіденційного електрозв’язку, що дозволить проводити безпечний обмін важливою інформацією між абонентами.

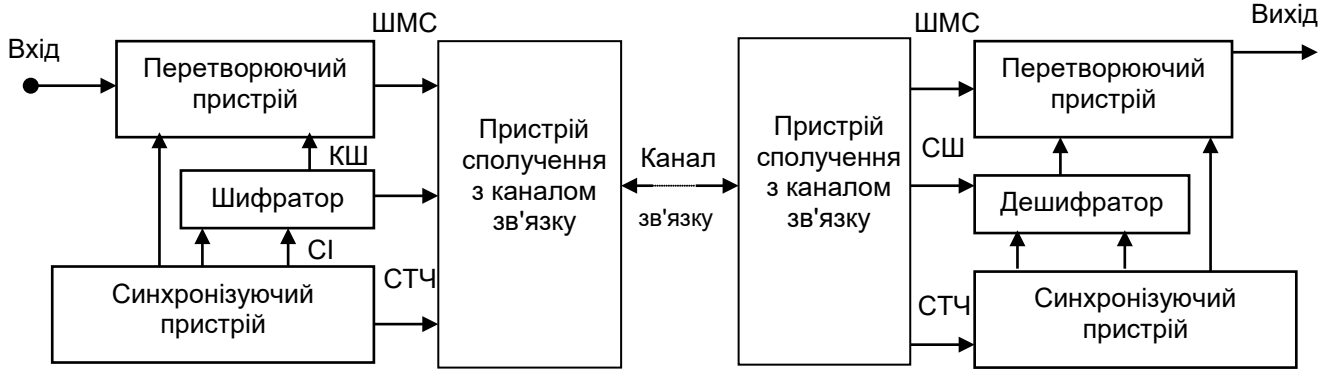
1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Побудова пристроїв конфіденційного зв'язку

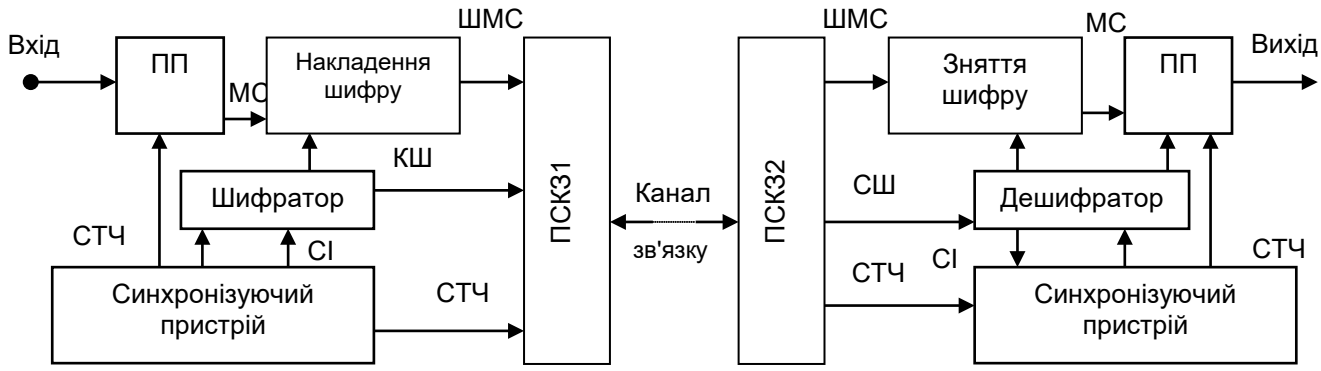
Пристрої конфіденційного зв'язку або пристрої захисту (засекречування) телефонних переговорів призначені для таких перетворень мовних сигналів, при яких абоненти, що знаходяться на крайових пунктах системи зв'язку, можуть вести переговори так само, як це відбувається в звичайних телефонних мережах, але в той же час розбірливість мови в каналах і лініях зв'язку (залишкова розбірливість) дуже мала, а в граничному випадку дорівнює нулю.

При застосуванні сучасних технічних засобів перехоплення і обробки сигналів з використанням самої швидкодіючої обчислювальної техніки можливо розкрити зміст переговорів, проте зробити це досить важко, а в деяких випадках практично неможливо або потрібна багаторічна робота.

Структурні схеми всіх відомих пристроїв захисту можна звести до двох різновидів, показаних на рис.1.1.



а)



б)

Рисунок 1.1. Структурні схеми пристроїв захисту мовних сигналів

Інформаційний сигнал поступає на вхід перетворюючого пристрою (ПП). Необхідні для роботи цього пристрою тактові частоти і інші допоміжні сигнали (СТЧ) поступають від синхронізуючого пристрою (СП), який управляє також роботою інших вузлів схеми. Шифроутворюючі пристрої (ШП) виробляють сигнали, необхідні для забезпечення засекречування мовних сигналів (МС), а також сигнали (синхроімпульси – СІ), необхідні для забезпечення синхронної і синфазної роботи приймальної і передавальної частин апаратури. Синхроімпульси СІ встановлюють шифроутворюючі і інші пристрої в початковий стан. По каналу зв'язку (КЗ) передаються зашифровані мовні сигнали (ШМС), сигнали, що синхронізують роботу шифратора і дешифратора (СШ), сигнали необхідні для синхронізації мовоперетворюючих пристроїв і тактових частот (СТЧ). Об'єднання цих сигналів для передачі по каналу зв'язку і їх розділення здійснюється в пристроях сполучення з каналом зв'язку (ПСКЗ).

Алгоритм роботи перетворюючого пристрою на рис.1.1.а. змінюється по командам від шифроутворюючих пристроїв – КШ. У схемі на рис.1.1б. алгоритм роботи ПП не змінюється, а в канал зв'язку поступає сукупність мовних сигналів і сигналів від шифроутворюючого пристрою. Ця сукупність у вузлі накладення шифру (НШ), може формуватися різними методами (складання, перемножування і тому подібне). Зворотне перетворення відбувається у вузлі зняття шифру (ЗШ).

Ступінь захисту інформації або як її іноді називають "стійкість засекречування" у схемах на рис.1.1. визначається роботою двох пристроїв: шифроутворюючого і перетворюючого.

Під стійкістю засекречування можна розуміти здатність протистояти несанкціонованому доступу до передаваної по каналу зв'язку інформації. Одним з основних критеріїв при оцінці стійкості засекречування є відношення тривалості часового інтервалу, необхідного для несанкціонованого розтину інформації до тривалості початкового повідомлення. Зазвичай несанкціонованим розтином інформації займаються фахівці, яких називають дешифрувальниками. Передбачається, що дешифрувальник має доступ до каналу зв'язку і може записати передане зашифроване повідомлення для подальшої багатократної

обробки, використовує найдосконаліші комп’ютери, йому відома схема і параметри апарату, що засекречує (або він має цей апарат), проте він не знає "ключа", введеного в шифроутворюючий пристрій.

Шифроутворюючі пристрої можуть забезпечити практично будь-яку задану стійкість засекречування. Підвищення стійкості досягається зазвичай за рахунок ускладнення схемно-технічних рішень і, отже, приводить до збільшення вартості устаткування. Враховуючи це, при проектуванні шифроутворюючих пристроїв стійкість засекречування задають з урахуванням техніко-економічних характеристик [2].

При використанні схеми на рис.1.1.а зашифрований сигнал в каналі зв'язку зберігає ряд властивостей початкових сигналів. Наприклад, при перетвореннях мовних сигналів в каналі зв'язку міститимуться більш менш виражені такі ознаки, як: частота основного тону і її гармоніки, місцеположення частот, формант і тому подібне. Використовуючи ці ознаки і статистичні властивості мовних сигналів, можна здійснити дешифровку без аналізу шифроутворюючого пристрою і без визначення "ключа". У цих випадках при скільки завгодно високій криптографічній стійкості шифратора, стійкість засекречування мови може бути відносно невисокої і повністю визначатиметься стійкістю алгоритмів перетворення мови.

Стійкість засекречування, обумовлена зміною алгоритмів перетворень мовних сигналів, для більшості відомих типів мовоперетворюючих пристроїв також може бути оцінена на основі достатньо строгих критеріїв і методів. Підвищення стійкості засекречування також, як і для шифроутворюючих пристроїв, приводить до ускладнення технічних рішень. При цьому, як правило, при ускладненні алгоритмів перетворень погіршується якість і розбірливість мовних сигналів на виході дешифруючого пристрою. Тому отримати дуже високу стійкість засекречування за рахунок ускладнення алгоритмів перетворення мовних сигналів практично неможливо.

При використанні схеми на рис.1.1а. практично неможливо добитися усунення ознак початкових сигналів в каналі зв'язку і відповідно стійкість

засекречування відносно невисока. Проте, враховуючи, що технічна реалізація подібної схеми зазвичай простіша, а також те, що у ряді випадків достатньо зберегти конфіденційність переданої інформації в перебігу обмеженого часу, схема на рис.1.1а. має достатньо широке застосування.

Використання схеми на рис.1.1б. дозволяє повністю позбавитися від наявності ознак початкових мовних сигналів в каналі зв'язку. Це можна зробити, наприклад, перетворивши мовні сигнали, що поступають на вузол накладення шифру (НШ), в двійкові імпульси. Стійкість засекречування в цьому випадку може бути скільки завгодно високою і визначається криптографічною стійкістю шифроутворюючих пристроїв [2].

Слід зазначити, що при сучасному рівні розвитку мікроелектроніки і цифрових методів обробки сигналів, у всіх типах пристроїв захисту інформації, зокрема мовної, всі основні перетворення сигналів, як правило, здійснюються в цифровому вигляді. При цьому в ПП спочатку розташований аналогово-цифровий перетворювач (АЦП), потім проводиться обробка цифрових сигналів. На виході ПП може бути включений цифро-аналоговий перетворювач (ЦАП) і в канал зв'язку при цьому поступають аналогові сигнали. У загальному випадку шифратори, перевершуючи скремблери по складності, мають вищу стійкість засекречування. Двійкова послідовність абсолютно не розрізняється людським вухом. Перетворена в цифрову форму мова звучить подібно до безперервного виску. Двійкова послідовність пропускається через блок шифрування, який змінює її відповідно до математичної формули, відомої тільки учасникам засекреченого зв'язку. Дешифрувати зашифровану розмову, не маючи в своєму розпорядженні ключа шифрування, практично неможливо, оскільки число можливих варіантів ключів майже безмежно.

Аналогові сигнали, "засекречені" скремблером, можна прослуховувати "неозброєним" вухом. Для непрофесійного слухача скрембльована мова звучатиме подібно до іноземної мови, але для того, хто знає, як перетворити шифротекст у відкритий, вона буде осмисленою.

Застосовані кодові комбінації можуть бути відновлені спеціально підготовленими аналітиками, навченими розпізнаванню і інтерпретації засекреченої за допомогою скремблерів мови. Більш того, спеціалізоване лабораторне устаткування для електронного аналізу дозволяє легко розкривати засекречений аналоговий сигнал, оскільки кількість можливих комбінацій при скремблюванні менша, ніж при цифровому зв'язку.

Переваги цифрового методу шифрування над аналоговим (частотно-часовими перестановками) зведені в таблицю 1.1.

Таблиця 1.1. Переваги цифрового методу шифрування

Метод шифрування	**Аналоговий**	**Цифровий**
Наявність переговорів в лінії зв'язку	Є виразні ознаки	Немає ніяких ознак, оскільки в лінію йде чистий шифр (лінійний режим)
Розподіл амплітуди сигналу	Є ритм і гучність	У каналі зв'язку однорідна двійкова послідовність
Постійне шифрування в 4-дротяному каналі зв'язку	Неможливо	Можливо
Короткочасний спектр сигналу	Спектральні характеристики однорідні	Спектральні характеристики неоднорідні

1.2 Модель криптографічної системи та методи шифрування

В даний час для шифрування телефонних переговорів застосовують два принципово різних методи: перетворення аналогових параметрів мови і цифрове зашифровування. Обидва методи передбачають використання шифроутворюючих пристроїв, аналогічних тим, які використовуються в шифромашинах для обробки текстових повідомлень. Найбільш відомі роботи Шенона, зокрема доповідь "Теорія зв'язку в секретних системах". У основі цих робіт лежать наступні припущення:

- Криптограф намагається знайти методи забезпечення секретності і (або) автентичності (достовірності) повідомлень;

- Криптоаналітик намагається виконати зворотне завдання: розкрити шифротекст або підробити його так, щоб він був прийнятий як справжній;

- При цьому допускається, що криптоаналітик супротивника має повний шифротекст і йому відомий алгоритм шифрування, за винятком секретного ключа;

- При розробці методів найбільш надійного захисту інформації, криптограф допускає також, що криптоаналітик супротивника може мати декілька уривків відкритого тексту і відповідного йому шифротексту. На основі цього криптоаналітик може нав'язати фіктивний текст;

- Можливо також, що криптоаналітик супротивника може спробувати нав'язати раніше отриманий шифротекст замість фактично передаваного.

Модель криптографічної системи, запропонованої Шеноном, показана на рис.1.2.

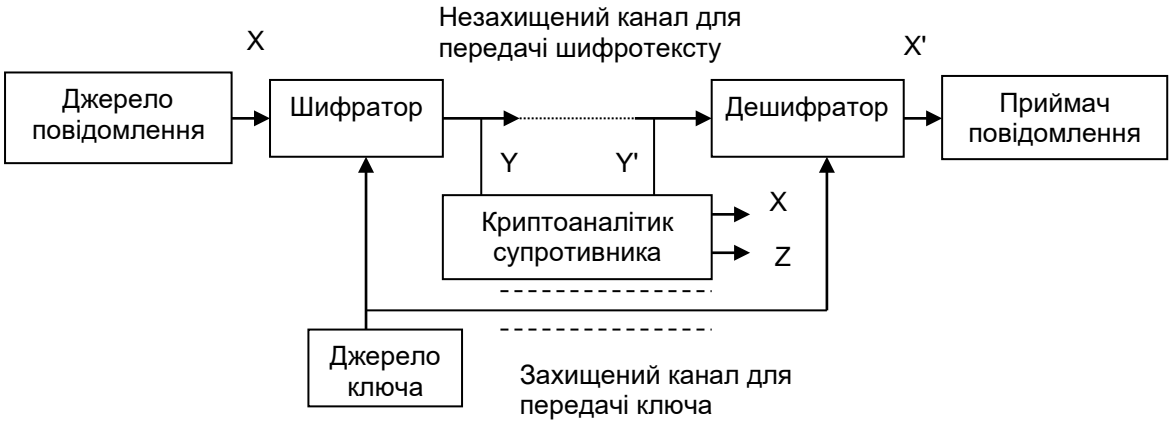


Рисунок 1.2. Модель криптографічної системи

Джерело повідомлень породжує відкритий текст

$$X=\{x1,x2,\dots xm\} \qquad (1.1)$$

Джерело ключів генерує *k* знаків ключа – символів деякого кінцевого алфавіту. Шифратор перетворить відкритий текст X в шифротекст:

$$Y=\{y1,y2,\dots ym\} \qquad (1.2)$$

Останнє перетворення записується у вигляді:

$$Y=Ez(X) \qquad (1.3)$$

Дешифратор, отримавши шифротекст, виконує зворотне перетворення:

$$X=Dz(Y) \qquad (1.4)$$

Важливою частиною моделі криптографічної системи є "захищений" канал, по якому передається секретний ключ:

$$Z=\{z1,z2,\dots zk\} \qquad (1.5)$$

Таким каналом може бути канал електрозв'язку з шифруванням іншими пристроями, ніж показані на рис 1.2, проте частіше ключі розвозяться спеціальними співробітниками. В цьому випадку ключ є таблицею цифр, перфострічкою, магнітною карткою або іншим типом носія із записаною інформацією.

Слід особливо відзначити, що X, Y і Z – незалежні випадкові величини. Статистичні властивості величини X визначаються джерелом повідомлення, Y задається розробником криптографічної системи, а Z створюється і тиражується спеціальним пристроєм заготівки ключів (джерелом ключа).

Шенон довів, що при двох допущеннях абсолютно секретні системи існують. Ці допущення наступні:

- секретний ключ використовується тільки один раз;
- криптоаналітику доступний лише шифротекст.

На основі цих допущень досконала секретність означає, що відкритий текст X і шифротекст Y статистично незалежні, тобто

$$P(X=x|Y=y)=P(X=x) \qquad (1.6)$$

для всіх можливих відкритих текстів X і шифротекстів Y. Іншими словами криптоаналітик не може поліпшити апостеріорний розподіл вірогідності відкритого тексту, використовуючи знання шифротексту незалежно від того, який час і обчислювальні ресурси він має в своєму розпорядженні для аналізу. Було доведено також, що ключ не повинен бути коротше відкритого тексту тобто K>X [3].

Таким чином, виникає проблема секретного ключа. Вона полягає в тому, що на один знак відкритого тексту потрібний, принаймні один знак секретного ключа. При обробці величезних масивів інформації, наприклад в крупних обчислювальних системах, забезпечити це досить складно або таке рішення неприйнятне по економічних причинах. Тому у ряді випадків використовують недосконалі шифри, що не забезпечують досконалу секретність.

Поява на ринку пристроїв захисту конфіденційної інформації з оригінальними ("фірмовими") алгоритмами перетворень сигналів створює непереборні труднощі при необхідності обміну інформацією між абонентами, що мають пристрої різних фірм. Крім того, деякі "фірмові" алгоритми не забезпечують необхідного ступеня захисту, головним чином ті, які розроблені недостатньо кваліфікованими фахівцями. З метою усунення цих недоліків в США був прийнятий стандарт засекречування даних DES (Data Encryption Standard), затверджений Національним бюро стандартів США. У цьому стандарті вперше був запропонований алгоритм засекречування загального користування, придатний для виробників і споживачів пристроїв захисту інформації в мережах передачі даних. До цього на комерційному ранці існувала безліч нестандартизованих алгоритмів [4].

1.3 Організація алгоритму засекречування даних DES

Алгоритм DES розроблений для шифрування і дешифровки блоків даних, що складаються з 64 битів, при дії на них ключа, також 64 біта. Дешифровка здійснюється за допомогою того ж самого ключа, який використовується для шифрування, але з адресацією битів, видозміненою так, щоб дешифровка була б зворотною процесу шифрування. Блок, який повинен бути зашифрований, спочатку піддається початковим перестановкам IP, потім складному перерахунку, залежному від ключа, і в кінці, перестановкам IP-1, які є інверсними початковим перестановкам. Перерахунок, залежний від ключа, може бути визначений як перетворення відповідно до функції шифрування f, функції розподілу ключів KS. На рис 1.3 наведена схема алгоритму шифрування.

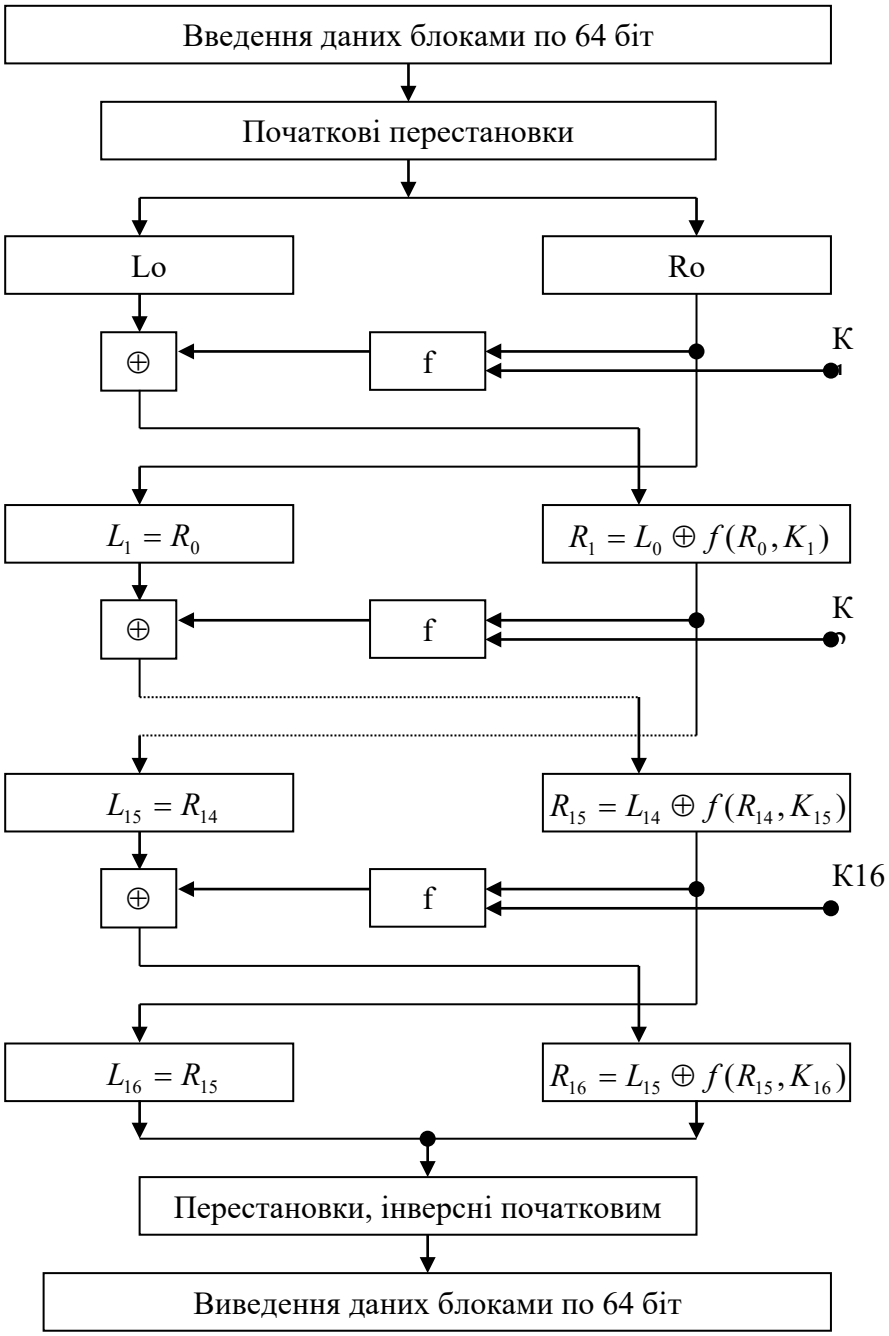


Рисунок 1.3. Алгоритм шифрування DES

Введення даних проводиться блоками по 64 біта. Спочатку проводяться перестановки відповідно до таблиці 1.2.

При цьому, наприклад, 58-й інформаційний біт вхідного блоку вийде як перший, 50-й як другий, 2-й біт вийде 8-м, 1-й біт - 40-м.

Потім вхідний блок з переставленими бітами поступає на схему перерахунків, яка складається з 16 послідовно включених вузлів – повторювачів (перетворення в кожному з них повторюють попередні).

Таблиця 1.2. Початкові перестановки (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Тут інформаційний блок (64 біта) розбивається на дві частини L і R по 32 біта, які поступають на два входи повторювача. Вхідний блок тепер може бути позначений як LR. На третій вхід повторювача поступають блоки K по 48 бітів з схеми утворення "ключа". Блоки R і K обробляються згідно із законом, який задається шифрувальною функцією f(R,K). Кожен біт отриманого блоку завдовжки 32 біта складається по модулю два з бітами блоку L.

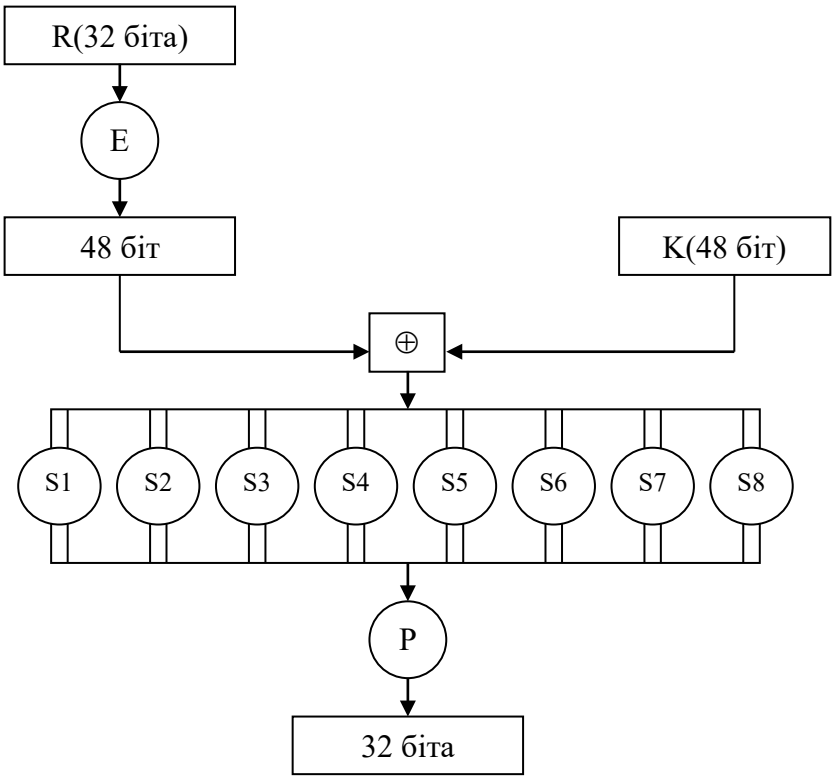


Рисунок 1.4. Обчислення f(R,K)

При цьому вихідні блоки L’ і R’ повторювача при вхідних блоках L і R і ключу K будуть рівні:

L’=R

R’=L (+) f(R,K),

де (+) – позначає складання по модулю два інформаційних біт, що поступають з одного і іншого напряму.

Алгоритм обчислення f(R,K) наведений на рис. 1.4.

Тут E – функція яка перетворить 32 біта (на вході) в 48 бітів (на виході). 48 біт виходу (8 блоків по 6 бітів) виходять вибором бітів (вхідних) відповідно до таблиці 1.3.

Таблиця 1.3. "E"(таблиця бітового вибору)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Далі функція Sn 6 біт (на вході) перетворить в 4 біта (на виході). Розглянемо це перетворення на прикладі функції S1:

Таблиця 1.4

Рядок	**Номер стовпця**															
№		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0		14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1		0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2		4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3		15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	3

Таблиця 1.5. Функція перестановки P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Таблиця 1.6. Функції S1…S8

S1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	4	2	3	6	15	0	9	10	4	5	3
S6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Якщо S1 – функція, визначена в цій таблиці і B – блок з 6 бітів, то S(B) визначається: перший і останній біти в блоці B у двійковій системі представляють число в області 0-3. Нехай це число рівне i. Середні 4 біта в блоці B у двійковій системі представляють число в області 0-15. Нехай це число рівне j. Знайдемо в таблиці число в i-й колонці і j-м стовпці. Це число в області від 0 до 15 і в двійковій системі представляється 4-х бітовим блоком. Цей блок є виходом S1 для введеного B. Наприклад, якщо B=011011, то номер колонки

дорівнює 1 (01B), номер стовпця 13 (1101B). По таблиці знаходимо а колонці 1 і стовпці 13 число 5, тобто на виході число 0101. Функції S1,S2.S8 приведені в таблиці 1.6. Функція перестановки P визначається таблицею 1.5.

Вихідне значення P(L) для P визначеного цією таблицею виходить таким чином: з блоку L береться 16-й біт L як перший біт P(L), 7-й біт як другий біт P(L), і так далі поки 25-й біт L не узятий як 32-й біт P(L).

Тепер нехай S1,...,S8 будуть вісім функцій вибору, P – функція перестановки і нехай E буде функція, визначена вище.

Для того, щоб визначати f(R,K) ми спочатку визначаємо B1...,B8 (по 6 бітів кожен):

$$B1B2...B8 = K(+)E(R) \qquad (1.7)$$

блок f(R,K) потім визначається:

$$P(S1(B1)S2(B2)...S\,8(B8)) \qquad (1.8)$$

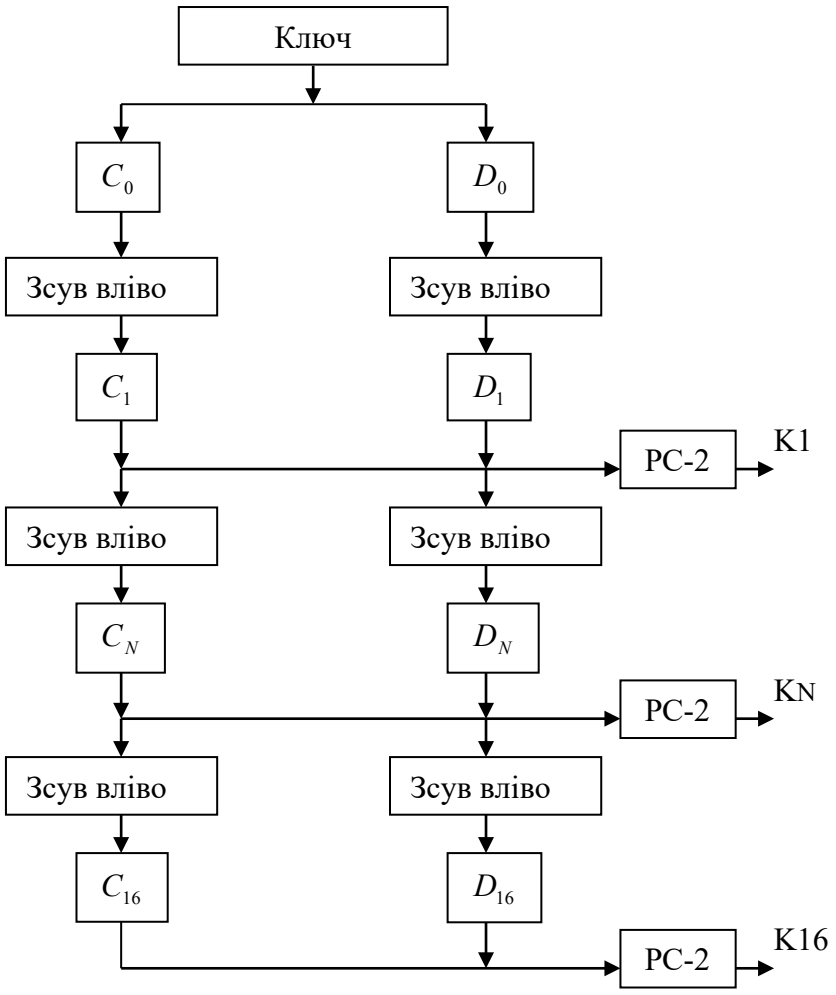


Рисунок 1.5. Алгоритм обчислення ключових блоків

Таким чином, K(+) E(R) спочатку розділяється на 8 блоків, як вказано в (1.7). Потім кожен Bi узятий як введення в Si і 8 блоків (S1(B1) S2(B2)...S8(B8) по 4 біта кожне перетворюються в 1 блок 32 біта, який вводиться в P. Вихід P (1.8) є потім виходом функції f для введення R і K [4].

Прийнято, що KS (n,KEY) є функція, яка визначається цілим числом n, яке змінюється від 1 до 16 (n – номер повторювача) ключем (KEY) з 64 бітів. Алгоритм обчислення Kn наведений на рис.1.5. Розглянемо алгоритм отримання функції KS. Спочатку 64 біт ключа піддаються перестановці PC-1 (таблиця 1.7).

Таблиця 1.7. Додаткові перестановки PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Таблиця розділена на дві частини, в першій частині вибираються біти C0, в другій – біти D0. Біти ключа перераховані з 1 по 64. Біти C0 є відповідно бітами 57, 49, 41..., 44 і 36 ключа, біти D0 є бітами 63, 55, 47..., 12 і 4 ключа.

Таблиця 1.8. Розклад зсувів

№ повторювача	**Число зсувів**
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Після визначення C0 і D0, ми тепер визначаємо блоки Cn і Dn, які виходять з блоків Cn-1 і Dn-1, відповідно, для n = 1, 2..., 16. Це виконується зсувом блоків вліво дотримуючись правил з таблиці 1.8.

Наприклад, C3 і D3 виходять з C2 і D2, відповідно, двома зсувами вліво, і C16 і D16 виходять з C15 і D15, відповідно, одним зсувом вліво.

Перестановки PC-2 визначаються таблицею 1.9:

Таблиця 1.9

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Отже, перший біт Kn – це 14-й біт CnDn, другий біт – 17, і так далі, 47-й – 29-й, і 48-й біт – 32.

Отримана на виході останнього (16-го) повторювача (Рис.1.3) попередня вихідна послідовність піддається перестановкам, інверсним початковим і заданим таблицею 1.10:

Таблиця 1.10. Перестановки інверсні початковим (IP-1)

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

При дешифровці використовується той же самий алгоритм рис.1.3 і ключ, що і при шифруванні. Проте необхідно використовувати зворотний порядок подачі на повторювачі ключових блоків. На перший повторювач подається 16-й ключовий блок (К16), на другий – 15 (К15) і так далі [5].

1.4 Вимоги до системи крипто-захисту у стандарті DES

Основні вимоги, що пред'являються до системи крипто-захисту у стандарті DES:

- забезпечувати високий рівень секретності і в той же час недвозначність і зрозумілість;
- забезпечувати для алгоритму шифрування можливість публічного використання і відкритого існування;
- при цьому необхідно добиватися такого положення, при якому тільки ключ шифру повинен бути секретним, що забезпечить універсальність у використанні алгоритму шифрування;
- запобігти можливості для несанкціонованих супротивників прочитувати дані, замінювати або видозмінювати їх без розкриття.

При виконанні цих вимог необхідно надати можливість санкціонованим користувачам отримати дані з мінімальними вартісними і тимчасовими витратами [6].

Особливі вимоги пред'являються до керування формуванням і розподілом ключів: ключі формуються за допомогою обов'язкових правил. Ключі повинні бути вибрані випадковим чином зі всіх можливих за стандартом DES 2^56 (72 квадрильйони) ключів. Ключі можна утворювати, використовуючи для цього алгоритм стандарту шифрування даних. Кожен вибраний ключ повинен бути незалежний від раніше використаного ключа. Ключі можуть розподілятися і доставлятися кур'єром (уручну) або через закриту пошту, причому повинно бути унеможливлено розкрадання або запис ключів, що доставляються. Ключі можуть розподілятися електронним способом від центру керування і розподілу ключів. В цьому випадку вони повинні зашифровуватися "головним ключем" або "єдиним резервним ключем".

Обов'язково повинні бути прийняті заходи для захисту ключів:

- вони повинні бути захищені від всіх потенційних погроз їх розкриття;
- вони повинні бути знищені, якщо довгий час не будуть потрібні;
- при необхідності ключі повинні бути легко доступні;

- вони повинні зберігатися в пристроях, що реалізовують алгоритм стандарту засекречування даних і повинні бути захищені від сторонніх осіб.

У випадку, якщо ключі були скомпрометовані, або є якась можливість їх компрометації, то необхідно змінити робочі ключі. Ключі повинні бути доступні тим особам, які знають або мають дані, які вони захищають.

Слід пам'ятати, що ключі можуть бути викрадені з системи, а це приведе до втрати великої кількості інформації і до тривалого порушення штатного (нормального) функціонування системи.

У стандарті DES пропонуються деякі протоколи зв'язку.

Для аутентифікації користувача можна використовувати алгоритм однонапрямленого (необоротного) перетворення, при якому код аутентифікації користувача ніколи не може бути обчислений на підставі його еквівалента, поміщеного в пам'ять машини [7].

Двостороння аутентифікація між терміналом і комп'ютером проводиться у тому випадку, коли єдиний ключ шифрування є тільки в апаратурі шифрування (дешифровки) терміналу і комп'ютера.

Достовірність повідомлень можна криптографічно захистити шляхом обчислення криптографічної функції від всіх знаків повідомлення і передачі цього результату (код аутентифікації повідомлень) разом з повідомленням.

Приймач повідомлень обчислює ідентичну криптографічну функцію прийнятого повідомлення, використовуючи такий же секретний ключ, як ключ відправника, і порівнює її з кодом аутентифікації отриманого повідомлення.

Несанкціоноване введення або стирання повідомлень запобігається або виявляється включенням в повідомлення якого-небудь оригінального або унікального числа (імітовставка).

Помилки, введені випадково або навмисно в передавані дані, можна автоматично виявити або виправити шляхом застосування коду, що виявляє або виправляє помилки, який поміщається в кінці передаваного повідомлення і також утворюється криптографічними методами.

Обман, типовим варіантом якого є заміна частини одного повідомлення фрагментом з іншого повідомлення, можна передбачити, використовуючи методи аутентифікації.

Апаратура шифрування повинна встановлюватися в початковий стан з ключем і початковим заповненням, якщо застосовується режим шифрування із зворотним зв'язком. Вільні місця в повідомленні повинні бути заповнені випадковими числами для того, щоб повідомлення утворювало послідовність, кратну 64 бітам. Апаратуру засекречування необхідно синхронізувати, щоб вхід приймача з'єднувався з виходом передавача [8].

У апаратурі зв'язку повинні використовуватися ідентичні формати даних, а також режими шифрування, якщо такі зустрінуться. Виявляти або виправляти помилки слідує як усередині, так і зовні закритих каналів зв'язку.

У пристроях для забезпечення конфіденційності телефонних переговорів немає необхідності виконувати деякі з вимог стандарту DES. Обумовлено це специфікою телефонного зв'язку. Абоненти аутентифікують один одного по голосу, навмисне введення помилкового повідомлення (навіть раніше записаного з того ж голосу) легко виявляється по зміні змісту.

1.5 Розробка технічних вимог до пристрою крипто-захисту

Далі зазначені технічні вимоги до пристрою крипто-захисту каналу конфіденційного електрозв’язку. Відповідно до суті розробки та технічного завдання на дипломне проектування вони є такими:

- система крипто-захисту та взаємодії з периферійними пристроями повинна працювати у режимі відкритої і закритої передачі. У відкритому режимі на передачі інформація не шифрується, відповідно на прийомі не дешифрується. Відкритий режим необхідний для того, щоб можна було домовитися про номер ключа і перехід в закритий режим передачі, а також для передачі не конфіденційної інформації;
- вибір ключа здійснюватимемо комбінацією на DIP-перемикачах, підключених до старших розрядів шини адреси ПЗП;

- процесор повинен постійно аналізувати активність прийому в послідовний порт, і, якщо в нього в перебігу деякого часу не поступає сигнал заданого формату, то запалюється світлодіод "Втрата вхідного сигналу";
- при переході в закритий режим процесор вводить встановлений DIP-перемикачами ключ і продовжує аналізувати активність прийому. Якщо прийом в послідовний порт не відбувається, процесор передає в послідовний порт замість сигналу нулі і мигає світлодіод "Втрата вхідного сигналу";
- у паузах мови (якщо всі 64 біти дорівнюють нулю) в послідовний порт передаватимуться нулі (без шифрування), і, відповідно на прийомі не дешифруватимуться.

1.6 Розробка функціональної схеми пристрою крипто-захисту

З урахуванням зазначених вище вимог, розроблено спрощену функціональну схему пристрою крипто-захисту каналу конфіденційного електрозв'язку (рис. 4.1).

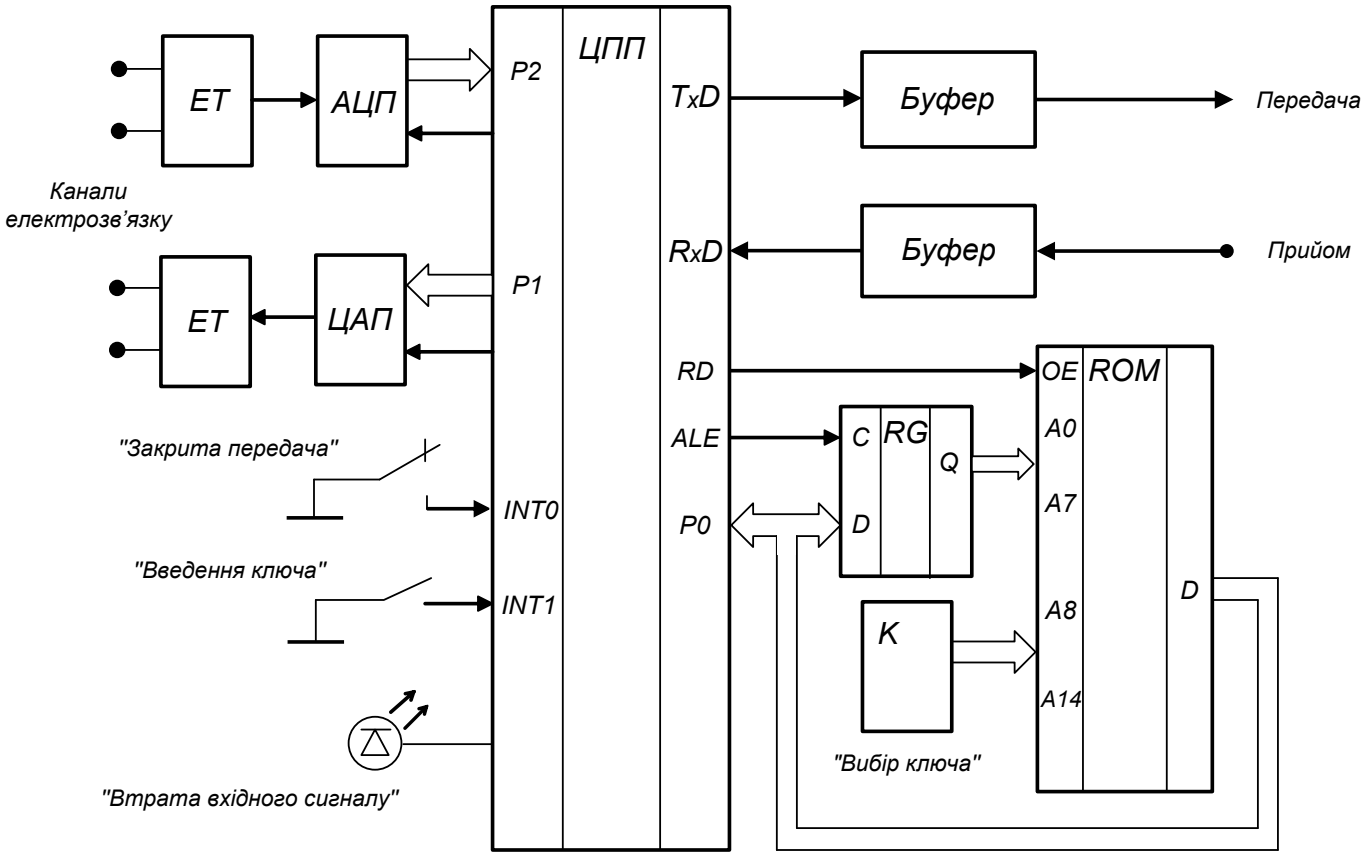


Рисунок 1.6. Функціональна схема пристрою крипто-захисту

Система працює у режимі відкритої і в режимі закритої передачі. Вхідний сигнал через електронний трансформатор (ЕТ) поступає на аналогово-цифровий перетворювач. Електронний трансформатор служить для узгодження вхідного сигналу з АЦП по опору. У аналогово-цифровому перетворювачі сигнал оцифровується і поступає в порт Р2. Програма відправляє черговий звіт в буфер зберігання даних, які підлягають шифруванню, а з буфера зберігання зашифрованих даних, також черговий звіт – в послідовний порт [9].

У закритому режимі після прийому восьми звітів відбувається шифрування, після чого зашифровані дані поступають у відповідний буфер.

У відкритому режимі після прийому 8-ми звітів (64 бітів) вони прямують в буфер зберігання зашифрованих даних без шифрування. Аналогічний процес відбувається при передачі сигналу у зворотному напрямі.

Процесор постійно аналізує активність прийому в послідовний порт, і, якщо в нього не поступає в перебігу деякого часу сигнал заданого формату, то запалюється світлодіод "Втрата вхідного сигналу", а в послідовний порт передає замість сигналу нулі. При переході в закритий режим процесор вводить встановлений DIP – перемикачами ключ, і, якщо прийом в послідовний порт не відбувається, мигає світлодіод "Втрата вхідного сигналу".

1.7 Розробка та опис принципової електричної схеми пристрою крипто-захисту

У пристрої крипто-захисту у відповідності до вимог, викладених у технічному завданні, використовуватимемо мікроконтролер сімейства MCS51 – DS87C520 фірми Dallas Semiconductor, що має наступні характеристики:

Таблиця 1.11

Об'єм резидентної пам'яті програм, Кбайт	16
Тип резидентної пам'яті програм	ПЗП
Об'єм резидентної пам'яті даних, байт	256
Максимальна частота проходження тактових сигналів, МГц	55
Напруга живлення, В	5
Струм споживання, мА	8
Об'єм адресуємої зовнішньої пам'яті програм, Кбайт	64
Об'єм адресуємої зовнішньої пам'яті даних, Кбайт	64

Структурна організація мікроконтролерів DS87C520 показана на рис. 1.7.

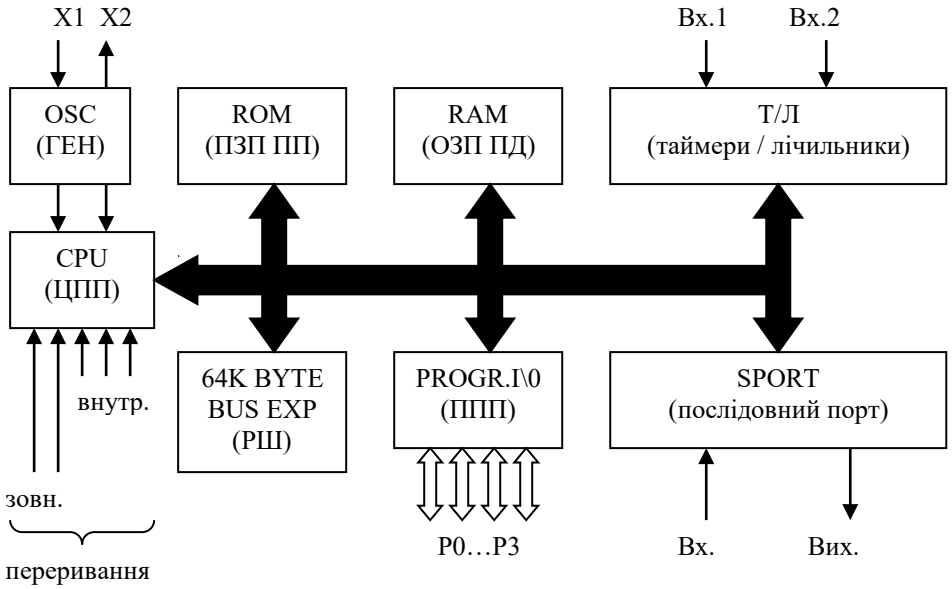


Рисунок 1.7. Структурна схема мікроконтролерів DS87C520

До складу структурної схеми входять наступні функціональні вузли:

- ЦПП – центральний процесорний пристрій;
- ПЗП ПП – постійний запам'ятовуючий пристрій пам'яті програми;
- ОЗП ПД – оперативний запам'ятовуючий пристрій пам'яті даних;
- ГЕН – задаючий генератор;
- ППП – програмовані паралельні порти;
- Послідовний порт;
- Т/Л – таймери/лічильники;
- РШ – розширювач шини для роботи із зовнішніми ЗП ємкістю до 64 Кбайт.

Всі вузли зв'язані між собою загальною восьмирозрядною шиною, по якій здійснюється обмін інформацією між ЦПП і рештою пристроїв.

ЦПП є сукупністю операційного ОП і управляючого УП пристроїв, що виконують програму, записану в ПЗП ПП, ємкість якого складає 16 Кбайт. ЦПП забезпечує виконання наступних груп операцій:

- арифметичні операції (складання, складання з урахуванням перенесення, віднімання з урахуванням позики, беззнакове множення і ділення, інкремент і декремент, десяткова корекція);

- логічні операції (І, АБО, викл. АБО, інверсія);
- операції зсуву;
- операції пересилки;
- бітові операції;
- операції передачі керування.

Проміжні результати обчислень зберігаються в ОЗП ПД ємкістю 256 байт.

Швидкість роботи ЦПП задається генератором, що виробляє необхідні для роботи часові послідовності. Тактова частота задається або кварцовим резонатором, включеним між виводами X1 і X2, або зовнішнім задаючим генератором, що підключається до входу X1 [10].

В цілях забезпечення послідовного доступу до ресурсів процесора при використанні однієї шини генератор формує машинний цикл процесора з чотирьох тактів резонатора (задаючого генератора).

Введення в процесор інформації, належної обробці, може бути здійснений або в паралельній байтовій (введення восьми розрядів однією командою), або в послідовній (по одному біту) формах, так само як і виведення результатів обробки з процесора.

Паралельний обмін інформації можливий через один з чотирьох підтримуваних мікроконтролером ППП.

Послідовний обмін інформацією в принципі може бути організований через будь-який з розрядів ППП, проте для полегшення процесу послідовного обміну і економії обчислювальних ресурсів, необхідних для його реалізації, мікроконтролер оснащений вбудованим програмованим послідовним портом, що дозволяє практично без витрат обчислювальних ресурсів організувати послідовний обмін по декількох видах протоколів.

Окрім розглянутих вузлів, до складу мікроконтролеру включені два шістнадцяти-розрядних таймера/лічильника, які можуть функціонувати або в режимі таймера, або в режимі лічильника зовнішніх подій.

Режим таймера використовується, головним чином, тоді, коли необхідно організувати циклічні процеси жорстко фіксованим і незалежним від часу

виконання програми періодом циклу, наприклад, при обробці мовних сигналів, коли необхідно забезпечити необхідний (по теоремі Котельникова) інтервал дискретизації.

Розширювач шини РШ використовується для роботи із зовнішнім ЗП – пам'яті програм або пам'яті даних. Як правило зовнішнє ЗП використовується тоді, коли для розміщення програми або даних при рішенні якоїсь задачі внутрішніх ресурсів мікроконтролеру виявляється недостатньо, режим роботи із зовнішнім ЗП не є типовим для мікроконтролеру

Система переривань мікроконтролеру DS87C520 підтримує переривання від п'яти джерел:

- INT0 – зовнішнє переривання по стану / зміні стану логічного сигналу на вході INT0 (вивід 12);
- INT1 – зовнішнє переривання по стану / зміні стану логічного сигналу на вході INT1 (вивід 13);
- T/C0 – внутрішнє переривання по переповнюванню таймера/лічильника T/C0;
- T/C1 – внутрішнє переривання по переповнюванню таймера/лічильника T/C0;
- S – внутрішнє переривання від послідовного порту.

Переривання в загальному вигляді є засобом змусити процесор припинити виконання поточної програми і перейти до виконання іншої програми (підпрограми), що є частиною загального для вирішуваного завдання прикладного програмного забезпечення, і асоційованою з даним перериванням.

Кожним джерелом може бути сформований запит на переривання, що встановлює відповідний прапор, обслуговування запитів може бути дозволене або заборонене.

Будь-якому з джерел переривань може бути встановлений високий або низький пріоритет встановленням / скиданням відповідних бітів в регістрі IP; при цьому підпрограми переривань вищого пріоритету можуть переривати підпрограми нижчого.

У пристрої крипто-захисту каналу передачі конфіденційної інформації у якості електронного трансформатору застосуємо операційний підсилювач А747 фірми Fairchild [11].

Операційний підсилювач – це транзисторний багатокаскадний підсилювач постійного струму, виконаного у вигляді ІМС, що обумовлює його особливості схемотехніки. Структурна схема операційного підсилювача на рис.1.8 містить диференціальний вхідний каскад, каскади посилення і вихідний каскад, що забезпечує задану потужність сигналу в навантаженні.

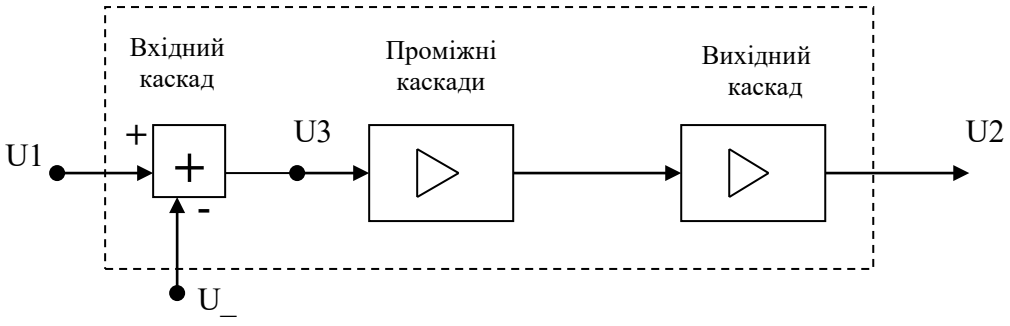


Рисунок 1.8. Структурна схема операційного підсилювача

Диференціальний вхідний каскад є мостовою схемою з двома входами, причому на його вихід сигнал з одного входу (прямого) подається без змін фази, а з іншого входу (інверсного) – у протифазі. Стабільність робочої точки вхідного каскаду забезпечується за рахунок глибокого негативного зворотного зв'язку, що створюється в емітерному ланцюзі, тому вхідний опір входів операційного підсилювача – дуже високий [12].

Основне посилення К=U2/U3 вносять проміжні каскади.

Вихідний каскад операційного підсилювача безтрансформаторний, виконаний на парі компліментарних (з доповнюючими один одного характеристиками) транзисторів, що створюють щодо різнополярних джерел живлення міст.

Двохполярне електроживлення забезпечує рівність потенціалів обох входів і виходу потенціалу корпусу, тому операційний підсилювач зазвичай не потребує ланцюгів розділення по постійному струму.

Операційні підсилювачі завжди охоплюють глибоким паралельним по виходу негативним зворотним зв'язком, сполучаючи вихід з інверсним входом. Завдяки цьому різко поліпшуються їх стабільність, частотні і інші характеристики, знижується до десятків омів вихідний опір. На практиці вхідний опір операційного підсилювача можна вважати нескінченним, а вихідний – нульовим.

Схема операційного підсилювача, що не інвертує сигнал, наведена на рис.1.9.

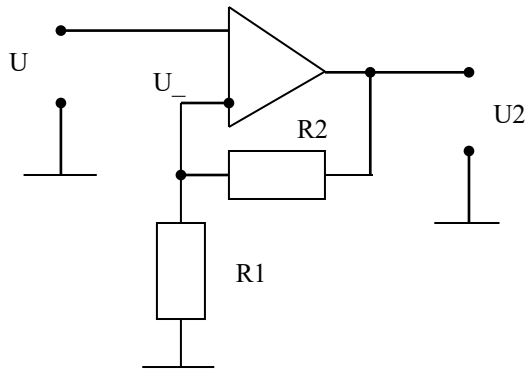


Рисунок 1.9. Схема неінвертуючого операційного підсилювача

У ланцюзі зворотного зв'язку включений дільник напруги з коефіцієнтом передачі:

$$\beta = \frac{R_1}{(R_1 + R_2)} \qquad (1.9)$$

Тоді вираз для коефіцієнта посилення неінвертуючого операційного підсилювача:

$$K_{OC} = \frac{1}{\beta} = 1 + \frac{R_2}{R1} \qquad (1.10)$$

Коефіцієнт посилення, в нашому випадку, рівний двом, тоді R1=R2=10кОм.

Для інвертуючого операційного підсилювача (Рис.1.10) коефіцієнт посилення:

$$K_{инв} = \frac{R_2}{R1} \qquad (1.11)$$

При коефіцієнті посилення рівному одиниці R1=R2=10 кОм.

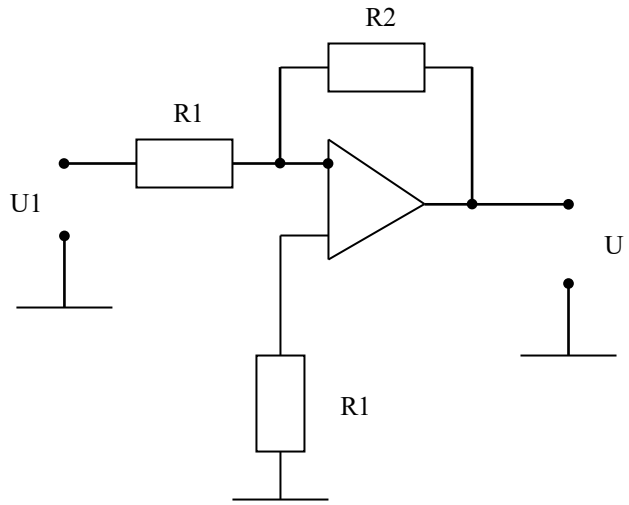


Рисунок 1.10. Схема інвертуючого операційного підсилювача

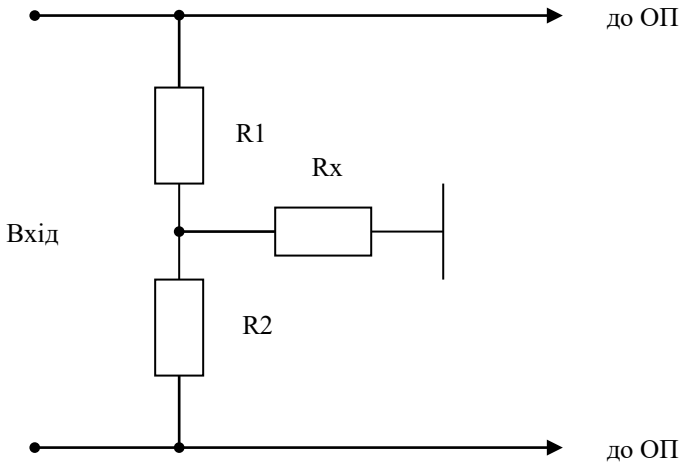


Рисунок 1.11. Пристрій узгодження

На вході операційного підсилювача, для забезпечення необхідного загасання віддзеркалення і асиметрії розрахуємо дільник (рис.1.11) на резисторах R1,R2,Rx.

Загасання віддзеркалення:

$$A_{отр} = 10\lg\left|\frac{(R1+R2)-600}{R1+R2+600}\right| \qquad (1.12)$$

Необхідна Аотр.тр.=26дб, тоді R1=R2=301 Ом.

Захищеність асиметрії:

$$A_{асим} = 20\lg\left|\frac{R1 + Rx + R2 + Rx}{R1 + Rx - (R2 + Rx)}\right| \qquad (1.13)$$

Необхідна Аасим=52дб, тоді при допуску резисторів ±5% Rx=10 кОм.

В якості аналогово-цифрового перетворювача візьмемо ІМС фірми ANALOG DEVICES AD7574. Структурна схема АЦП AD7574 приведена на рис.1.12.

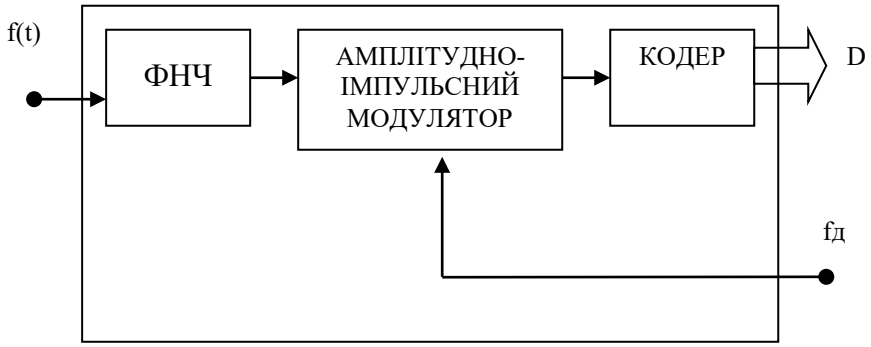


Рисунок 1.12. Структурна схема АЦП AD7574

Аналогово-цифровий перетворювач призначений для перетворення аналогового сигналу в цифровий. Складається з фільтру низької частоти (ФНЧ), який призначений для обмеження смуги частот передаваного телефонного сигналу, амплітудно – імпульсного модулятора і кодера, перетворюючого АІМ сигнал у восьмирозрядний цифровий сигнал, який поступає в порт Р2 мікроконтролера.

Для зберігання комбінацій ключів використаємо ІМС NM256Q. Вона є постійним запам'ятовуючим пристроєм на 2^{15}=32Кбайта. До старших шести розрядів підключимо DIP-перемикачі для вибору ключів, які самі собою є індикаторами. Кількість ключів буде дорівнювати:

$$N = 2^6 = 64$$

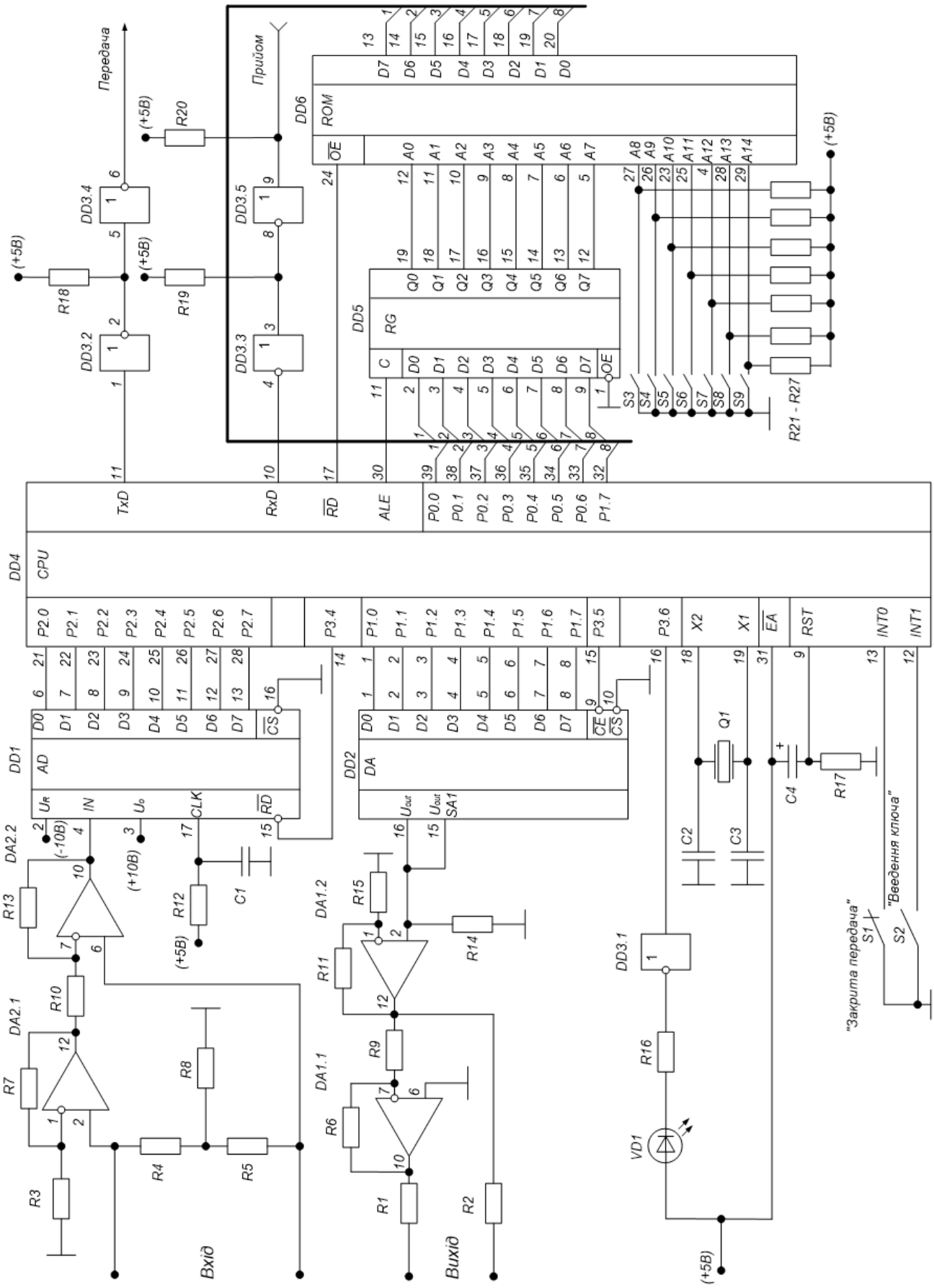


Рисунок 1.13. Принципова електрична схема пристрою криптозахисту

Електричну принципову схему розробленого пристрою крипто-захисту наведено на рис.1.13.

Оскільки для звернення до зовнішнього ПЗП і зчитування з нього даних використано одну шину, то для запам'ятовування адреси комірки використано регістр SN74ALS573. Введення ключа в процесор відбувається таким чином. При зверненні до зовнішньої пам'яті на P0 з'являється адреса комірки, по якій в ПЗП зберігається комбінація ключа, після установки сигналу ALE ця адреса запам'ятовується регістром і з'являється на адресній шині (молодший байт) мікросхеми пам'яті. Після появи сигналу RD з порту P0 зчитуються дані з даної адреси. Для збільшення потужності сигналу на виході і вході системи використано IMC SN74LS05.

1.8 Розробка алгоритмічного забезпечення пристрою

На рис.1.14-1.19 представлена блок-схема алгоритму роботи пристрою крипто-захисту каналу конфіденційного електрозв’язку з урахуванням технічних вимог, розроблених раніше.

У нашому пристрої використовуватимемо переривання в наступних цілях:

INT0 (низький пріоритет, рівневий режим переривань) – для переходу в режим закритої передачі і назад.

INT1 (низький пріоритет, краєвий режим переривань) – для введення ключа.

T/C0 (високий пріоритет) – для формування сигналів керування АЦП з f=64/8=8кГц, T=125мкс (період повторення).

Для отримання необхідної частоти визначимо перезавантажуване число, що міститься в регістрі TH0:

Період машинного циклу при частоті задаючого генератора 55 Мгц:

$$T_{Ц} = \frac{4}{f_T} = \frac{4}{55 \cdot 10^6} = 72 \cdot 10^{-9} \qquad (1.14)$$

Перезавантажуване число дорівнює:

$$n = 256 - \frac{T_{ПОВТ}}{T_{Ц}} = 256 - 173 = 83 \qquad (1.15)$$

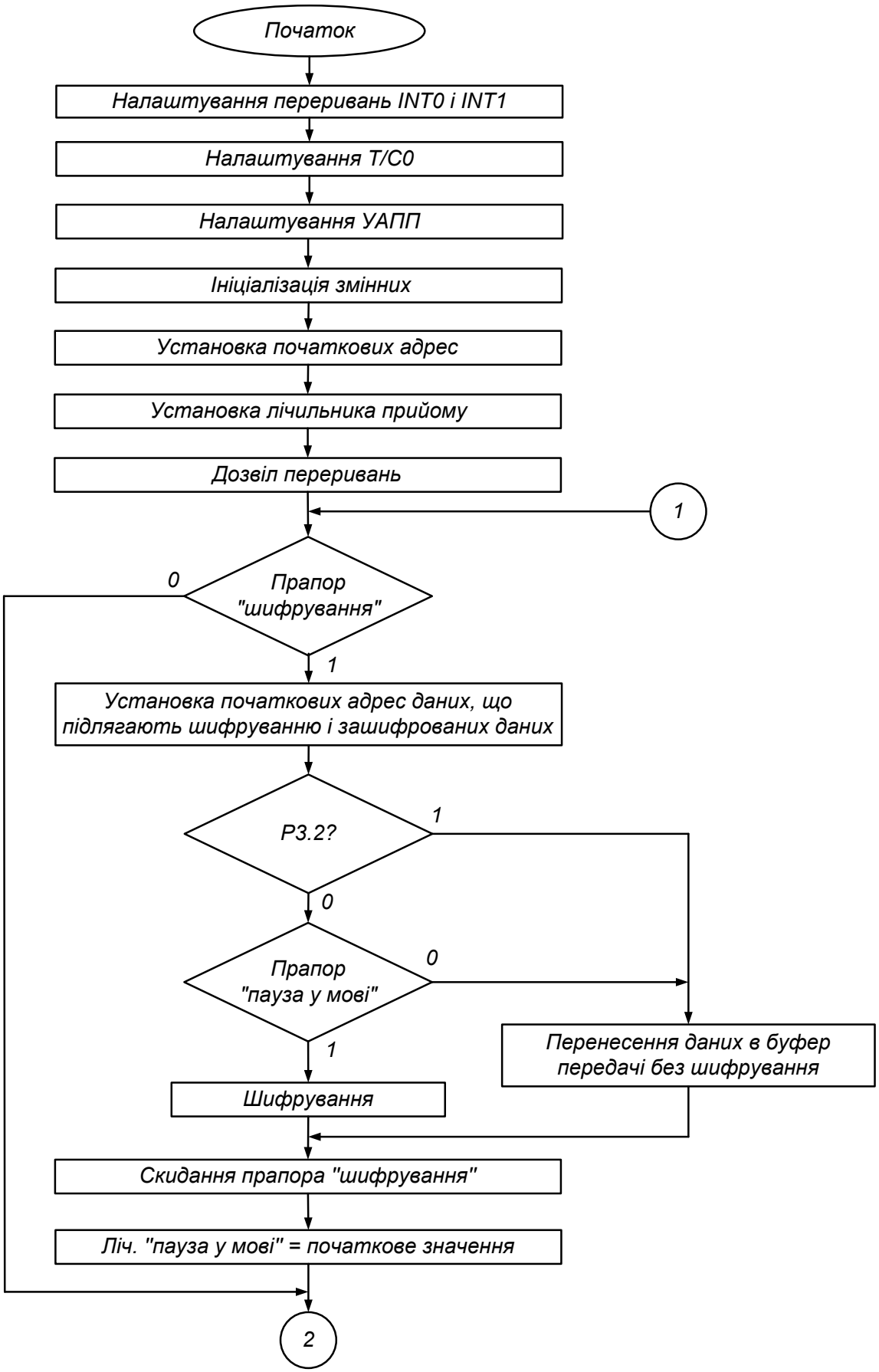


Рисунок 1.14. Алгоритм роботи пристрою криптозахисту каналу передачі конфіденційної інформації (початок)

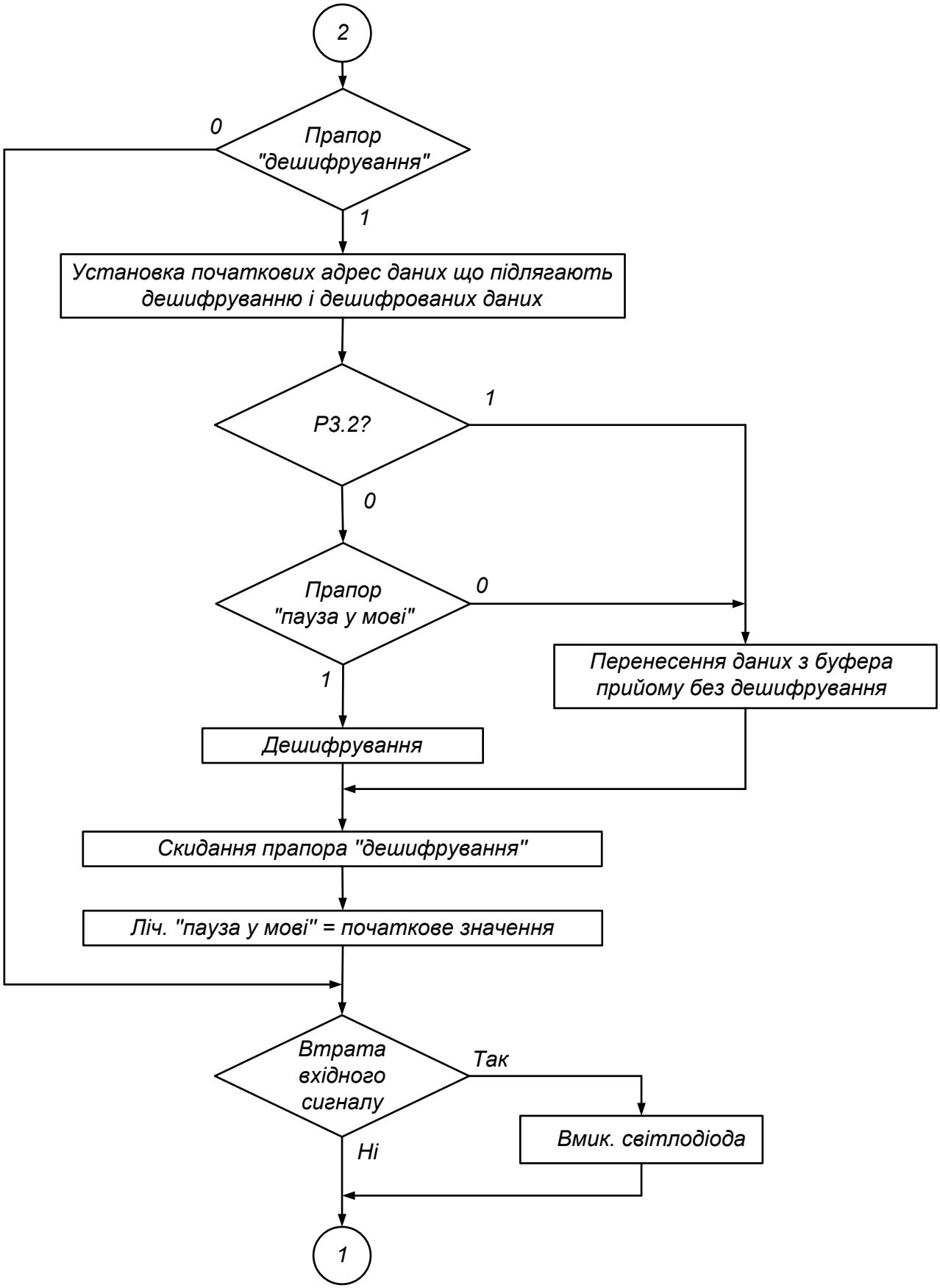


Рисунок 1.15. Алгоритм роботи пристрою криптозахисту каналу передачі конфіденційної інформації (закінчення)

S (високий пріоритет) – використовуваний для зчитування звіту, що поступив в послідовний порт.

Швидкість передачі визначається частотою переповнювання Т/С1, який працює в режимі 2. Швидкість передачі описана виразом:

$$f = (\frac{2^{SMOD}}{32})(\frac{f_{PE3}}{4})(256-(TH1)) \qquad (1.16)$$

При швидкості передачі 115200 біт/с знайдемо TH1: TH1=255.

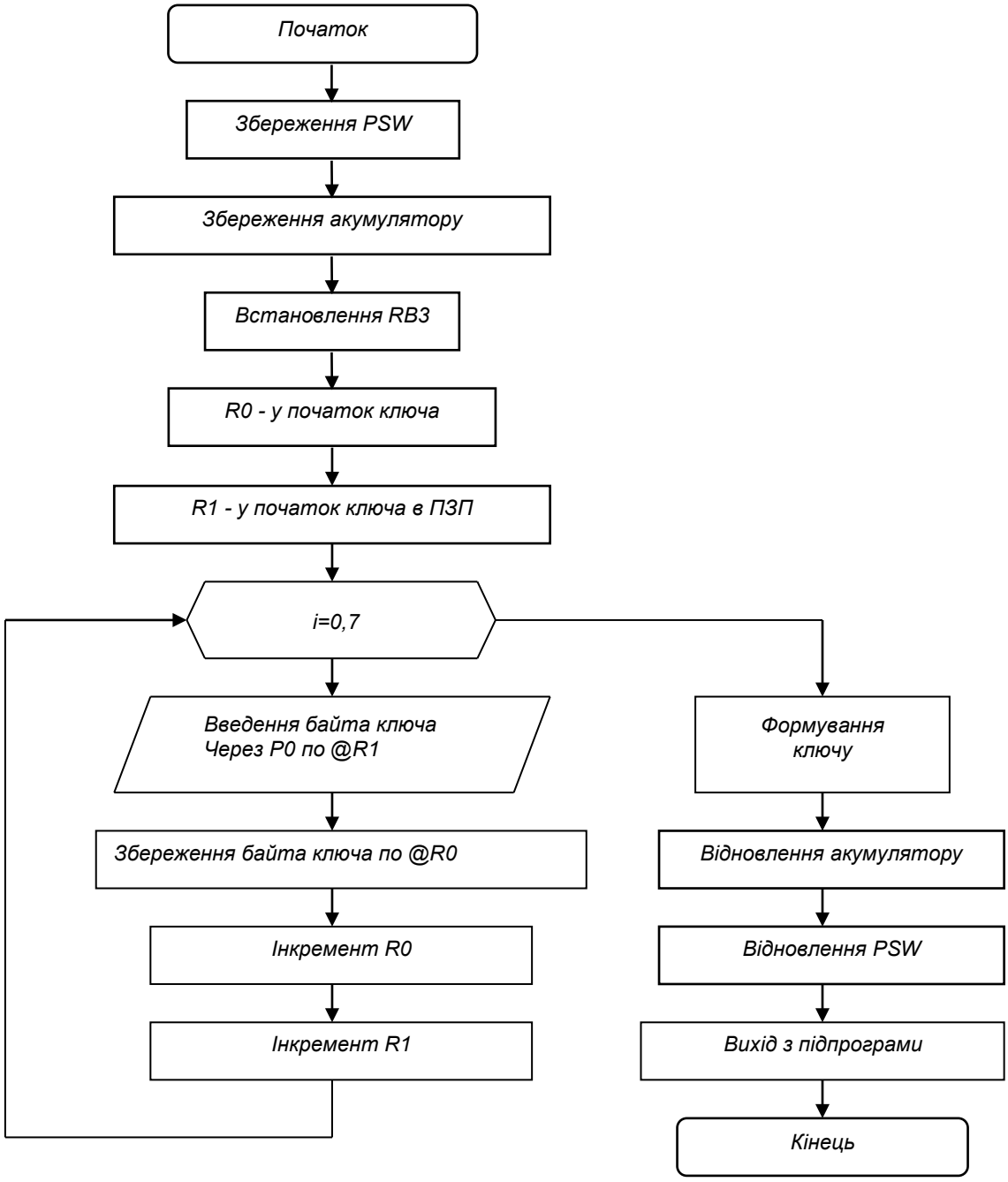


Рисунок 1.16. Підпрограма обробки переривань від INT1(низький пріоритет)

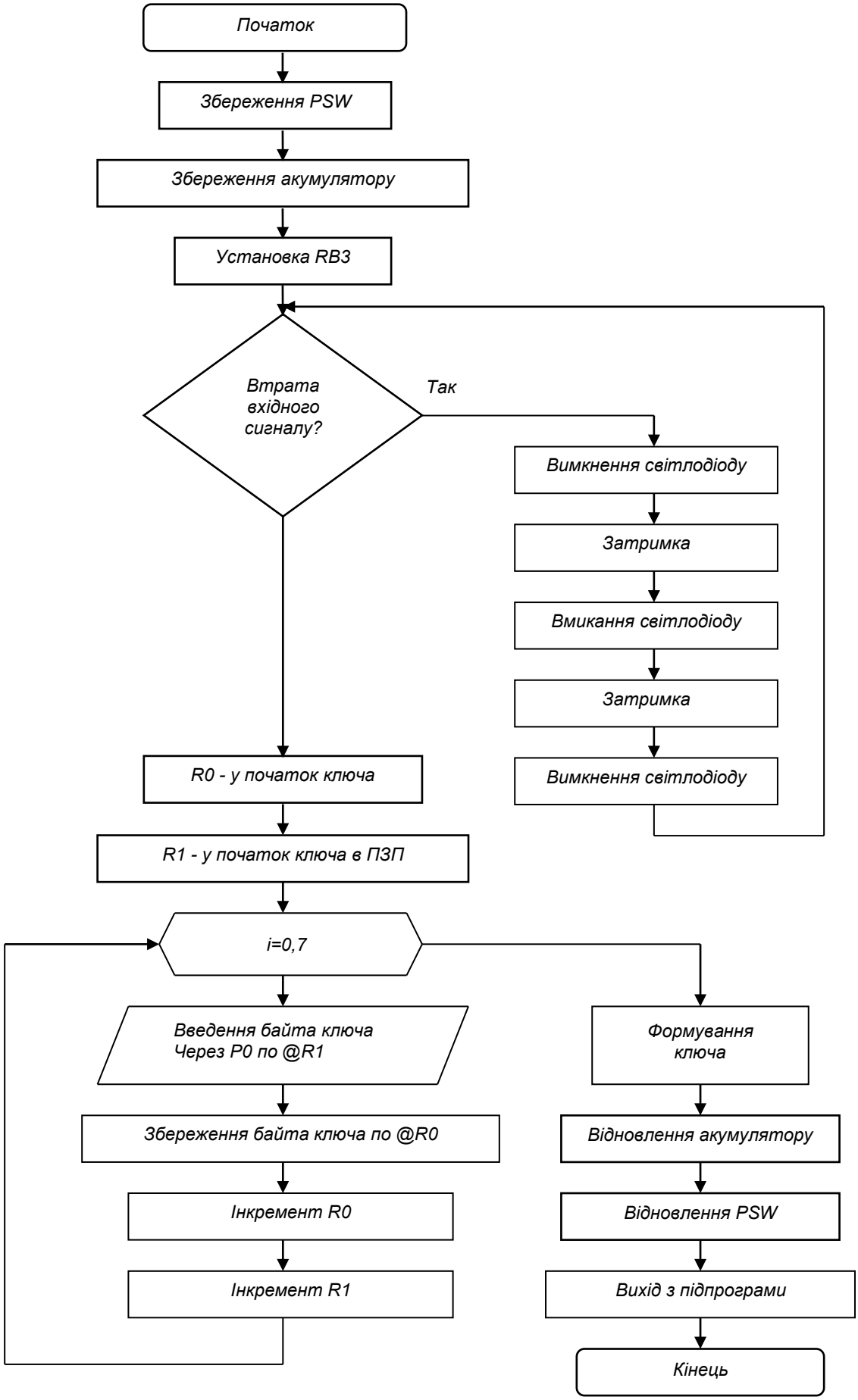


Рисунок 1.17. Підпрограма обробки переривань від INT0 (низький пріоритет)

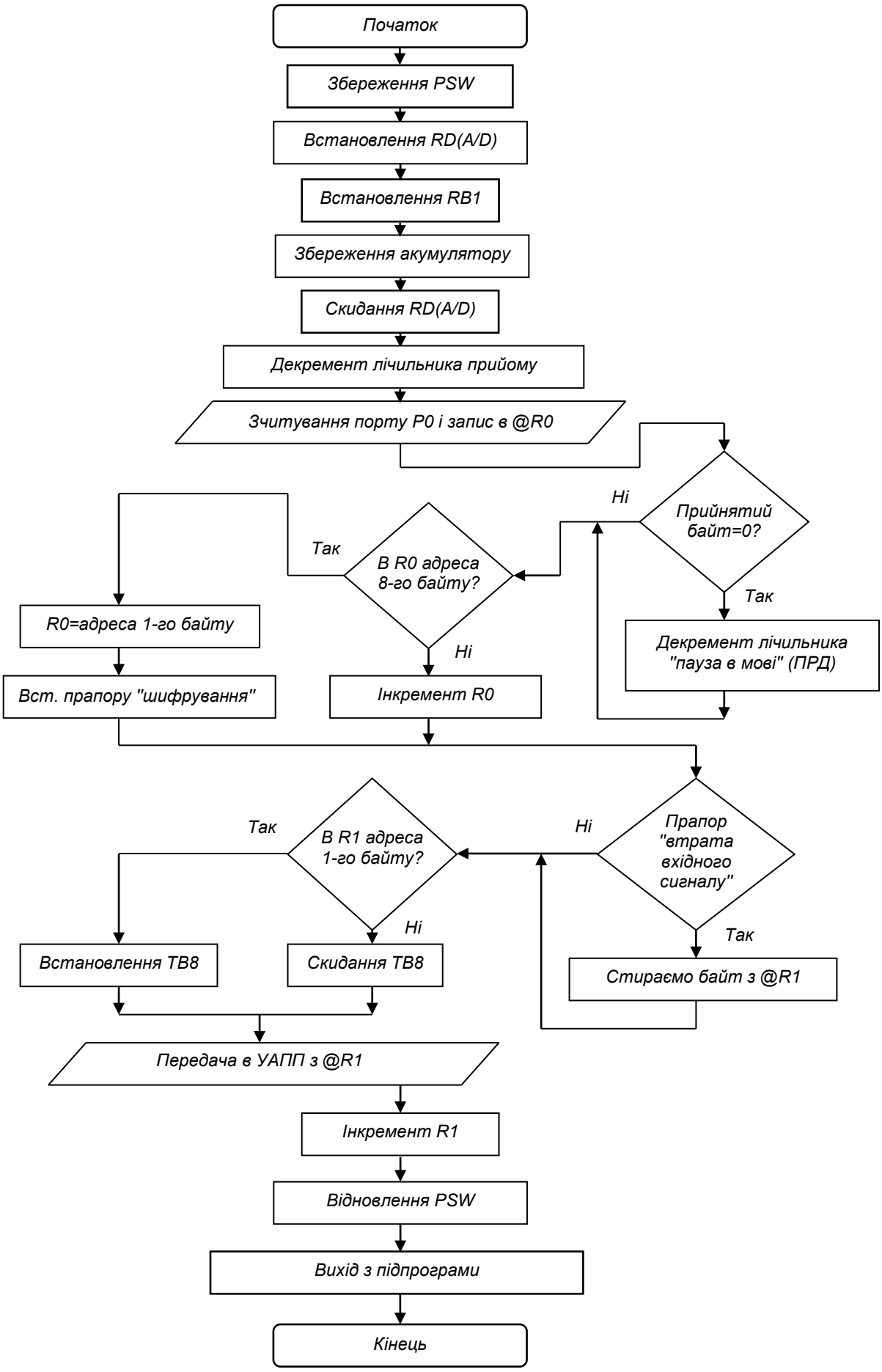


Рисунок 1.18. Підпрограма обробки переривань від T/C0 (високий пріоритет)

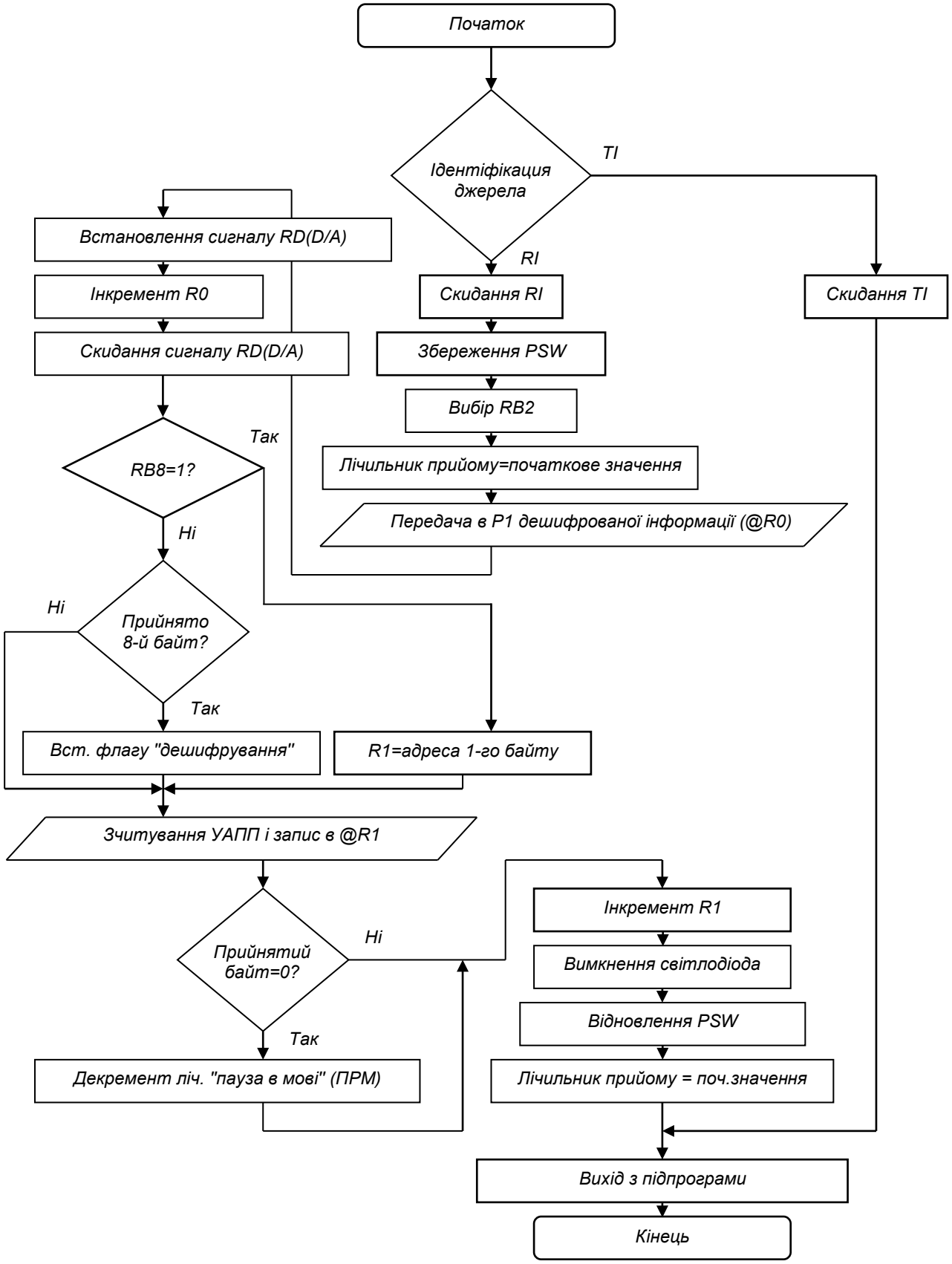


Рисунок 1.19. Підпрограма обробки переривань від УАПП (високий пріоритет)

1.9 Розробка програмного забезпечення для мікроконтролера пристрою крипто-захисту

Відлагодження програмного забезпечення зручно вести по окремих частинах, що виконують конкретні закінчені функції. В результаті реалізації наведених вище блок-схем алгоритмів отримано 5 закінчених функцій (сегментів) мовою Асемблера. Їх відлагодження проводитиметься в наступному порядку:

1. Основна програма;
2. Підпрограма обробки переривань від INT0;
3. Підпрограма обробки переривань від INT1;
4. Підпрограма обробки переривань від УАПП (універсального асинхронного прийомо-передавача);
5. Підпрограма обробки переривань від T/C0.

Процес компоновки здійснений на комп'ютері за допомогою програми лінкування. Програму, складену мовою Асемблера, було відлагоджено і перевірено на працездатність за допомогою пакету симуляції AVSIM51 (рис.1.20). Лістинг трансляції наведено у Додатку А.

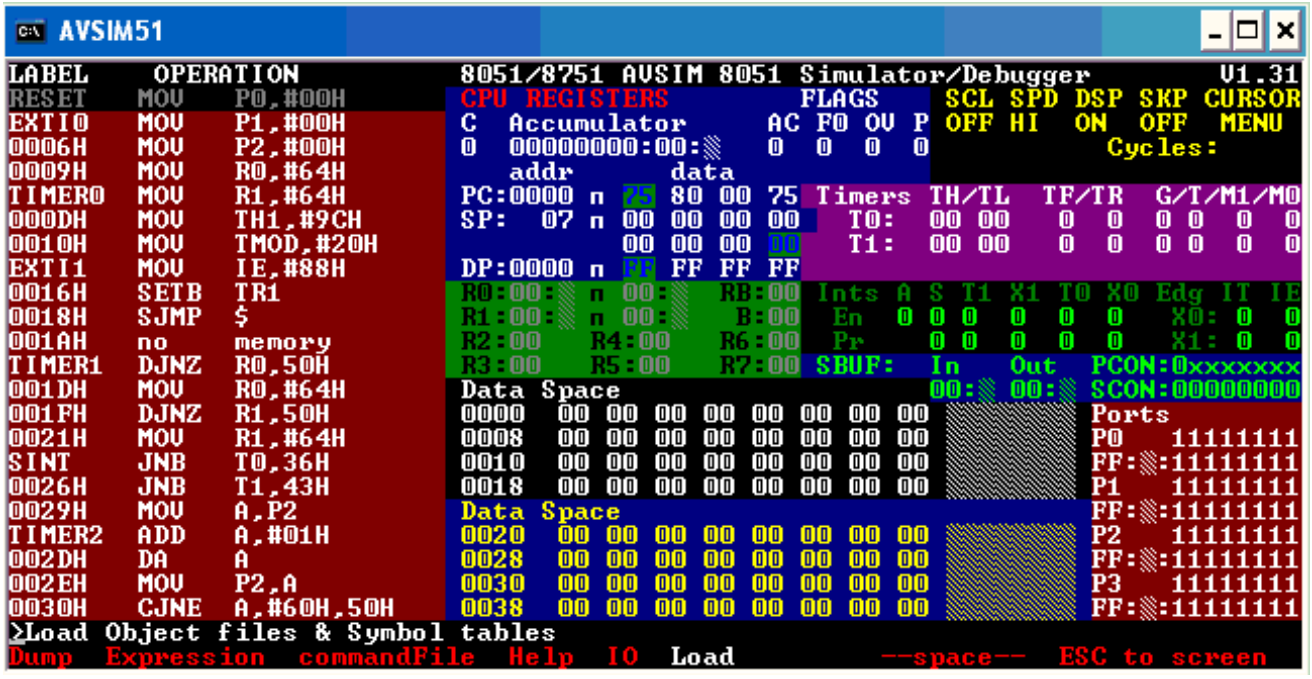


Рисунок 1.20. Емуляція роботи програми для мікроконтролера пристрою крипто-захисту засобами симулятору AVSIM51

2 ЕКОНОМІЧНА ЧАСТИНА

Розроблений у рамках дипломного проектування пристрій крипто-захисту каналу конфіденційного електрозв'язку дозволяє отримати високий рівень секретності, забезпечує для алгоритму шифрування можливість публічного використання і відкритого існування. Використаний у розробленому пристрої крипто-захисту мікроконтролер реалізує повноцінний алгоритм шифрування-дешифрування за стандартом DES, який вимагав би для реалізації засобами жорсткої логіки велику кількість електронних елементів, об'єднаних у сотні регістрів і схем. При використанні розробленого пристрою крипто-захисту оператор повинен знати, що, теоретично, при підборі ключу супротивник може його знайти, не використавши всіх комбінацій. Тому потрібно приймати заходи для захисту ключів. Застосування малогабаритної цифрової пам'яті з великими об'ємами і термінами зберігання інформації дозволяє забезпечувати пристрій крипто-захисту великою кількістю ключів, що позитивно вплине на крипостійкість системи в цілому.

У даному розділі визначається вартісна оцінка розробленого пристрою. Спочатку визначається калькуляція розробленого виробу укрупненим методом через вартість покупних комплектуючих елементів і виробів, для визначення якої складаємо перерахування елементів і виробів на основі відомості специфікацій (принципової схеми) по формі, приведених в таблиці 2.1

Таблиця 2.1 Розрахунок відомості покупних комплектуючих елементів

Найменування, тип, модель	**Од. вим**	**Норма витрат на виріб**	**Ціна, грн.**	**Вартість комплектуючих**
Мікросхема DS87C520	шт.	1	15.00	15.00
Мікросхема AD557	шт.	1	20.00	20.00
Мікросхема AD7574	шт.	1	25.00	25.00
Мікросхема NM256Q	шт.	1	14.00	14.00
Мікросхема К140УД20А	шт.	2	10.00	20.00
Мікросхема К555ЛН2	шт.	1	10.00	10.00
Мікросхема КР1533ИР33	шт.	1	20.00	20.00
Резистори МЛТ-0.125-301Ом	шт.	2	1.00	2.00
Резистори МЛТ-0.125-301Ом	шт.	2	1.00	2.00
Резистори МЛТ-0.125-10 кОм	шт.	1	1.00	1.00
Резистори МЛТ-0.125-10 кОм	шт.	9	1.00	9.00

Резистори МЛТ-0.125-100 кОм	шт.	1	1.00	1.00
Резистори МЛТ-0.125-3 кОм	шт.	10	1.00	10.00
Резистори МЛТ-0.125-8.2кОм	шт.	1	1.00	1.00
Конденсатори К50-12-10мкФ	шт.	1	3.00	3.00
Конденсатори КМК-2А-100пФ	шт.	1	3.00	3.00
Конденсатори КМК-2А-30пФ	шт.	2	3.00	6.00
Кварцовий резонатор 55МГц	шт.	1	20.00	20.00
Світлодіод АЛ307А	шт.	1	4.00	4.00
Кнопка П-2К	шт.	1	10.00	10.00
Перемикач DIP-7	шт.	1	10.00	10.00
Перемикач П-2К-1	шт.	1	10.00	10.00
Загальна вартість покупних комплектуючих елементів				216
Транспортні витрати (10%)				21,6
Всього (Впк)				237,6

Калькуляцію планової собівартості розробленого виробу розраховуємо з використанням методу питомих ваг і структури собівартості аналогічної продукції: питома вага матеріалу → αм = 20%; питома вага покупних виробів →αпк =62%; питома вага основної заробітної плати → αозп =18%

Таблиця 2.2 Калькуляція планової собівартості

Найменування статті витрат	**Значення статті, грн.**	**Розрахунок**
1. Сировина і матеріал	76,6	Вм = $\alpha_м$ * Впк/αпи = 20 * 237,6 / 62
2. Комплектуючі вироби і покупні напівфабрикати	237,6	Впк =см.табл.4.1
3. Основна заробітна плата	68,9	Воз= αозп * Впк/αпи = 18 * 237,6 /62
4. Додаткова заробітна плата	27,56	Вдз = 0,4 * Воз = 0,4 * 68,9
5. Відрахування о єдиного соцфонду	21,22	Вєс = (Воз + Вдз) * 0.22 Вєс= (68,9 + 27,56) * 0.22
6.Загально-виробничі витрати	96,46	Взаг.вир= (1,2…1,5)* Воз Взаг.вир =1.4 * 68,9
7. Виробнича собівартість	528,34	Свир = Вм+ Впк+ Воз+ Вдз+ Вєс +Взаг.вир
8.Адміністративні витрати	20,67	Ва = Воз * 0,3 = 68,9 * 0.3
9. Витрати на збут	10,56	Взб = Свир * 0,02 = 528,34* 0,02
10.Інші операційні витрати	5,28	Воп = Свир *0,01 = 528,34 * 0,01
Повна собівартість	564,85	Спов.= Свир+ Ва+ Взб+ Воп Спов=528,34+20,67+10,56+5,28

Розмір планового прибутку, що включається в ціну, визначаємо по формулі:

П= (Спов* ρ)/100% = (564,85 * 10%) / 100% = 56,48 грн.

де ρ-планова рентабельність продукції (10%...30%)

Оптову ціну виробу визначаємо по формулі:

$Ц_о$ = Спов + П = 564,85 + 56,48 грн = 621,33 грн.

Ціну реалізації виробу встановлюємо з урахуванням ПДВ:

Цр = Цо + Пз = 621,33 + 124,26 = 745,59 грн.

де Пз - податкове зобов'язання з ПДВ:

Пз = Цо * 0,2 = 621,33 * 0.2 = 124,26 грн.

Отримана в таблиці 2.2 повна собівартість являє собою витрати виготовлення одиниці виробу для даного року виробництва. Запропонуємо прогноз обсягів продажів даного виробу на другій стадії життєвого циклу виробу «Виробництво» з розподілом по роках (прогноз продажів передбачаємо на 4 роки). Характерні зони промислового випуску виробу представлені на малюнку:

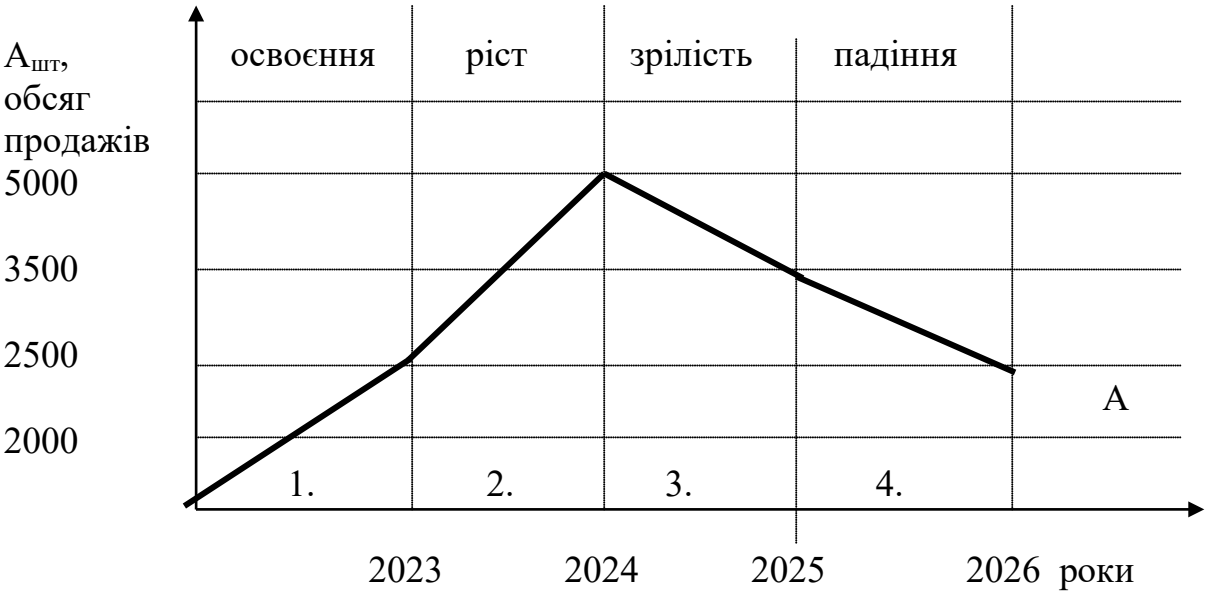


Рисунок 2.1 Прогноз обсягів продажу

В 2023 році обсяг продажів передбачається в розмірі 2500 шт під замовлення.

В 2024 році прогнозується збільшення обсягу продажів,тому витрати виробництва визначаємо по формулі:

$$C_{пов\ i+1} = C_{пові} \left(\frac{A_i}{A_{i=1}}\right)^{0.23}, \qquad (2.1)$$

де A_i – обсяг продажів (виробництва) у 1 рік розрахункового періоду, шт.;

$_i$– обсяг продажів (I+1)-ом року, шт.;

0,23 – показник ступеня, що характеризує вплив росту обсягів виробництва на собівартість продукції.

Звідси випливає, що

Спов$_{2024}$ = *564,85 *(2500/5000)$^{0.23}$ = 480,12 грн.*

В 2025 – 2026 роках обсяг продажів зменшується, витрати виробництва приймаються на рівні попереднього року.

Спов$_{2025,2026}$=480,12 грн.

Плановий прибуток, що включається в оптову ціну підприємства, для наступного року при збільшенні обсягу продажів, визначаємо по формулі:

$$П_{i+1} = C_{пi+1} * \frac{\rho}{100}$$ Звідси: *П$_{2024,2025,2026}$ = 480,12 * 20/100 = 96.02 грн.*

Оптову ціну підприємства в наступні роки розрахункового періоду визначаємо по формулі:

$$Ц_{O_{i+1}} = C_{n_{i+1}} + П_{i+1}$$ Звідси: *Ц$_{2024,2025,2026}$ = 480,12 + 96.02 = 576,14 грн.*

Податкове зобов'язання визначається по формулі:

$$Пз_{i+1} = Ц_{O_{i+1}} * 0.2$$ Звідси: *ПЗ$_{2024,2025,2026}$ = 576,14 * 0.2 = 115,22 грн.*

Ціну реалізації одиниці продукції в наступні роки визначаємо по формулі:

$$Ц_{P_{i+1}} = Ц_{O_{i+1}} + Пз_{i+1}$$ Звідси: *Ц$_{р\ 2024,2025,2026}$ = 576,14 + 115,22 = 691,36 грн.*

Вартісну оцінку результатів за розрахунковий період ($Р_т$) визначаємо по формулі:

$$P_T = \sum_{i=t_p}^{t_k} A_i * Ц_{P_i} * \alpha_i \qquad (2.2)$$

де t_p, t_k – відповідно розрахунковий і кінцевий рік розрахункового періоду;

$Ц_{pi}$ – ціна реалізації в і-тім році, грн.;

$А_i$ – обсяг продажів у і-тім році, грн.;

α_i – коефіцієнт, що включає фактор часу, тобто коефіцієнт приведення різночасних витрат і результатів до розрахункового року.

Вартісну оцінку за розрахунковий період визначаємо по формі, приведеної в таблиці 2.3.

Виробництво дає змогу одержати дохід за 4 роки 1175312 грн.

Таблиця 2.3 Розрахунок вартісної оцінки результатів

Найменування показника	**Позначення**	**Розрахунок виробничого періоду**			
		1-й	**2-й**	**3-й**	**4-й**
Обсяг продажів, шт	A_i	2500	5000	3500	2500
Ціна реалізації, грн.	$Ц_{pi}$	576,14	691,36	691,36	691,36
Вартісна оцінка результатів, млн грн.	$A_i * Ц_{pi}$	1440350	3456800	2419760	1728400
Коефіцієнт, що враховує фактор часу	α_i	0.91	0.83	0.75	0.68
Вартісна оцінка результатів з урахуванням фактора часу, млн грн.	$A_i * Ц_{pi} * \alpha_i$	1310718,5	2869144	1814820	1175312

3 ОХОРОНА ПРАЦІ

3.1 Охорона праці в Україні

В політики значну роль має відігравати постійне поліпшення умов і безпеки праці, зменшення рівнів травматизму та професійної захворюваності.

Ймовірність загинути, отримати травму чи набути професійне захворювання існує на тих підприємствах, установах та організаціях, де нехтуються правила безпеки і не виконуються вимоги охорони праці. Людина, яка володіє професійними навичками та знаннями правил безпеки, передбачає цей ризик і застосовує заходи, які його зменшують або зовсім виключають.

Широке впровадження комп'ютерної техніки, що дає змогу автоматизувати багато рутинних операцій, одержати доступ до численних джерел інформації, швидко проводити потрібні розрахунки і т.п. підвищує продуктивність праці. Проте активне впровадження у практику персональних комп'ютерів має і негативну сторону – з'являються фактори, які несприятливо впливають на здоров'я працюючої людини.

Тому безпечні умови праці по підприємствах, виробництвах можуть бути забезпечені тільки при суворому дотримані норм безпеки, виробничої санітарії і пожежної безпеки.

Законодавча база охорони праці України налічує ряд законів, основними з яких є Закон України «Про охорону праці» та Кодекс законів про працю. До законодавчої бази також належать Закони України: «Про загальнообов'язкове державне соціальне страхування від нещасних випадків на виробництві та професійних захворювань, які спричинили втрату працездатності», «Про охорону здоров'я», «Про пожежну безпеку», «Про забезпечення санітарного та епідеміологічного благополуччя населення», та інші. Їх доповнюють державні міжгалузеві й галузеві нормативні акти – це стандарти, інструкції, правила, норми, положення, статути та інші документи, яким надано чинність правових норм, обов'язкових для виконання усіма установами і працівниками.

На робочому місці оператора ЕОМ присутні шкідливі виробничі фактори, що притаманні використанню обчислювальної техніки та лазерного випромінювання.

3.2 Охорона праці при роботі оператора ПК

Оператори ПК і програмісти зіштовхуються із впливом таких фізично небезпечних і шкідливих виробничих факторів, як підвищений рівень шуму, підвищена температура зовнішнього середовища, відсутність або недостатня освітленість робочої зони, електричний струм, статична електрика й інші.

На робочому місці програміста повинні бути створені умови для високопродуктивної праці.

Оператор як і користувач персонального комп'ютера випробовує значне навантаження, як фізичне (сидяче положення, навантаження на очі), так і розумове, що приводить до зниження його працездатності до кінця робочого дня.

На робочому місці оператор ПК піддається впливу наступних несприятливих факторів:

- недостатнє освітлення;
- шум від працюючих машин;
- електромагнітне випромінювання;
- виділення надлишків теплоти.

Тому необхідно розробити засоби захисту від цих шкідливих факторів.

До даних засобів захисту відносять: вентиляція, штучне освітлення, звукоізоляція. Існують нормативи, що визначають комфортні умови й гранично припустимі норми запиленості, температури повітря, шуму, освітленості. У системі мір, що забезпечують сприятливі умови праці, велике місце приділяється естетичним факторам: оформлення виробничого інтер'єра, устаткування, застосування функціональної музики та ін., які впливають на організм людини. Важливу роль грає фарбування приміщень, що повинна бути світлої.

Розвитку стомлюваності сприяють наступні фактори:

- неправильна ергономічна організація робочого місця, нераціональні зони розміщення устаткування по висоті від підлоги, по фронту від осі симетрії і т.д.;
- характер протікання праці - важливе значення має чергування праці й відпочинку, зміна одних форм роботи іншими.

3.3 Санітарія і гігієна праці

Для нормальної життєдіяльності в умовах виробництва треба створити санітарні умови, які б дали змогу їй плідно працювати не перевтомлюючись та зберігати своє здоров'я.

Для цього треба, щоб енергетичні витрати при праці компенсувалися відпочинком та умовами оточуючого середовища. Ці умови створюються забезпеченням для працюючого:

- зручного робочого місця;
- чистого повітря;
- нормованої освітленості;
- захисту від шуму та вібрації;
- захисту від дії шкідливих речовин та випромінювань;
- робочим одягом та різними засобами індивідуального захисту;
- побутовими приміщеннями та спеціальними службами, що призначені створювати безпечні та нормальні санітарні умови праці

3.3.1 Виробничі будівлі та приміщення

Основні вимоги до будівель виробничого призначення викладені в СниП 2.09.02.-85.

Об'ємно-планувальні рішення будівель та приміщень, де експлуатуються відеодисплейні термінали мають відповідати вимогам ДСанПІН 3.3.2.007-98.

Розміщення робочих місць з ЕОМ і ПЕОМ у підвальних приміщеннях, на цокольних поверхах заборонено.

Для приміщень, які призначені для роботи доцільно обрати орієнтацію вікон на північ або північний схід. На вікнах повинні бути жалюзі, що регулюються, або штори, що дають можливість їх повністю закривати. Приміщення відповідно до СниП 11-4-79 повинні мати природнє та штучне освітлення.

При приміщеннях з ВДТ мають бути обладнані побутові приміщення для відпочинку, психологічного розвантаження тощо.

3.3.2 Гігієнічне нормування параметрів повітря робочої зони

Мікроклімат виробничих приміщень нормується в залежності від теплових характеристик виробничих приміщення, категорії робіт по важкості і періоду року. Основні нормативні документи, де наводяться норми мікроклімату – це санітарні норми та стандарти безпеки праці.

Оптимальні мікрокліматичні умови – це такі параметри температури, вологості і швидкості руху повітря, які при тривалому і систематичному впливі на людину забезпечують нормальний тепловий стан організму без напруги і порушення механізмів терморегуляції.

При нормуванні мікроклімату календарний рік поділяється на два періоди:

- холодний період (середньодобова температура нижча +10 С;

- теплий період (середньодобова температура становить+10 С

Визначити параметри метеорологічних умов, які необхідно забезпечити у виробничих приміщеннях, джерела виділення шкідливих газів, парів, пилу, їх концентрації у повітрі робочих зон, можливий вплив на працівників.

Висвітлити питання щодо вибору системи опалення та обладнання припливно-витяжної загально обмінної вентиляції, різних типів місцевої припливної (повітряні душі, теплові завіси) та місцевої витяжної вентиляції (відсмоктувачі, витяжні шафи, зонти, всмоктувальні панелі тощо). Аргументувати необхідність застосування кондиціювання повітря.

3.3.3 Освітлення виробничих приміщень

Стан виробничого освітлення повинен відповідати СніП 11-4-79 «Природне та штучне освітлення. Норми проектування».

Стан освітлення виробничих приміщень відіграє важливу роль для попередження виробничого травматизму.

Раціональне освітлення повинно відповідати таким умовам:

- бути достатнім, відповідним нормі;

- рівномірним, не утворювати тіней на робочій поверхні;

- не засліплювати працюючого;

- напрямок світлового потоку повинен відповідати зручному виконанню роботи;

Головними джерелами світла для промислового освітлення є лампи розжарювання та газорозрядні лампи різноманітних типів.

3.3.4 Заходи щодо захисту від дії шуму та вібрації

При проектуванні та модернізації діючого обладнання повинні передбачатися заходи, знижуючі шум та вібрацію під час їх роботи.

Шум характеризується частотою коливань звуку, звуковим тиском, інтенсивністю(силою) звуку і рівнем гучності.

Припустимий рівень шуму на робочих місцях в виробничих приміщеннях не повинен перевищувати вимог Державних стандартів Україні 12.1.003 – ССБТ.

Вібрація (струс) – сукупність механічних рухів пружистих тіл, машин, верстатів, механізмів та пристроїв, які повторюються через окремі проміжки часу та розповсюджуються на будівельні конструкції через опори, перекриття, а також на корпус машин та інструментів.

ВИСНОВКИ

Розроблений у рамках дипломного проектування пристрій крипто-захисту каналу конфіденційного електрозв’язку дозволяє отримати високий рівень секретності, забезпечує для алгоритму шифрування можливість публічного використання і відкритого існування.

Використаний у розробленому пристрої крипто-захисту мікроконтролер реалізує повноцінний алгоритм шифрування-дешифрування за стандартом DES, який вимагав би для реалізації засобами жорсткої логіки велику кількість електронних елементів, об'єднаних у сотні регістрів і схем. При використанні розробленого пристрою крипто-захисту оператор повинен знати, що, теоретично, при підборі ключу супротивник може його знайти, не використавши всіх комбінацій. Тому потрібно приймати заходи для захисту ключів. Застосування малогабаритної цифрової пам'яті з великими об'ємами і термінами зберігання інформації дозволяє забезпечувати пристрій крипто-захисту великою кількістю ключів, що позитивно вплине на крипостійкість системи в цілому.

Розроблений пристрій крипто-захисту каналу конфіденційного електрозв’язку заснований на використанні алгоритму шифрування DES і дозволить проводити безпечний обмін інформації при використанні з пристроями різних фірм-виробників обладнання з аналогічним алгоритмом шифрування.

Стійкість алгоритму DES може бути підвищена за допомогою певних удосконалень і модифікацій, зокрема використання алгоритму 3DES, що буде потребувати модифікації лише мікропрограмної частини пристрою. Створювані на основі стандарту DES пристрої мають розроблятися так, щоб їх можна було використовувати у обчислювальних системах або мережах для забезпечення криптографічного захисту даних, представлених у вигляді двійкового коду. При цьому має бути забезпечена можливість їх випробувань і перевірки на точне виконання перетворень при шифруванні та дешифруванні.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бабаш А.В. Криптографические методы защиты информации / А.В. Бабаш, Е.К. Баранова. – Изд.-во: Кнорус, 2016. – с. 190.

2. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. – М.: Гелиос АРВ, 2015. – 376 с.

3. Бузов, Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. – М.: Горячая линия – Телеком, 2016. – 186 с.

4. Горев, А И; Симаков А А Обеспечение Информационной Безопасности / А Горев А И; Симаков А. – Москва: ИЛ, 2016. – 494 с.

5. Грибунин, Вадим Геннадьевич Цифровая стеганография / Грибунин Вадим Геннадьевич. – М.: Солон-Пресс, 2016. – 589 с.

6. Жданов, О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования / О.Н. Жданов. – М.: ИНФРА-М, 2015. – 869 с.

7. Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. – Москва: Огни, 2013. – 192 с.

8. Литвинская, О. С. Основы теории передачи информации. Учебное пособие / О.С. Литвинская, Н.И. Чернышев. – М.: КноРус, 2015. – 168 с.

9. Осмоловский, С. А. Стохастическая информатика. Инновации в информационных системах / С.А. Осмоловский. - М.: Горячая линия – Телеком, 2012. – 322 с.

10. Шаньгин, В. Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – Москва: Огни, 2016. – 551 с.

11. Аграновский А.В., Р.А. Хади Практическая криптография: алгоритмы и их программирование. – М.: СОЛОН-Пресс, 2009, 256 с.

12. Магда Ю. С. Микроконтроллеры серии 8051: практический подход. — М.: ДМК Пресс, 2008. – 228 с.

ДОДАТОК А

Перелік елементів до схеми принципової електричної пристрою крипто-захисту каналу конфіденційного електрозв'язку

Позначення на схемі	Найменування та номінал	Кількість
C4	Конденсатор К50-12-10 мкФ	1
C1	Конденсатор КМК-2А-100 пФ	1
C2,C3	Конденсатор КМК-2А-30 пФ	2
DD4	Мікросхема DS87C520	1
DD2	Мікросхема AD557	1
DD1	Мікросхема AD7574	1
DD6	Мікросхема NM256Q	1
DA1, DA2	Мікросхема А747	2
DD3	Мікросхема SN74LS05	1
DD5	Мікросхема SN74ALS573	1
R1,R2	Резистор МЛТ-0,125-301 Ом	2
R4,R5	Резистор МЛТ-0,125-301 Ом	2
R3	Резистор МЛТ-0,125-10 кОм	1
R6-R14	Резистор МЛТ-0,125-10 кОм	9
R15	Резистор МЛТ-0,125-100 кОм	1
R18-R27	Резистор МЛТ-0,125-3 кОм	10
R17	Резистор МЛТ-0,125-8,2 Ом	1
Q1	Кварцевий резонатор 55 МГц	1
VD1	Світлодіод АЛ307А	1
S2	Кнопка П-2К	1
S3	Перемикач DIP-7	1
S1	Перемикач П-2К-1	1

ДОДАТОК Б
Лістинг програми для мікроконтролера пристрою крипто-захисту (мовою Асемблера)

```
================================================================
 AVCASE 8051-Family Linker
================================================================
Date:         16/05/23 17:45:08
Image File:   DESSYS.hex
Symbol File:  DESSYS.sym
Options:      -SY
              -SM
              -SM
              -SP
Startup Addr: Unspecified
=================
 INPUT FILES
=================
          Input File Name             L    Date & Time         Version
DESSYS.obj                             16/05/23 17:45:08
================
 MEMORY MAP
================
 Space    Start     End    Length       Segment          Module
ROM      0000H    01B1H      1B2H    BEG              DESSYS
ROM      01B2H    FFFFH     FE4EH    -unallocated
RAM        00H      07H        8H    REG0             DESSYS
RAM        08H      FFH       F8H    -unallocated
XRAM     0000H    FFFFH     10000H    -unallocated
==================================
 ALPHABETICAL LIST OF SEGMENTS
==================================
   Segment      Class   Start  End   Length  Align  Other Attributes
BEG            CODE     0000  01b1   01b2   BYTE   ABSOLUTE
BIT            BIT      0000  0000   0000   BIT
CODE           CODE     0000  0000   0000   BYTE
DATA           DATA     0000  0000   0000   BYTE
IDATA          IDATA    0000  0000   0000   BYTE
REG0           DATA     0000  0007   0008   BYTE   ABSOLUTE,OVERLAID
XDATA          XDATA    0000  0000   0000   BYTE
==================================
 SYMBOLS BY CLASS AND ADDRESS
==================================
 Class           Symbol Name           Value      Module       Segment
=====================================
 MODULES, ALPHABETICALLY BY NAME
=====================================
Module DESSYS:
         File:    DESSYS.obj
         Date:    16/05/23 17:44:03
            Segment      Space   Start   End   Length
         BEG             ROM     0000H  01B1H  01B2H
         REG0            RAM     0000H  0007H  0008H
============================
 UNALLOCATED SEGMENTS
```

```
==========================
   Segment      Class     Space     Reason Not Allocated
CODE           CODE      ROM       Zero Length
DATA           DATA      RAM       Zero Length
BIT            BIT       BIT       Zero Length
IDATA          IDATA     RAM       Zero Length
XDATA          XDATA     XRAM      Zero Length
                                    1                DEFSEG  BEG,ABSOLUTE
                                    2                SEG     BEG
        =0000                       3                ORG     0H
0000 0125                           4                AJMP    MET2
        =0003                       5                ORG     03H
0003 01D7                           6                AJMP    INTER0
        =000B                       7                ORG     0BH
000B 215A                           8                AJMP    TIMER
        =0013                       9                ORG     13H
0013 210B                          10                AJMP    INTER1
        =0023                      11                ORG     023H
0023 2122                          12                AJMP    SER_P
0025 D2 88                         13   MET2:        SETB    IT0                ;
0027 D2 8A                         14                SETB    IT1                ;
0029 C2 B8                         15                CLR     PX0                ;
002B C2 BA                         16                CLR     PX1                ;
002D D2 A8                         17                SETB    EX0                ;
002F D2 AA                         18                SETB    EX1                ;
0031 75 89" 22                         19                MOV   TMOD,#00100010B ;
0034 75 8D" 36                     20                MOV     TH1,#54 ;
0037 75 8C" 32                     21                MOV     TH0,#50 ;
003A C2 AB                         22                CLR     ET1                ;
003C D2 A9                         23                SETB    ET0                ;
003E D2 B9                         24                SETB    PT0                ;
0040 75 98" D0                     25                MOV     SCON,#11010000B ;
0043 D2 AC                         26                SETB    ES                 ;
0045 D2 BC                         27                SETB    PS                 ;
0047 75 00 38                      28                MOV     00H,#38H           ;
004A 75 01 30                      29                MOV     01H,#30H           ;
004D 75 10 28                      30                MOV     10H,#28H           ;
0050 75 11 20                      31                MOV     11H,#20H           ;
0053 75 18 40                      32                MOV     18H,#40H           ;
0056 75 19 00                      33                MOV     19H,#0H            ;
0059 75 12 00                      34                MOV     12H,#0             ;
005C 75 13 00                      35                MOV     13H,#0             ;
005F 75 14 00                      36                MOV     14H,#0             ;
0062 75 15 08                      37                MOV     15H,#8             ;
0065 75 16 08                      38                MOV     16H,#8             ;
0068 75 81" 72                     39                MOV     SP,#72H            ;
006B C2 B4                         40                CLR     P3.4               ;
006D C2 B5                         41                CLR     P3.5               ;
006F D2 8E                         42                SETB    TR1                ;
0071 D2 8C                         43                SETB    TR0                ;
0073 D2 AF                         44                SETB    EA                 ;
0075 E5 14                         45   SH:          MOV     A,14H              ;
0077 60 25'                        46                JZ      DE                 ;
0079 75 00 38                      47                MOV     00H,#38H           ;
007C 75 01 30                      48                MOV     01H,#30H           ;
007F 20 B2# 04'                    49                JB      P3.2,SS            ;
```

```
0082 E5 15          50              MOV     A,15H           ;
0084 70 4D'         51              JNZ     SHIFR           ;
                    52
;ПЕРЕНЕСЕННЯ 8-МИ БАЙТІВ В БУФЕР ПЕРЕДАЧІ БЕЗ ШИФРУВАННЯ
0086 C2 D4          53  SS:         CLR     RS1             ;
0088 C2 D3          54              CLR     RS0             ;
008A 7F 08          55              MOV     R7,#8           ;
008C E6             56  P_S:        MOV     A,@R0           ;
008D F7             57              MOV     @R1,A           ;
008E 08             58              INC     R0              ;
008F 09             59              INC     R1              ;
0090 DF FA'         60              DJNZ    R7,P_S          ;
0092 75 00 38       61  RE_SH:  MOV         00H,#38H        ;
0095 75 01 30       62              MOV     01H,#30H        ;
0098 75 14 00       63              MOV     14H,#0          ;
009B 75 15 08       64              MOV     15H,#8          ;
009E E5 13          65  DE:         MOV     A,13H           ;
00A0 60 25'         66              JZ      KON             ;
00A2 75 11 20       67              MOV     11H,#20H        ;
00A5 75 10 28       68              MOV     10H,#28H        ;
00A8 20 B2# 04'     69              JB      P3.2,DD         ;
00AB E5 16          70              MOV     A,16H           ;
00AD 70 26'         71              JNZ     DESHIFR         ;
                    72
;ПЕРЕНЕСЕННЯ 8-МИ БАЙТІВ З БУФЕРУ ПРИЙОМУ В P1
00AF D2 D4          73      DD:     SETB    RS1             ;
00B1 C2 D3          74              CLR     RS0             ;
00B3 7F 08          75              MOV     R7,#8           ;
00B5 E7             76      P_S1:   MOV     A,@R1           ;
00B6 F6             77              MOV     @R0,A           ;
00B7 08             78              INC     R0              ;
00B8 09             79              INC     R1              ;
00B9 DF FA'         80              DJNZ    R7,P_S1         ;
00BB 75 11 20       81      RE_DE:  MOV     11H,#20H        ;
00BE 75 10 28       82              MOV     10H,#28H        ;
00C1 75 16 08       83              MOV     16H,#8          ;
00C4 75 13 00       84              MOV     13H,#0          ;
00C7 E5 12          85      KON:    MOV     A,12H           ;
00C9 70 04'         86              JNZ     SH1             ;
00CB D2 B6          87              SETB    P3.6            ;
00CD 0175           88              AJMP    SH              ;
00CF C2 B6          89      SH1:    CLR     P3.6            ;
00D1 0175           90              AJMP    SH              ;
00D3 0192           91      SHIFR:  AJMP    RE_SH           ;
00D5 01BB           92      DESHIFR:AJMP    RE_DE
                    93
                    94
;ОБРОБКА ПЕРЕРИВАНЬ ВІД INT0 (НАТИСНУТА КНОПКА “ЗАКРИТА ПЕРЕДАЧА”)
00D7 C0 D0          95      INTER0: PUSH    PSW             ;
00D9 D2 D4          96              SETB    RS1             ;
00DB D2 D3          97              SETB    RS0             ;
00DD FB             98              MOV     R3,A            ;
00DE AA 12          99      POTER:  MOV     R2,12H          ;
00E0 BA 00 18'     100              CJNE    R2,#0,NO        ;
00E3 C2 B6         101              CLR     P3.6            ;
00E5 7D 0F         102              MOV     R5,#0FH         ;
```

```
00E7 7C 01          103   TIM2:   MOV   R4,#01H          ;
00E9 EC             104   TIM1:   MOV   A,R4             ;
00EA DC FD'         105           DJNZ  R4,TIM1          ;
00EC DD F9'         106           DJNZ  R5,TIM2          ;
00EE D2 B6          107           SETB  P3.6             ;
00F0 7D 0F          108           MOV   R5,#0FH          ;
00F2 7C 01          109   TIM4:   MOV   R4,#01H          ;
00F4 EC             110   TIM3:   MOV   A,R4             ;
00F5 DC FD'         111           DJNZ  R4,TIM3          ;
00F7 DD F9'         112           DJNZ  R5,TIM4          ;
00F9 01DE           113           AJMP  POTER            ;
00FB 78 40          114   NO:     MOV   R0,#40H          ;
00FD 79 00          115           MOV   R1,#0            ;
00FF 7C 08          116           MOV   R4,#8            ;
0101 E3             117   KEY:    MOVX  A,@R1            ;
0102 F6             118           MOV   @R0,A            ;
0103 09             119           INC   R1               ;
0104 08             120           INC   R0               ;
0105 DC FA'         121           DJNZ  R4,KEY           ;
0107 EB             122           MOV   A,R3             ;
0108 D0 D0          123           POP   PSW              ;
010A 32             124           RETI                   ;
                    125
                    126
;ПІДПРОГРАМА ОБРОБКИ ПЕРЕРИВАНЬ ВІД INT1
010B C0 D0          127   INTER1: PUSH  PSW    ;
010D D2 D4          128           SETB  RS1    ;
010F D2 D3          129           SETB  RS0    ;
0111 FB             130           MOV   R3,A   ;
0112 78 40          131           MOV   R0,#40H ;
0114 79 00          132           MOV   R1,#0  ;
0116 7C 08          133           MOV   R4,#8        ;
0118 E3             134   KEY2:   MOVX  A,@R1       ;
0119 F6             135           MOV   @R0,A        ;
011A 09             136           INC   R1           ;
011B 08             137           INC   R0           ;
011C DC FA'         138           DJNZ  R4,KEY2 ;
011E EB             139           MOV   A,R3         ;
011F D0 D0          140           POP   PSW          ;
0121 32             141           RETI               ;
                    142
;ПІДПРОГРАМА ОБРОБКИ ПЕРЕРИВАНЬ ВІД УАПП
0122 10 98# 05'     143   SER_P:  JBC   RI,PR        ;
0125 10 99# 31'     144           JBC   TI,ENDP ;
0128 2159           145           AJMP  ENDP         ;
012A C0 D0          146   PR:     PUSH  PSW          ;
012C D2 D4          147           SETB  RS1          ;
012E C2 D3          148           CLR   RS0          ;
0130 FF             149           MOV   R7,A         ;
0131 75 12 03       150           MOV   12H,#3  ;
0134 86 90          151           MOV   P1,@R0  ;
0136 D2 B5          152           SETB  P3.5         ;
0138 08             153           INC   R0           ;
0139 C2 B5          154           CLR   P3.5         ;
013B B8 30 01'      155           CJNE  R0,#30H,IN_1    ;
013E 18             156           DEC   R0
```

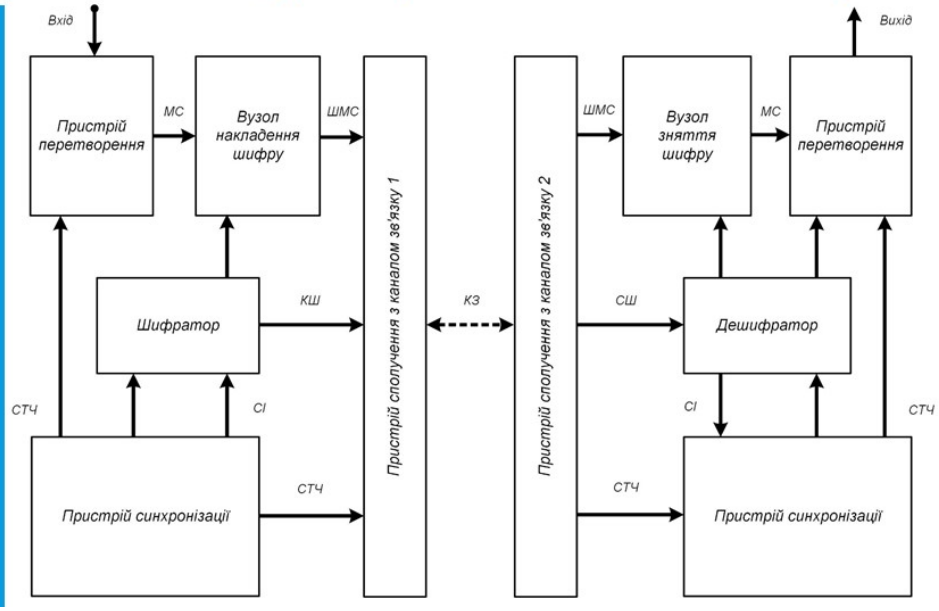
```
013F 30 9A# 04'          157     IN_1:   JNB     RB8,IN4 ;
0142 79 20               158             MOV     R1,#20H ;
0144 214C                159             AJMP    INF
0146 B9 27 03'           160     IN4:    CJNE    R1,#27H,INF
0149 75 13 01            161             MOV     13H,#1  ;
014C E5 99               162     INF:    MOV     A,SBUF  ;
014E F7                  163             MOV     @R1,A       ;
014F 70 02'              164             JNZ     IN2         ;
0151 15 16               165             DEC     16H         ;
0153 09                  166     IN2:    INC     R1          ;
0154 C2 B6               167     IN3:    CLR     P3.6        ;
0156 EF                  168             MOV     A,R7        ;
0157 D0 D0               169             POP     PSW         ;
0159 32                  170     ENDP:   RETI                ;
                          171
                         172
;ПІДПРОГРАММА ОБРОБКИ ПЕРЕРИВАНЬ ВІД T\C0
015A C0 D0               173     TIMER:  PUSH    PSW         ;
015C D2 B4               174             SETB    P3.4        ;
015E C2 D4               175             CLR     RS1         ;
0160 C2 D3               176             CLR     RS0         ;
0162 FB                  177             MOV     R3,A        ;
0163 C2 B4               178             CLR     P3.4        ;
0165 E5 12               179             MOV     A,12H       ;
0167 60 02'              180             JZ      TC          ;
0169 15 12               181             DEC     12H         ;
016B E5 A0               182     TC:     MOV     A,P2        ;
016D F6                  183             MOV     @R0,A       ;
016E 70 02'              184             JNZ     M           ;
0170 15 15               185             DEC     15H         ;
0172 B8 3F 07'           186     M:      CJNE    R0,#3FH,NET     ;
0175 78 38               187             MOV     R0,#38H ;
0177 75 14 01            188             MOV     14H,#1  ;
017A 217D                189             AJMP    NET0        ;
017C 08                  190     NET:    INC     R0          ;
017D E5 12               191     NET0:   MOV     A,12H       ;
017F 70 02'              192             JNZ     PER         ;
0181 77 00               193             MOV     @R1,#0  ;
0183 B9 30 04'           194     PER:    CJNE    R1,#30H,N       ;
0186 D2 9B               195             SETB    TB8         ;
0188 218C                196             AJMP    PE1         ;
018A C2 9B               197     N:      CLR     TB8         ;
018C 87 99               198     PE1:    MOV     SBUF,@R1        ;
018E 09                  199             INC     R1          ;
018F B9 38 02'           200             CJNE    R1,#38H,PE2             ;
0192 79 30               201             MOV     R1,#30H     ;
0194 EB                  202   PE2:      MOV     A,R3        ;
0195 D0 D0               203             POP     PSW         ;
0197 32                  204             RETI    ;
                         205             END
```

No lines contained errors.

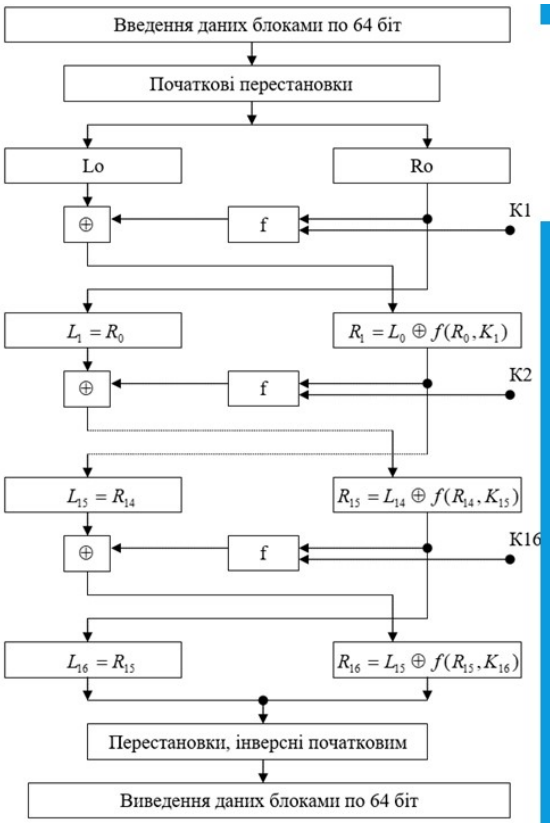
Кудрявцев Олександр, ВСП “ОТФК ОНТУ”

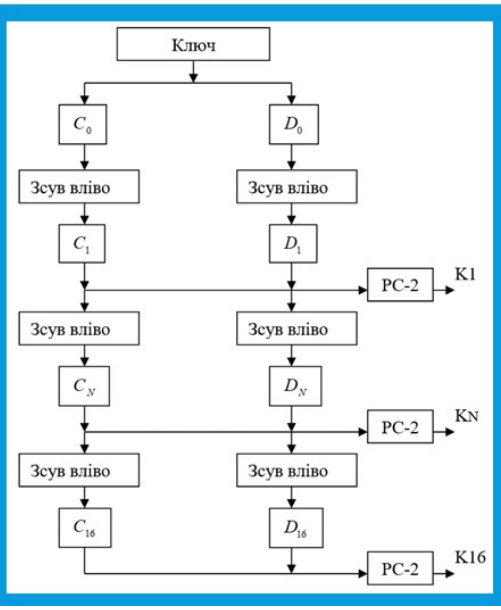
Розробка пристрою крипто-захисту каналу конфіденційного електрозв’язку

СТРУКТУРНА СХЕМА КРИПТО-ЗАХИСТУ КАНАЛУ ПЕРЕДАЧІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

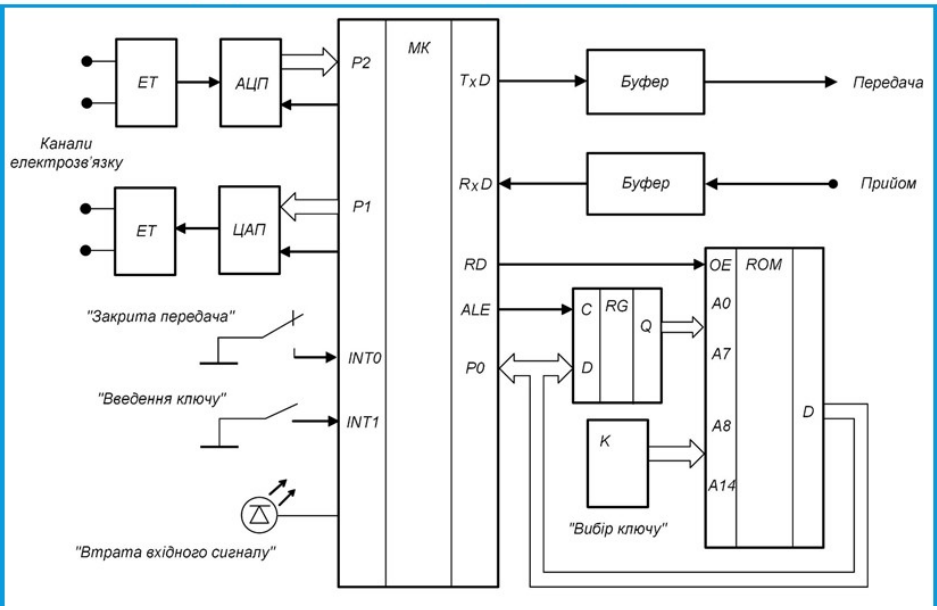


БЛОК-СХЕМА АЛГОРИТМУ ШИФРУВАННЯ DES ТА ОБЧИСЛЕННЯ КЛЮЧОВИХ БЛОКІВ





ФУНКЦІОНАЛЬНА СХЕМА ПРИСТРОЮ КРИПТО-ЗАХИСТУ КАНАЛУ ПЕРЕДАЧІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ



СТРУКТУРНА СХЕМА МІКРОКОНТРОЛЕРІВ DS87C520

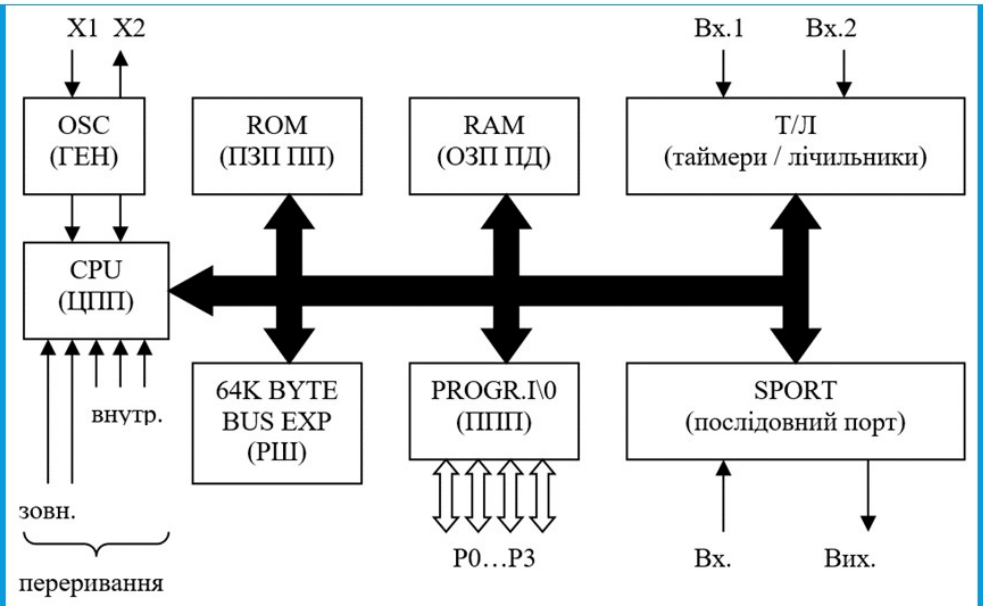
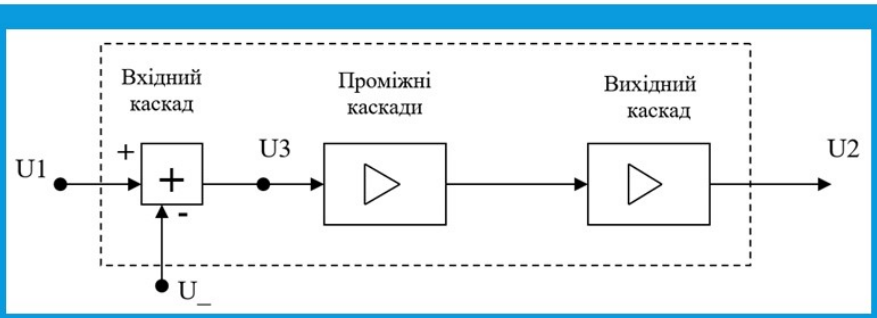
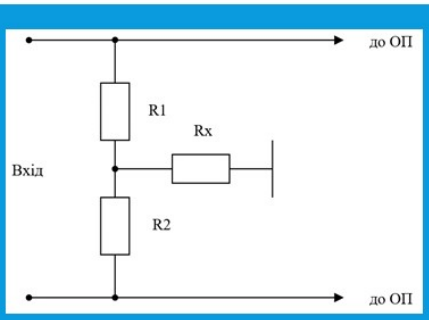
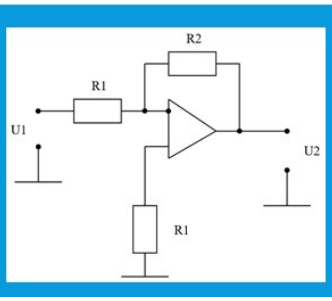
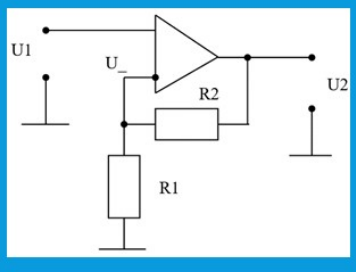


СХЕМА ОПЕРАЦІЙНОГО ПІДСИЛЮВАЧА ТА УЗГОДЖУВАЧА

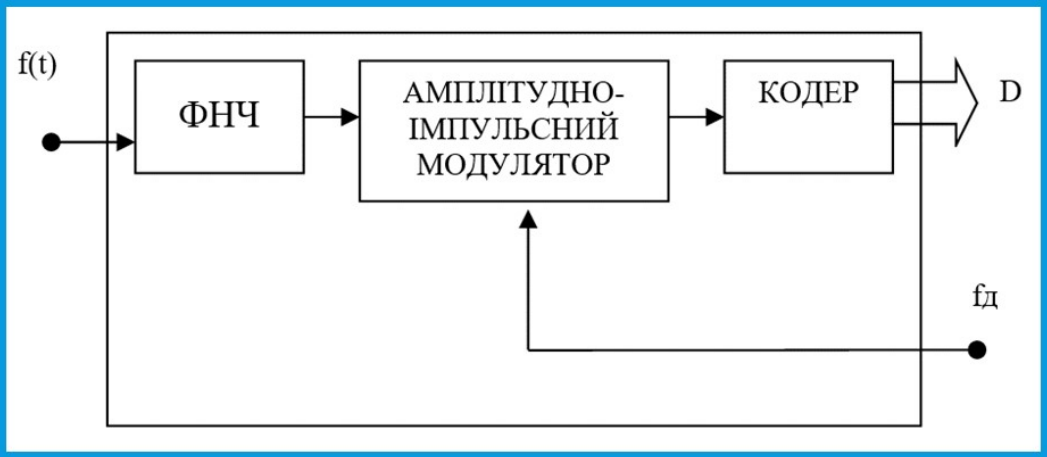


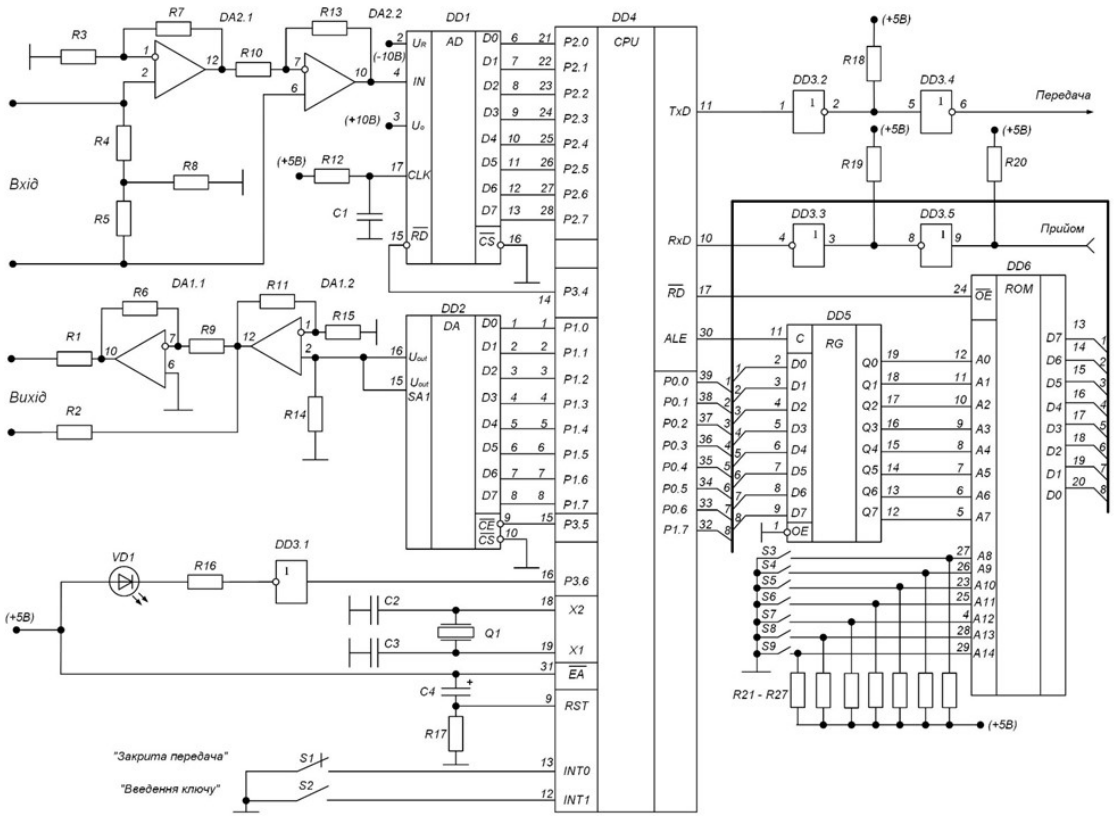




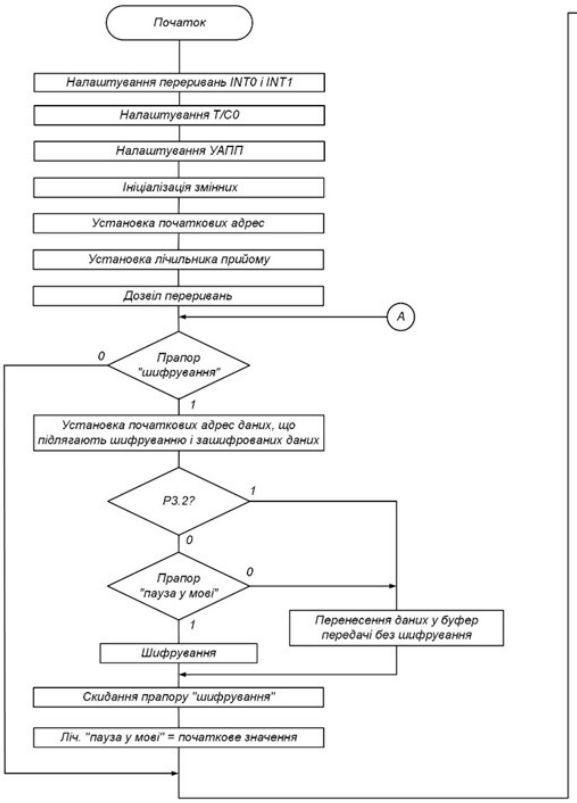


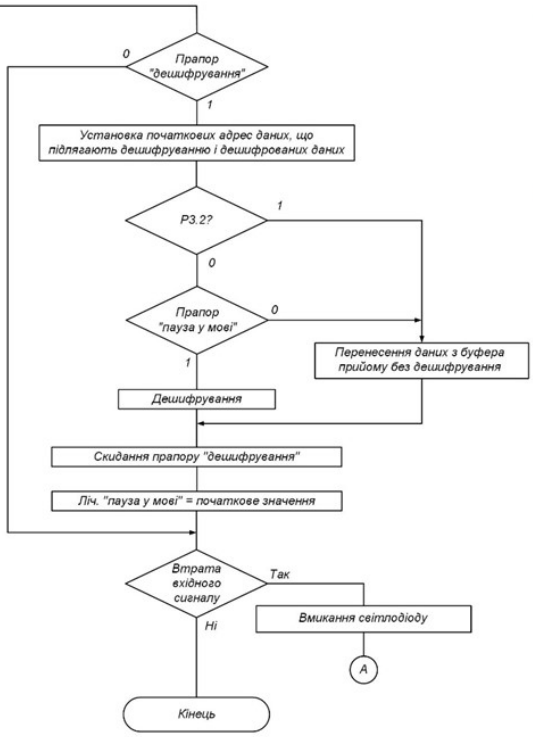
СТРУКТУРНА СХЕМА АЦП AD7574



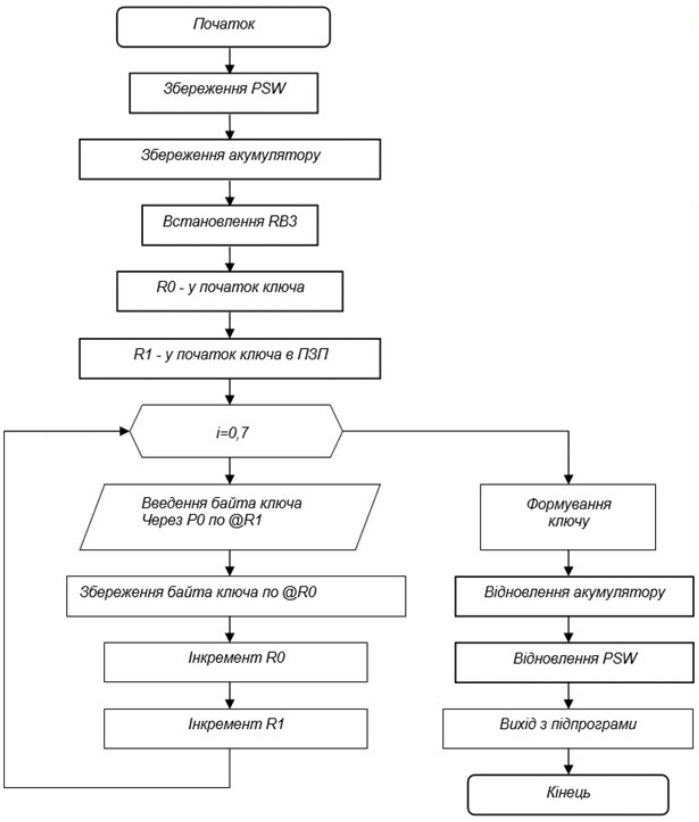


Принципова електрична схема пристрою крипто-захисту

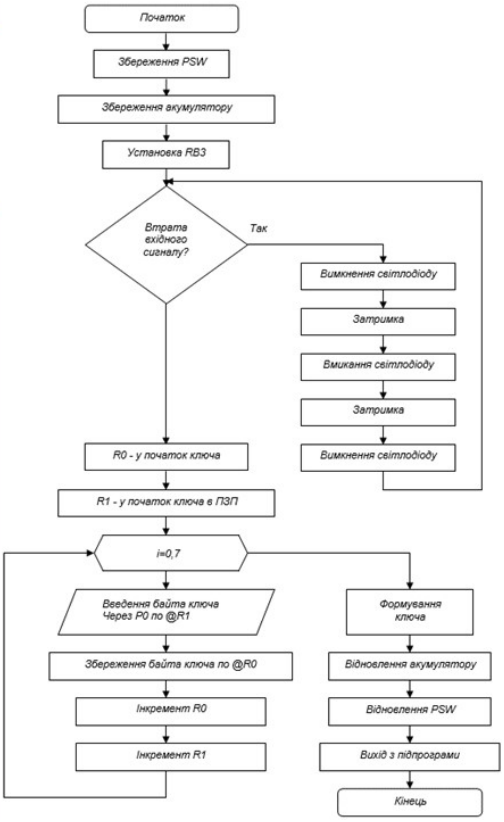


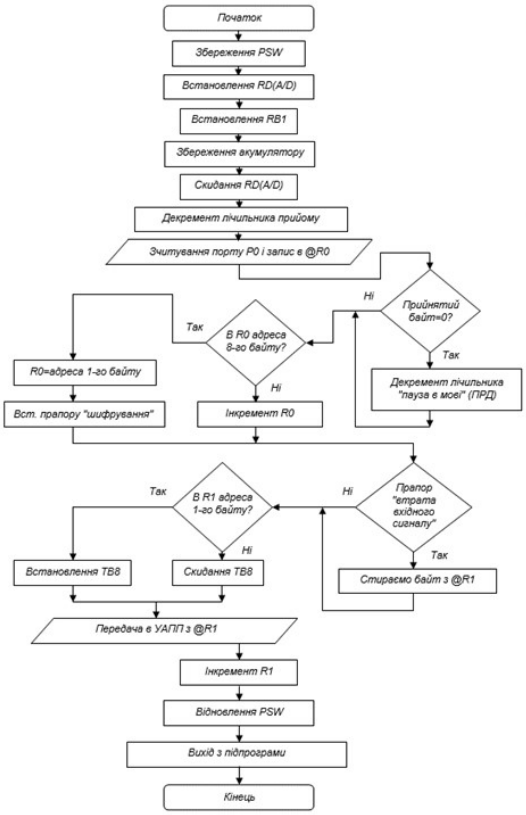


Алгоритм роботи пристрою крипто-захисту каналу передачі конфіденційної інформації

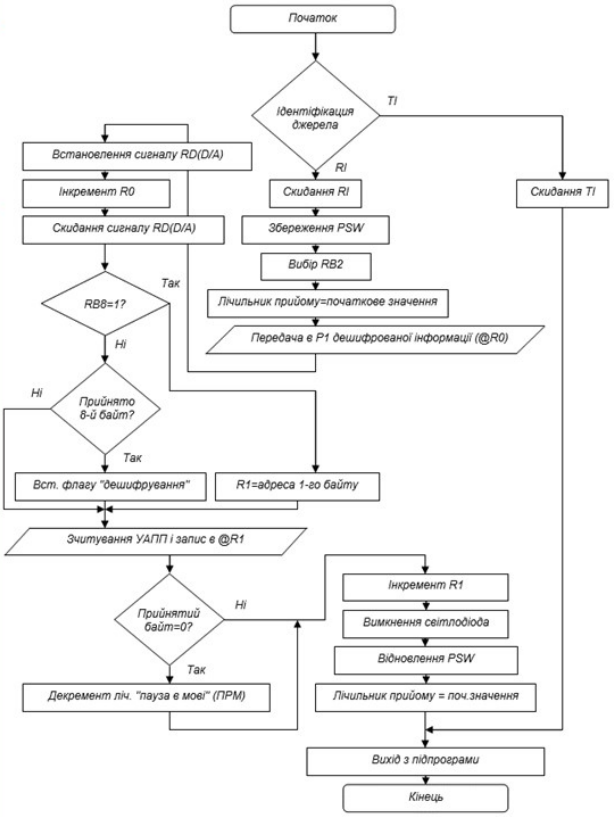


Підпрограми обробки переривань від INT1 (низький пріоритет) та від INTo (низький пріоритет)

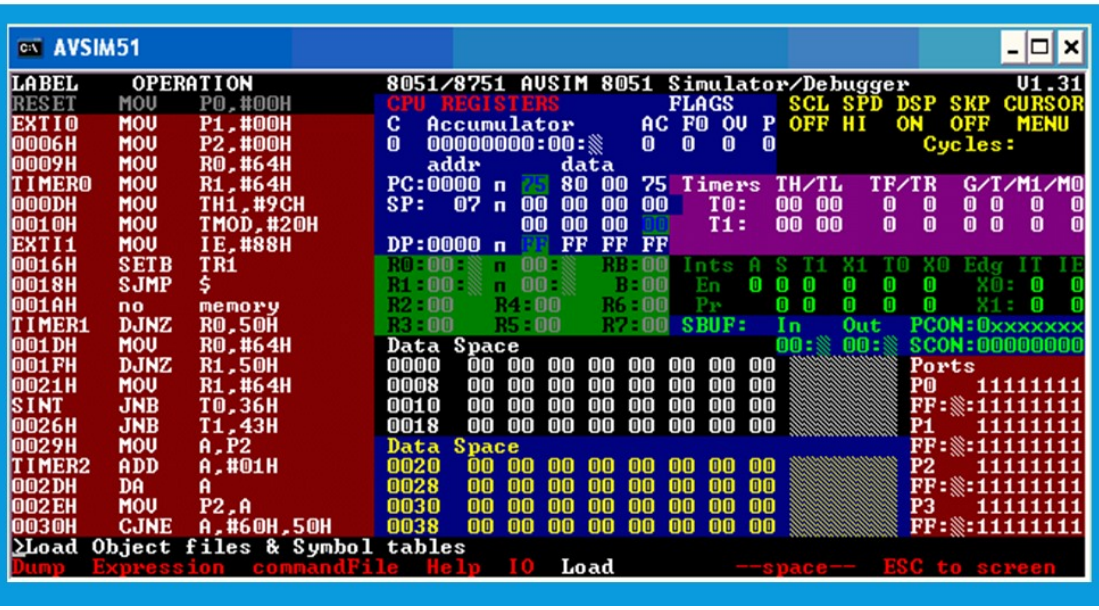




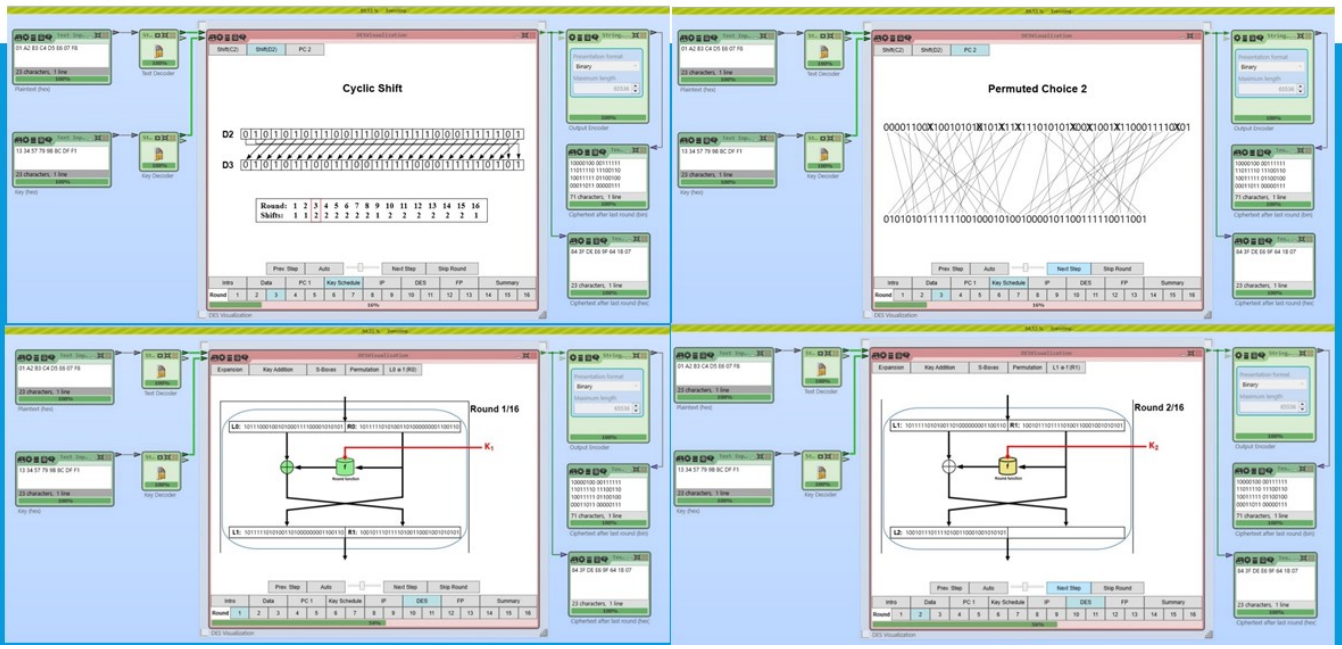
Підпрограми обробки переривань від T/Co (високий пріоритет) та від УАПП (високий пріоритет)



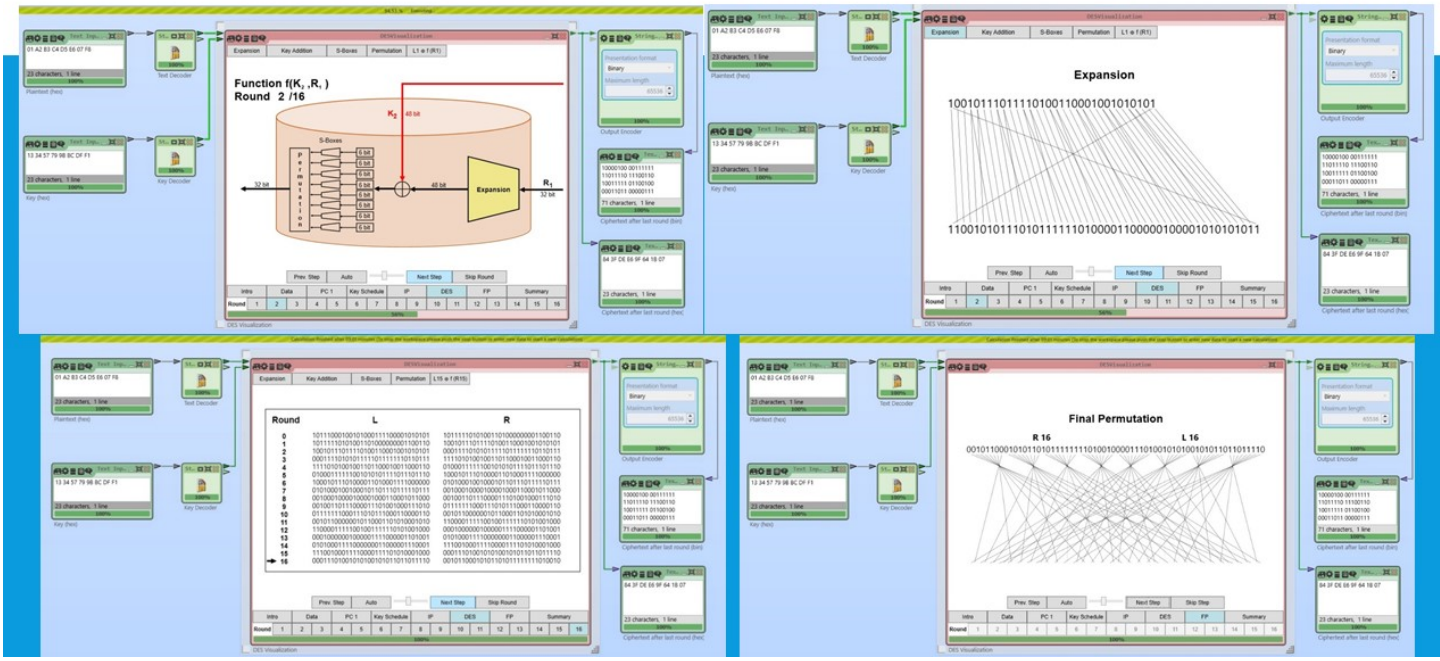
ЕМУЛЯЦІЯ РОБОТИ ПРОГРАМИ ДЛЯ МІКРОКОНТРОЛЕРА ПРИСТРОЮ КРИПТО-ЗАХИСТУ ЗАСОБАМИ СИМУЛЯТОРУ AVSIM51



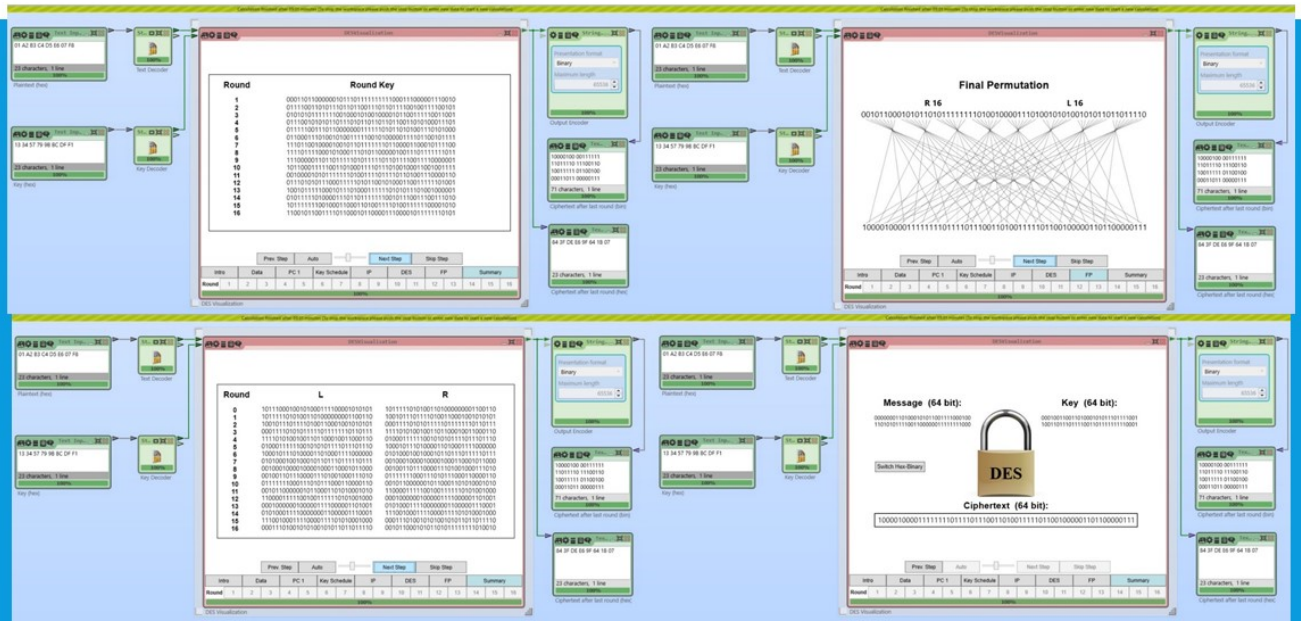
КРОКИ МОДЕЛЮВАННЯ АЛГОРИТМУ DES ПРИ ШИФРУВАННІ ДАНИХ



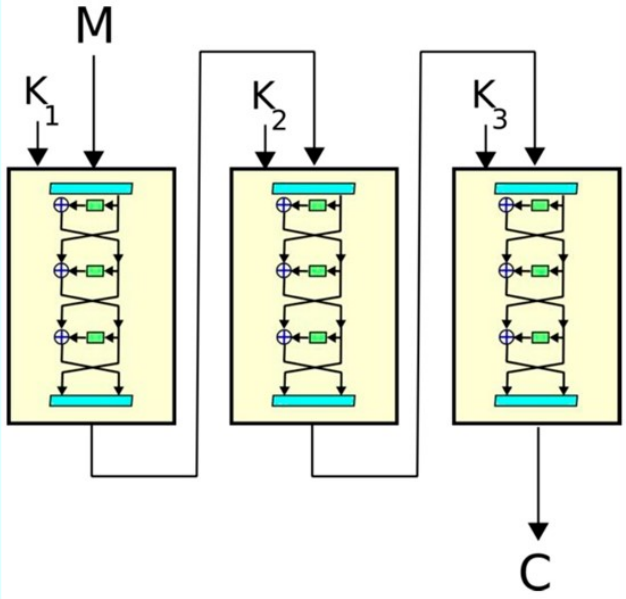
КРОКИ МОДЕЛЮВАННЯ АЛГОРИТМУ DES ПРИ ШИФРУВАННІ ДАНИХ



КРОКИ МОДЕЛЮВАННЯ АЛГОРИТМУ DES ПРИ ШИФРУВАННІ ДАНИХ



МОДИФІКАЦІЯ АЛГОРИТМУ DES (3DES)



ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Кудрявцева Олександра Ігоровича

(прізвище, ім`я та по батькові)

Спеціальність: 123 "Комп'ютерна інженерія"

Освітня програма: «Комп'ютерна графіка і Web-дизайн»

Тема дипломного проекту: Розробка пристрою крипто-захисту каналу конфіденційного електрозв'язку

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки) Дипломний проект виконано відповідно технічному завданню. Пояснювальна записка містить 68 сторінок. У пояснювальній записці описано розробку пристрою крипто-захисту каналу конфіденційного електрозв'язку. Графічна частина складається з 16 слайдів мультимедійної презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та графічної частини добра, розробку виконано в повному обсязі.

б) самостійність роботи над проектом: Протягом всього строку дипломного проектування здобувач освіти Кудрявцев О.І. поступово та послідовно виконував всі етапи розробки. Всі роботи Кудрявцев О.І. виконував самостійно, з оглядом на рекомендації керівника

в) теоретична підготовка випускника (випускниці): Здобувач освіти Кудрявцев О.І. під час роботи над дипломним проектом вивчив достатню кількість літературних джерел та матеріалів за даною тематикою. Вважаю, що теоретична підготовка дипломника достатня і він готовий до захисту дипломного проекту

г) вміння розв'язувати виробничі та конструкторські питання

Під час дипломного проектування здобувач освіти Кудрявцев О.І. мав змогу самостійно приймати окремі рішення з реалізації принципової електричної схеми пристрою та показав вміння організовано працювати над поставленим завданням, використовуючи сучасні програмні засоби розробки, зокрема САПР NI Multisim та ін.

Оцінка розрахункової частини Добре

Оцінка графічної частини Добре

Загальна оцінка Добре

Прізвище, ім'я, по батькові керівника дипломного проекту

Кірєєв Ігор Анатолійович

Місце роботи і посада керівника дипломного проекту

Державний університет інтелектуальних технологій і зв'язку, доцент каф. інформаційної безпеки та передачі даних

Підпис

«12» 06 2023 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект (роботу) здобувача (здобувачки) освіти

відділення комп'ютерних систем

Кудрявцева Олександра Ігоровича

(прізвище, ім`я та по батькові)

Спеціальність 123 "Комп'ютерна інженерія"

Освітня програма «Комп'ютерна графіка і Web-дизайн»

Керівник дипломного проекту (роботи) Кірєєв Ігор Анатолійович

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи) Розробка пристрою крипто-захисту каналу конфіденційного електрозв'язку

Обсяг розрахунково-пояснювальної записки 68 сторінок

Обсяг графічної (презентаційної) частини 16 аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту (роботи) завданню

Представлений на рецензію дипломний проект повністю відповідає меті проектування та технічному завданню. Тематика дипломного проекту є актуальною та присвячена розробки пристрою крипто-захисту каналу конфіденційного електрозв'язку

б) характеристика виконання кожного розділу дипломного проекту (роботи)

Дипломний проект складається зі вступу, трьох розділів, висновків, переліку використаних джерел. У технологічному розділі виконано огляд і аналіз оцінки побудова пристроїв конфіденційного зв'язку, розробка технічних вимог до пристрою крипто-захисту, розробка та опис принципової електричної схеми пристрою крипто- захисту, розробка алгоритмічного забезпечення пристрою, розробка програмного забезпечення для мікроконтролера пристрою крипто-захисту.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту (роботи) Графічна частина виконана на достатньо високому рівні у вигляді презентації із використанням офісного пакету Microsoft PowerPoint та Visio. Пояснювальна записка виконана акуратно та у відповідності до норм оформлення документів із використанням офісного пакету Microsoft Word. Загальна якість виконання документації – добра, академічного плагіату у роботі не виявлено

г) перелік позитивних якостей дипломного проекту (роботи)

Розроблений пристрій крипто-захисту каналу конфіденційного електрозв'язку заснований на використанні алгоритму шифрування DES і дозволить проводити безпечний обмін інформації при використанні з пристроями різних фірм-виробників обладнання з аналогічним алгоритмом шифрування.

д) основні недоліки дипломного проекту (роботи)

1. У пояснювальній записці непередбачені заходи для захисту ключів.
2. У розділі охорони праці наведені відомі нормативні вимоги загального плану замість конкретних розрахунків освітлення приміщення, вентиляції, рівня шуму.

Оцінка розрахункової частини добре

Оцінка графічної частини добре

Загальна оцінка добре

Прізвище, ім'я, по батькові рецензента Стайкуца Сергій Володимирович

Місце роботи і посада рецензента "Державний університет інтелектуальних технологій і зв'язку", доцент кафедри кібербезпеки та технічного захисту інформації, помічник декана факультету інформаційних технологій та кібербезпеки

Підпис:

«_____» _____ 2023 р.

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ
КАДРІВ ДУІТЗ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ * 43997335 * ВІДДІЛ КАДРІВ

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Кудрявцев Олександр Ігорович,
здобувач освіти гр. 4ФКГ-06, та

Кірєєв Ігор Анатолійович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи фахового молодшого спеціаліста на тему:

«Розробка пристрою крипто-захисту каналу конфіденційного електрозв'язку» (автор роботи – Кудрявцев О.І., керівник роботи – Кірєєв І.А.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Кудрявцев О.І. /

Керівник _____ / Кірєєв І.А. /

« 12 » червня 2023 р.

UNICHECK

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015254159

Дата перевірки:
25.05.2023 16:40:01 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
25.05.2023 16:43:49 EEST

ID користувача:
100011688

Назва документа: 4ФКГ-06 Кудрявцев О.І

Кількість сторінок: 49 Кількість слів: 9363 Кількість символів: 63754 Розмір файлу: 764.79 KB ID файлу: 1014928923

30.7%
Схожість

Найбільша схожість: 20.6% з Інтернет-джерелом (https://ela.kpi.ua/handle/123456789/28950)

30.7% Джерела з Інтернету	753	..... Сторінка 51

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	33