МІНІСТРЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра електроніки і комп'ютерної техніки

«До захисту допущено»
Завідувач кафедри
_____ Анатолій ОПАНАСЮК
_____ 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавра

зі спеціальності 172 «Телекомунікації та радіотехніка»,
освітньо-професійної програми «Мережеві та інтернет технології»
На тему:
Пристрій захисту інформації на базі алгоритму книжкового гамування

Здобувача групи ТК-91 Бирин Олександр Олександрович

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

_____ Олександр БИРИН

Керівник, старший викладач,
кандидат фізико-математичних наук, доцент

_____ Ольга БЕРЕЖНА

Суми – 2023

Сумський Державний Університет

Факультет Очний **Кафедра** ЕЛІТ

Спеціальність Телекомунікації та радіотехніка

ЗАТВЕРДЖУЮ:
Зав. кафедри Опанасюк А.С.
«____» _____ 20__ г.

Завдання
на кваліфікаційну роботу бакалавра студенту

Бирину Олександру Олександровичу
(прізвище,ім'я,по батькові)

1. Тема проекта «Пристрій захисту інформації на базі алгоритму книжкового гамування»

затверджено наказом по інституту від «31 » березня 2023 р. № 0316 - VI

2. Термін здачі студентом закінченого проекту 01.06.23

3. Вихідні дані до проекту Розробити пристрій захисту інформації на базі алгоритму книжкового гамування. Синтез пристрою виконати на базі мікропроцесора.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які підлягають розробці) Вступ. 1. Огляд літератури та постановка завдання. 2. Розробка алгоритму функціонування та структурної схеми проектованого пристрою.3. Розробка та розрахунок принципових електричних схем вузлів та блоків пристрою. Висновки.

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

Календарний план

№ п/п	Найменування етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1.	Огляд технічної літератури	31.01.23	
2.	Розробка алгоритму функціонування та структурної схеми пристрою	15.02.23	
3.	Розрахунок вузлів та блоків пристрою та розробка схеми електричної принципової	10.03.23	
4.	Оформлення графічної частини	1.05.23	
5.	Оформлення пояснювальної записки	15.05.23	
6.	Рецензування та підготовка до захисту	30.05.23	

Студент-дипломник _____

Керівник проекту _____

АНОТАЦІЯ

Пояснювальна записка містить: 35 аркушів, 13 рисунків, 9 джерел літератури.

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

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

Перший розділ містить загальну інформацію про методи шифрування, їх різновид, плюси та мінуси.

Другий розділ присвячений розробці алгоритму функціонування та структурної схеми проектованого пристрою.

Третій розділ присвячений розробці принципової схеми пристрою.

ЗМІСТ

ВСТУП

Конфіденційна інформація в сучасному цифровому світі стає все більш цінною та піддається різноманітним загрозам безпеки. Володіти та захищати цю інформацію стає важливим завданням для компаній, установ, організацій та індивідуальних користувачів. Цей проект на присвячений вивченню та розробці ефективних методів і технологій для забезпечення конфіденційності, цілісності та доступності цієї важливої інформації.

Метою даного проекту є проведення детального аналізу загроз та вразливостей, що становлять ризик для конфіденційної інформації, та розробка комплексної системи захисту. Проект передбачає використання сучасних криптографічних алгоритмів, механізмів контролю доступу в сфері захисту інформації.

Результатом дипломного проекту буде розроблена система, що забезпечує високий рівень шифрування даних та контроль цілісності.

Враховуючи постійно зростаючу важливість захисту конфіденційної інформації, цей дипломний проект буде мати практичне значення для багатьох сфер діяльності, включаючи банківський сектор, торгівлю, медицину, державні установи та багато інших. Цей проект має на меті сприяти розвитку та вдосконаленню практик захисту конфіденційної інформації, що є критично важливим у сучасному цифровому світі.

1 ОГЛЯД ЛІТЕРАТУРИ І ПОСТАНОВКА ЗАВДАННЯ ПРОЕКТУВАННЯ

1.1 Завдання захисту інформації в інфокомунікативних системах

На сучасному етапі розвитку економіки і суспільства в цілому інформація, серед основних завдань захисту даних в інфокомунікативних системах є забезпечення конфіденційності повідомлень, текстів, документів, тощо; забезпечення вірної аутентифікації; забезпечення засобів безпеки цілісності даних; забезпечення доступності інформації для легальних користувачів. Так за джерелом [1]: конфіденційність - це властивість інформації бути захищеною від несанкціонованого ознайомлення; цілісність - це властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення; доступність - це властивість інформації бути захищеною від несанкціонованого блокування; технічний захист інформації - це діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Іншими словами, конфіденційність – це гарант доступу до потрібної інформації, що зберігается в інфокомунікаційній системі і пересилаються по каналам зв’язку користувачам які мають до неї право доступу.

Цілісність - це гарантування можливості модифікації інформації, що міститься в інформаційній системі і пересилається по каналах зв'язку тільки тими суб'єктами, які мають на це право. Модифікація може означати: запис, зміну, зміну стану, видалення, створення повідомлень, що пересилаються.

Керування доступом – це можливість дати доступ до контролю над інформаційним ресурсом або самою системою.

Доступність – це гарант авторизованим суб'єктам доступу до даних, що зберігається в системі в разі необхідності.

Суб’єкт та Об’єкт інформаційної діяльності – це той, хто створює або модифікую данні та власне «предмет праці» - дані, повідомлення, тексти що складаються Суб’єктом з символів певного алфавіту, певними правилами та несуть інформацію, що потребує захисту

Криптографічне шифрування - це кодування, як своєрідна форма подання інформації дискретними даними, з метою забезпечити вирішення

згаданих вище завдань захисту інформації.

Аналіз загрози інформації виходячи з мети її досягнення, моделі зловмисника, уявлення про можливий сценарій виконання та процедури реалізації має назву «модель загрози інформації».

1.2 Моделі цифрових систем комунікації

Під терміном канал передачі даних зазвичай розуміють сукупність середовища розповсюдження сигналу та каналоутворюючого обладнання. На Рисунку 1.1 наведено одну з можливих сучасних моделей цифрової системи зв’язку.

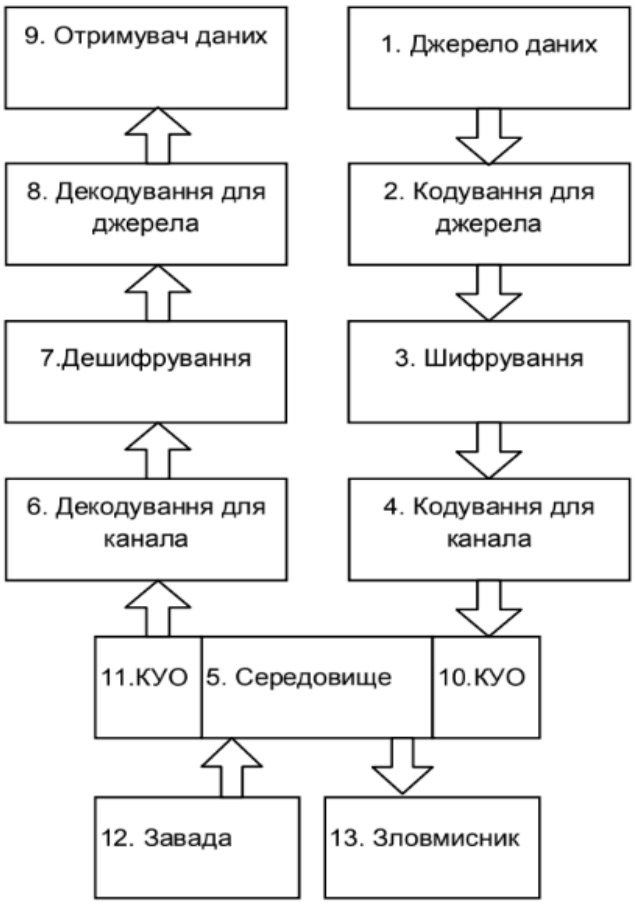

Рисунок 1.1 – Модель цифрової системи комунікації

На Рисунку 1.1 позначені функціональні блоки сучасної цифрової системи комунікації: Джерело даних 1 та Отримувач даних 9; Кодек для джерела 2 та 8; Блоки Шифрування/Дешифрування 3 та 7; Кодек для канал 4 та 6; канал передачі даних 5,10 та 11; Джерело завад 12; Зловмисник 13.

Принцип роботи: Джерело 1 направляє Отримувачу 9 відкрите, незахищене повідомлення яке може перехопити Зловмисник 13 у Середовищі 5.

Кодек для джерела (блоки 2 та 8) виконує функцію стиснення і відновлення даних для джерела (архівування/деархівування), що зменшує витрати ресурсів на подальше зберігання, перетворення та передачу повідомлень за рахунок зменшення кількості символів, якою подається задана у висхідному повідомленні кількість інформації.

Криптографічні блоки Шифрування/Дешифрування 3 та 7 у моделі Рис.1 виконують функцію забезпечення конфіденційності повідомлень у блоках 4, 5, 6, 10 та 11, і, власне, у Середовищі 5, де очікується, що вони можуть бути перехоплені Зловмисником.

Кодек для канала 4 та 6 виконує функцію кодування/декодування повідомлень надлишковими кодами для забезпечення завадостійкості повідомлень, що передаються, у разі випадкового спотворення Завадою 12 деяких символів тих повідомлень.

Симетричною називають криптосистему з єдиним (секретним,приватним) ключем K для зашифрування і дешифрування повідомлення, для якого потрібно забезпечити конфіденційність у разі зберігання, або передавання його через відкритий, незахищений канал зв’язку.

Асиметричною називають криптосистему з двома математично взаємообумовленими ключами. Один із них називають відкритим або публічним ключем, а інший - секретним або приватним ключем. Публічний ключ є у відкритому доступі для інших користувачів у будь-який час. Знаходження приватного ключа за відомим значенням публічного не є можливим без знання певних секретних даних.[1]

На рисунку 1.2 представлене основні особливості симетричних та асиметричних форм шифрування.

Симетричне шифрування	Асиметричне шифрування
Один ключ використовується для шифрування і дешифрування даних.	Пара ключів використовується для шифрування і дешифрування. Ці ключі відомі як “відкритий ключ” і “закритий ключ”.
Простий метод шифрування, так як використовується тільки один ключ.	У зв’язку з тим, що використовується пара ключів – процес складний.
Використовується для шифрування великих об’ємів даних.	Забезпечує аутентифікацію.
Забезпечує високу продуктивність і вимагає менше обчислювальної потужності.	Складні процеси протікають повільніше і вимагають більшої обчислювальної потужності.
Для шифрування даних використовується менша довжина ключа (128-256 біт).	Використовуються довші ключі шифрування (1024-4096 біт).
Ідеально підходить для шифрування великої кількості даних.	Використовується при шифруванні невеликого об’єму даних.
Стандартні алгоритми: RC4, AES, DES, 3DES і QUAD.	Стандартні алгоритми: RSA, Diffie-Hellman, ECC, El Gamal і DSA.

Рисунок 1.2 – основні особливості симетричних та асиметричних форм шифрування

З точки зору безпеки, асиметричне шифрування, безсумнівно, краще, оскільки воно забезпечує аутентифікацію. Однак продуктивність є аспектом, який не можно ігнорувати, тому симетричне шифрування завжди буде необхідно.

Оцінка якості та ефективності криптоалгоритмів визначається криптостійкістю. Криптостійкість криптоалгоритма це обсяг часу, потрібний криптоаналітику для розкриття смислу зашифрованого текста без знання секретних даних, наприклад, секретного ключа [2].

1.3 Шифри заміни

Заміна (підстановка) – це метод шифрування, при якому кожен знак вихідного тексту взаємнооднозначно замінюється шифропозначенням – одним або декількома знаками деякого набору символів (алфавіту).

Шифр однобуквеної простої заміни – один з найдавніших шифрів. Шифропозначення для нього застосовувались різні – від букв алфавіту до фігурок «танцюючих чоловічків». Давно відомі і його очевидні слабкості – у шифрованому тексті зберігаються всі частотні характеристики відкритого тексту, усі сполучення і повторення. У зв'язку з цим, навіть у художній і науково-популярній літературі наводяться приклади його дешифрування. У

найпростішому вигляді даний шифр полягає в тому, що буква переходить у букву, а вхідний і вихідний алфавіти збігаються як множини, тобто з точністю до перестановки. Для зашифрування чергової букви відкритого тексту визначається її номер у вхідному алфавіті і на відповідне місце формовного шифртексту поміщається буква з тим же номером, але вже з вихідного алфавіту. Нехай, наприклад, вхідний, вихідний алфавіти і відкритий текст мають, відповідно, вигляд

ABCDEFGHIJKLMNOPQRSTUVWXYZ

JKLMNOPQRSTUVWXYZABCDEFGHI

TOBEORNOTTOBETHATISTHEQUESTION .

Буква T – двадцята у вхідному алфавіті. У вихідному алфавіті на двадцятому місці знаходиться буква C. Таким чином, першим знаком шифртексту є буква C. Аналогічно, друга буква, яка має у вхідному алфавіті номер 15, заміняється на п'ятнадцяту букву вихідного алфавіту, тобто X. Отже, другою буквою шифрованого тексту є буква X. У підсумку, виходить таке зашифроване повідомлення:

XKNXAWXCCXKNCQJCRBCQNZDNBCRXE

Наступний приклад являє собою так званий шифр двозначної заміни, у якому кожна буква вхідного алфавіту замінюється взаємно однозначною парою цифр. Для користувача, застосовуються таблиці.

Буква, яка підлягає зашифруванню, відшукується в таблиці. На відповідне місце в шифртексті розміщується пара цифр, яка складається з номера рядка і номера стовпця, на перетині яких знаходиться згадана буква. Наприклад, буква T знаходиться на перетині першого рядка і третього стовпця. Отже, вона заміняється на пару 13. Аналогічно, буква O виглядає як пара цифр 30. Після зашифрування відкритого тексту з попереднього прикладу отримуємо таке шифроване повідомлення:

133002243014113013133002241343031333321343241021243213333011.

У розглянутих нами прикладах шифрів перетворення повідомлення проводилось поетапно: спочатку перетворювався перший елемент відкритого тексту (буква), потім другий і так далі. Неважко узагальнити цю ситуацію на сполучення трьох, чотирьох і більше знаків. У криптографії послідовні етапи перетворення відкритого тексту називаються тактами шифрування. Елемент, що перетворюється в одному такті шифрування, є найменшою складовою

відкритого тексту, яку можна зашифрувати за допомогою даного шифру. Наприклад, під час заміни пар букв на пари, можна зашифрувати сполучення АВ, але неможливо зашифрувати букву А або букву В окремо.

На кожному такті шифрування, у випадку простої заміни, діє та ж сама таблиця. У більш складних шифрах на кожному такті може діяти своє перетворення. Це не означає, що для кожного такту необхідний свій ключ. Просто в інших видах шифрсистем ключ визначає і закони формування таблиць перетворень і послідовність вибору цих таблиць.

Протягом одного такту шифрування шифрсистема може перетворити один або кілька знаків, деяку ділянку відкритого тексту, склад, фразу, слово і, в принципі, ціле повідомлення. Шифри заміни перетворять на кожному такті групусимволів. Кількість знаків у групі при цьому фіксована і називається значністю групи. Групи значності 2 називаються біграмами, значності 3 – триграмами, значності 4 – чотириграмами і так далі. У загальному випадку групи значності v називаються v -грамами.

Можлива побудова шифру, аналогічного шифрові заміни, коли в такті шифрування можуть перетворюватися групи різної значності. Такою властивістю володіють шифрсистеми, які називаються кодами. Специфічною особливістю кодів є те, що вони оперують не з довільними комбінаціями символів, а зі словами, складами і фразами. У найпростішому випадку код являє собою список, який нагадує словник, у якому кожній відкритій величині (слову, фразі) відповідає кодова група: комбінація символів, яка замінює відповідну величину під час зашифрування. Значність кодових груп постійна. Зазвичай до складу коду входять також деякі допоміжні величини – цифри, розділові знаки та інше.

Очевидно, що код, який дозволяє зашифрувати на рівні слів довільний відкритий текст, повинен мати об’єм, порівняний з докладним словником природної мови, що для практичного застосування незручно, тим більше, якщо врахувати, що коди традиційно відносяться до ручних систем шифрування, тобто не розраховані на використання засобів автоматизації. В цьому зв'язку, під час складання коду, основним етапом є вивчення словникового складу майбутнього листування, у результаті чого визначається набір слів і фраз, які підлягають занесенню в список словникових величин. Чим яскравіше виражена специфіка листування, тим

компактніше та зручніше у використанні код. На практиці цеприводить до «спеціалізації» кодів, тобто до того, що не будь-який відкритий текст може бути якісно зашифрований за допомогою конкретного коду. З іншого боку, перевагою кодів є ущільнення інформації під час зашифрування, оскільки кодові групи, як правило, коротші величин, які вони заміняють. Як і будь-який інший шифр, код може бути тим або іншим чином модифікований. Він може бути ускладнений, наприклад, за рахунок використання різних кодових груп для зашифрування однієї і тієї ж відкритої величини. Вибір кодової групи з відповідного списку здійснюється випадковим чином.

Аналогічна процедура, яка називається рандомізацією, може застосовуватися для перетворення відкритого тексту перед зашифруванням незалежно від системи шифру. Перетворення полягає в тому, що знаки відкритого тексту замінюються на символи іншого алфавіту, більшого за об’ємом, ніж вихідний. У процесі заміни конкретна буква переходить випадковим чином в один із зв'язаних з нею символів. Кількість таких символів для кожної букви різна і пропорційна частоті її зустрічності у вихідному відкритому тексті. В результаті отримується послідовність, усі знаки якої зустрічаються приблизно з однаковою частотою. Рандомізація може бути введена в будь-яку криптографічну систему і її використання ускладнює розкриття шифру на основі статистичного аналізу.

1.4 Шифри перестановки

Розглянуті вище шифри здійснювали перетворення відкритого тексту за методом заміни його знаків деякими шифрпозначеннями. Тим часом можливий й інший метод перетворення – перестановка знаків відкритого тексту за заданим правилом. Шифри типу перестановки застосовувались ще з античних часів. Відмінність цього типу шифру від шифрів заміни полягає в тому, що під час зашифрування буква аі відкритого тексту переходить не у фіксований знак алфавіту, а в іншу букву того ж відкритого тексту, скажемо, аj у результаті чого букви розташовуються на нових місцях, тобто переставляються. Ключем для даного шифру також служить таблиця заміни, тільки не букв алфавіту, а їхніх індексів (номерів місць) у тексті, який підлягає зашифруванню. У загальному випадку розмір таблиці заміни дорівнює довжині відкритого тексту. Такі таблиці зручно формувати (і

записувати) у вигляді так званих підстановок, тому нагадаємо коротенько їхні деякі властивості. Підстановкою називається взаємно однозначне відображення скінченої множини на себе. Зазвичай підстановки записують у вигляді двох рядків.

Верхній рядок є операндом підстановки, а нижній – результатом її дії на операнд.

1.5 Шифри гамування

Шифрування гамування полягає в складанні символів тексту із символами деякої випадкової послідовності, іменованою гамою шифру. Стійкість шифру визначається довжиною неповторюваної частини гами шифру. Оскільки за допомогою сучасних комп'ютерів можно згенерувати практично нескінченну гаму шифру, то даний спосіб є одним із основних для шифрування даних в інфокомунікаційних системах. Перед шифруванням відкритий текст поділяється на блоки однакової довжини $T_0^{(i)}$ зазвичай по 64 біти. Гама шифру виробляється у вигляді послідовності блоків аналогічної довжини $Г_ш^{(i)}$.

$$T_ш^{(i)} = Г_ш^{(i)} \oplus T_0^{(i)},\ i=1,..к$$ – процес шифрування

$$T_0^{(i)} = Г_ш^{(i)} \oplus T_ш^{(i)},\ i=1,..к$$ – процес дешифрування

Де $T_ш^{(i)}$- i-й блок шифру; $T_0^{(i)}$- i-й блок відритого тексту; $Г_ш^{(i)}$ - i-й блок гами; $к$- кількість блоків.

Гамування - це процес накладання за певним законом гами шифру на відкриті дані. Під гамою шифру розуміється псевдовипадкова двійкова послідовність, що виробляється за заданим алгоритмом для зашифровування відкритих даних і розшифрування зашифрованих даних.

Такий шифротекст є складним для розкриття, так як ключ є постійною змінною. Гама шифру має змінюватися випадково для кожного зашифровуваного тексту. Якщо період гами перевищує довжину всього зашифрованого тексту то стійкість шифру визначається довжиною ключа.[3]

До криптографічно стійкого генератора псевдовипадкової послідовності чисел (гами шифру) пред'являються три основних вимоги:

- період гами має бути надто великим дня шифрування повідомлень різної довжини;
- гама шифру має бути практично непередбачуваною, що означає неможливість передбачати наступний біт гами, навіть якщо відомі є тип генератора і попередній фрагмент гами;
- генерування гами шифру не повинно призводити до великих технічних складностей.

Довжина періоду гами шифру є найважливішою характеристикою генератора псевдовипадкових чисел. Після закінчення періоду гами шифру числа розпочнуть повторюватися – і їх можна буде передбачати. Необхідна довжина періоду гами шифру визначається ступенем закритості даних. Чим довшим є ключ, тим складніше його підібрати. Довжина періоду гами шифру залежить від обраного алгоритму отримання псевдовипадкових чисел.

Щоби гама шифру вважалася непередбачуваною, тобто насправді випадковою, необхідно, аби її період був надто великим, а різноманітні комбінації бітів певної довжини були рівномірно розподілені по всій її довжині.

Третя вимога зумовлює можливість практичної реалізації генератора програмно чи апаратно із забезпеченням потрібної швидкодії.

Один з перших способів генерування псевдовипадкових чисел з використанням ЕОМ запропонував у 1946 році Джон фон Нейман. Суть цього способу полягає в тому, що кожне наступне випадкове число утворюється піднесенням до квадрата попереднього числа з відкиданням цифр молодших і старших розрядів. Однак цей спосіб виявився ненадійним – і від нього невдовзі відмовились.

1.6 Постановка завдання проекту

Метою даної роботи є створення пристрою захисту інформації на базі алгоритму книжкового гамування.

Для досягнення цієї мети необхідно виконати наступне:

1. Визначити основні функції та завдання, які повинен виконувати пристрій захисту інформації.
2. Розробити алгоритм функціонування пристрою.
3. Розробити схему електричну структурну пристрою захисту інформації.
4. Розробити схему електричну принципову пристрою захисту інформації на базі алгоритму книжкового гамування.

2 РОЗРОБЛЕННЯ, ОБҐРУНТУВАННЯ АЛГОРИТМУ ФУНКЦІОНУВАННЯТА СТРУКТУРНОЇ СХЕМИ ПРИСТРОЮ, ЩО ПРОЕКТУЄТЬСЯ

2.1 Розроблення алгоритму роботи пристрою захисту інформації

У роботі було розглянуто ідеальний шифр – шифр, що використовує одноразовий блокнот. Відправник використовує кожну літеру з блокнота, щоб зашифрувати рівно одну літеру відкритого тексту повідомлення, причому блокнот використовується лише один раз.

Перевага даного шифрування в тому, що зашифроване повідомлення не буде схильне до частотного аналізу, що сильно підвищує стійкість даного шифру до несанкціонованого розшифрування. Головний недолік даного шифру - складність у передачі одноразового блокнота.

Щоб вирішити цю проблему шифру, використовувалася заздалегідь певна, незмінна та загальнодоступна бібліотека літературних творів, яка буде безліччю різноманітних комбінацій одноразових блокнотів.

Для однозначного визначення одноразового блокнота для відправника та одержувача використовувався ключ, який також не передавався між відправником та одержувачем, а вибирався за заздалегідь визначеним алгоритмом, використовуючи відкрите джерело. Таким чином, відпадає необхідність передачі одноразового блокнота, адже кожен учасник обміну зможе згенерувати його на своєму боці.

Принцип шифрування полягає у посимвольній заміні вихідного повідомлення на порядковий номер символу в одноразовому блокноті.

Алгоритм роботи пристрою наведений на рисунку 2.1.

Алгоритм функціонування пристрою захисту інформації на базі методу книжкового гамування полягає у наступному.

Крок 1.Введення відкритого тексту

Крок 2. Перевірка на здійснення введення тексту

Крок 3. Визначення алфавіту

Крок 4. Виконується числове кодування символів в алфавіті.

Крок 5. Двійкове кодування номерів символів алфавіту.

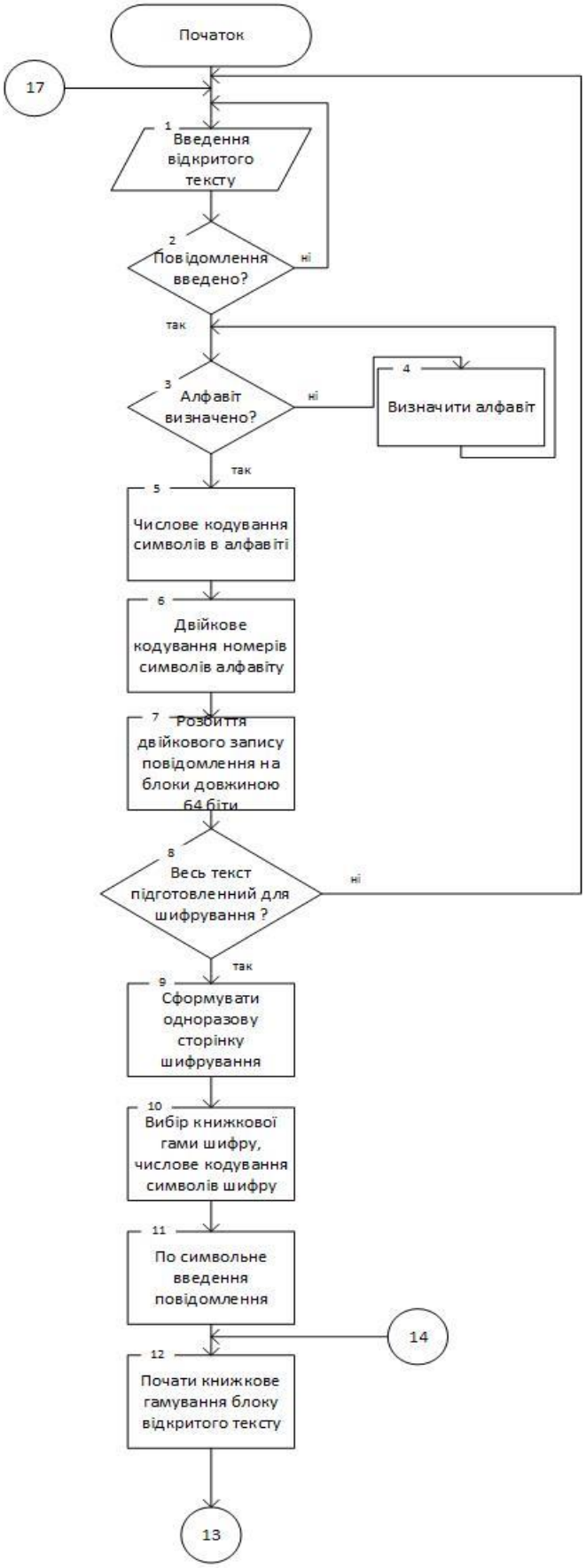

Рисунок 2.1 - Схема алгоритму роботи пристрою

Продовження рисунку 2.1

Крок 6. Виконується розбиття двійкового запису повідомлення на блоки довжиною 64 біти.

Крок 7. Перевірка готовності тексту до шифрування.

Крок 8. Формування одноразової сторінки шифрування.

Крок 9. Вибір книжкової гами шифру, числове кодування символів шифру.

Крок 10. По символьне введення повідомлення.

Крок 11. Початок книжкового гамування відкритого тексту.

Крок 12. Підсумування числових символів тексту та гами шифру по

модулю потужності алфавіту.

Крок 13. Перевірка чи всі блоки зашифровано.

Крок 14. Запис шифрограми.

Крок 15. Передача шифрограми.

Крок 16. Запит за продовження роботи.

У період класичної криптографії не виникало потреби записувати відкритий текст та криптотекст якось інакше, ніж у звичайній абетці. Завдяки цьому криптограф-практик не потребував для роботи нічого, крім письмового приладдя свого часу, чого було достатньо і для шифрування, і для пересилання повідомлення. Але як тільки необхідно скористатися модерними засобами зв'язку для передачі повідомлення, або доручити шифрування комп'ютерові, то виявляється, що у технічному відношенні традиційний текст не є найзручнішою формою для перетворення та передачі інформації.

З цього погляду вигіднішим є подання інформації у цифровій формі. Кожен символ тексту заміняється його номером у алфавіті. Нумерація, як правило, починається з 0. Для прикладу, слово банан буде подане як 01 00 17 00 17. Кожна літера представлена своїм номером, записаним двома цифрами, перша з яких може бути нулем. При потребі в алфавіт можна включити окрім букв також знаки пунктуації, пропуск, цифри тощо.

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И
0	1	2	3	4	5	6	7	8	9	10
І	Ї	Й	К	Л	М	Н	О	П	Р	С
11	12	13	14	15	16	17	18	19	20	21
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
22	23	24	25	26	27	28	29	30	31	32

Рисунок 1.3 – Нумерація букв українського алфавіту.

Номери букв можна записувати в двійковій системі числення. Для того ж слова банан матиме місце запис 000001000000010001000000010001, де кожен блок із шести цифр є номером відповідної букви у двійковому записі. Така форма подання тексту називається двійковою.

Таким чином, довільний текст можна записати у двійковій формі, використовуючи всього лише два символи - 0 та 1. Ці два символи називаються бітами. Будь-яку послідовність бітів називають двійковим словом.

Шифр одноразового блокноту був винайдений у 1917 році Гілбертом Вернамом. Назва шифру походить від того, що агент, який здійснював шифрування вручну, отримував свої копії ключів записаними у блокноті. Як тільки ключ використовувався, сторінка з ним знищувалась. Зрозуміло, що шифр просто реалізується і технічними засобами.

Перед шифруванням повідомлення M записують у двійковій формі. Ключем K служить довільні двійкове слово однакової з M довжини. Криптотекст C отримують побітовим додаванням повідомлення і ключа, тобто $C = M \oplus K$.

Для прикладу, нехай потрібно зашифрувати слово банан. Записуємо його у двійковій формі:

$$M = 000001000000010001000000010001.$$

В якості ключа виберемо

$$K = 001101110101100010011000111010.$$

Сумування цих двох двійкових послідовностей вже проведене вище. Отож маємо криптотекст

$$C = 001100110101110011011000101011.$$

Дешифрування у шифрі одноразового блокноту збігається із шифруванням, тобто щоб отримати вихідне повідомлення M, слід додати до криптотексту C той же ключ K. Це випливає з того, що оскільки $C = M \oplus K$, то

$$C \oplus K = (M \oplus K) \oplus K = M \oplus (K \oplus K) = M \oplus 0 = M .$$

Однак обмеженість сфери застосувань шифру очевидна, оскільки вінвимагає ключа не меншої довжини, як саме повідомлення. З цією обставиною пов'язані дві проблеми. Перша полягає в генеруванні довгої послідовності випадкових бітів. Другою проблемою є необхідність у надійному каналі для регулярного обміну довгим ключем (на зразок дипломатичної пошти). У більшості ситуацій такого каналу або взагалі нема, або ж він не є достатньо швидким [4].

Буква	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
Код	0	1	2	3	4	5	6	7	8	9	10	11	12
Буква	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Код	13	14	15	16	17	18	19	20	21	22	23	24	25
Буква	Ь	Ы	Ъ	Э	Ю	Я							
Код	26	27	28	29	30	31	32						

Рисунок 2.2 - Табличне представлення шифру книжкового гамування для Української мови

Використовуючи номер книги, який є частиною ключа, вибирається книга з бібліотеки. У блоці шифрування отриманий твір подається на підблок формування блокнота шифрування, де за допомогою 2 частини ключа (символьного зсуву) здійснюється вибір потрібної частини книги, яка стане одноразовим блокнотом шифрування. Одноразовий блокнот пересилається до блоку циклічної заміни, який здійснює шифрування відкритого тексту.

2.2 Розробка структурної схеми

На основі алгоритму функціонування розробляється структурна схема пристрою. Вона являє собою сукупність блоків з відображенням відповідних зв’язків між ними. На рис 2.3 представлена структурна схема пристрою.

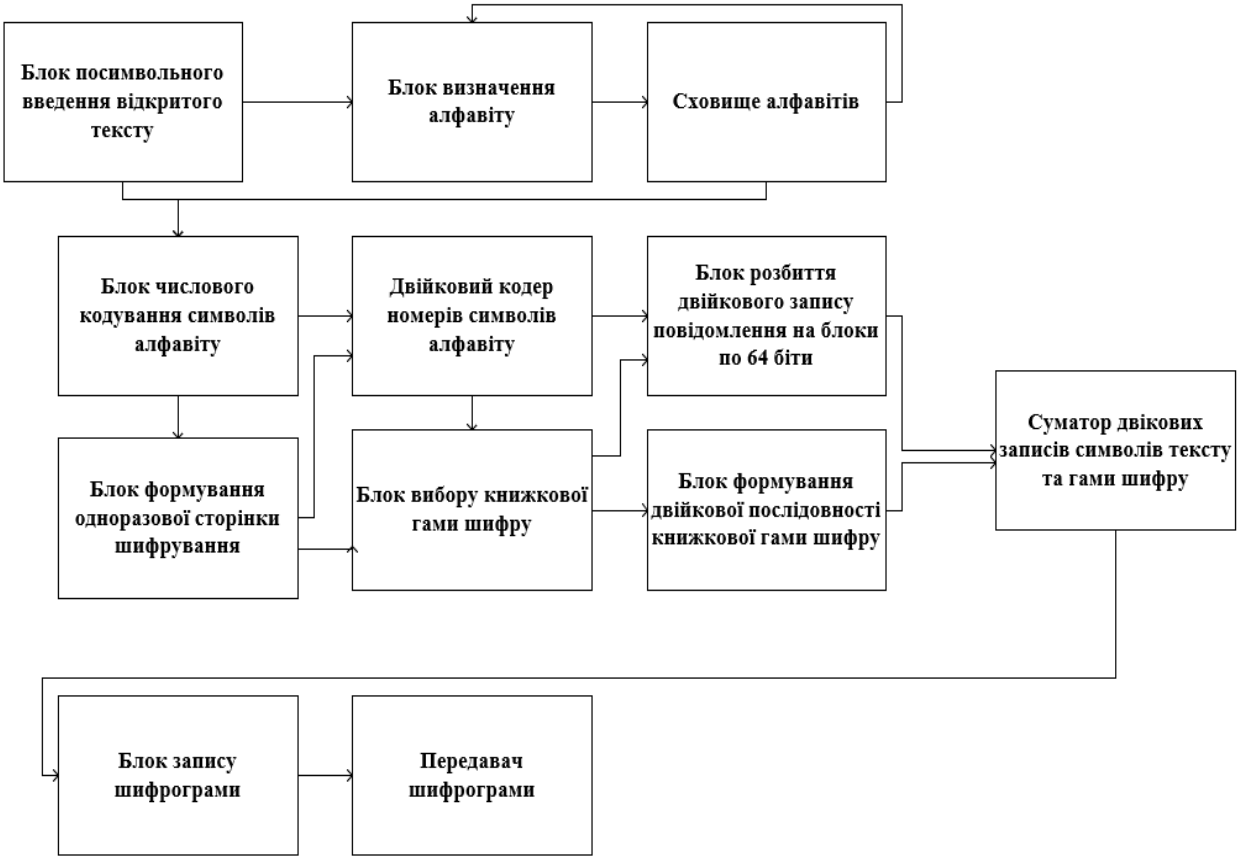

Рисунок 2.2 – Структурна схема пристрою

Всі блоки, які входять до складу структурної схеми, виконують певні функції.

Формування ключа - даний блок призначений для введення ключа для шифрування даного рядка.

Введення команд - даний блок призначений для введення команд для керування.

Вибір рядка - даний блок призначений для вибору рядка, в якому вказаний текст для шифрування.

Перевірка символів в рядку - блок, який виявляє помилки у рядку. Аналіз - визначення мови, для тексту в рядку.

Заміна символів - блок, який виправляє помилки у рядку.

Керування - видає керуючі сигнали, необхідні для коректної роботи всіх блоків.

Гамування - блок призначений для формування гамми

Пам’ять - блок призначений для запису інформації.

Шифрування - блок, який виконує шифрування даного тексту.

Шифрограмма - зашифрований текст.

Принцип роботи пристрою захисту конфіденційної інформації полягає в наступному:

Керування пристроєм здійснюється за допомогою пульта керування, який формує відповідні команди керування, шифрує їх за допомогою шифру книжкового гамування та передає до одержувача за допомогою каналу зв’язку. Принцип шифрування детальніше наведений при поясненнях до алгоритму роботи пристрою

3 РОЗРОБЛЕННЯ ПРИНЦИПОВОЇ ЕЛЕКТРИЧНОЇ СХЕМИ ПРИСТРОЮ

3.1 Вибір елементної бази

Для побудови пристрою захисту інформації необхідно вибрати серію мікросхем, на яких будуть розроблені схеми пристрою.

Аналізуючи умови та функціонал приладу підібрані такі мікросхеми:

─ мікроконтролер – КР1816ВЕ51;

─ буферний регістр– KR580ИР82;

─ логічного елемента 2І-НЕ – 564ЛА10;

─ пам’ять постійного зберігання – КР573РФ2.

─ пам’ять з довільним зберіганням – КР537РУ10;

─програмований контролер паралельного вводу-виводу–КР580ВВ55;

─ перетворювач сигналу – MAX232.

3.2 Мікроконтролер – КР1816ВЕ51

Однокристальный мікроконтролер КР1816ВЕ51 (МР51) виконаний в корпусі ВІС на основі високорівневої n-МОП технології, що дозволяє одержати вищий ступінь інтеграції в порівнянні з біполярними структурами. Корпус ВІС має 40 зовнішніх виводів. Цокольовка корпусу і назва виводів приведені на рисунку 3.1. Для роботи потрібне одне джерело живлення +5В. Через чотири програмовані порти вводу-виводу МК51 взаємодіє з середовищем в стандарті ТТЛ-схем з трьома станами входу.

Корпус МК51 має два виводи для підключення кварцевого резонатора, чотири виводи для сигналів, що управляють режимом роботи МК, і 8 ліній порту 3, які можуть бути запрограмовані користувачем на виконання спеціалізованих (альтернативних) функцій обміну інформацією з середовищем.

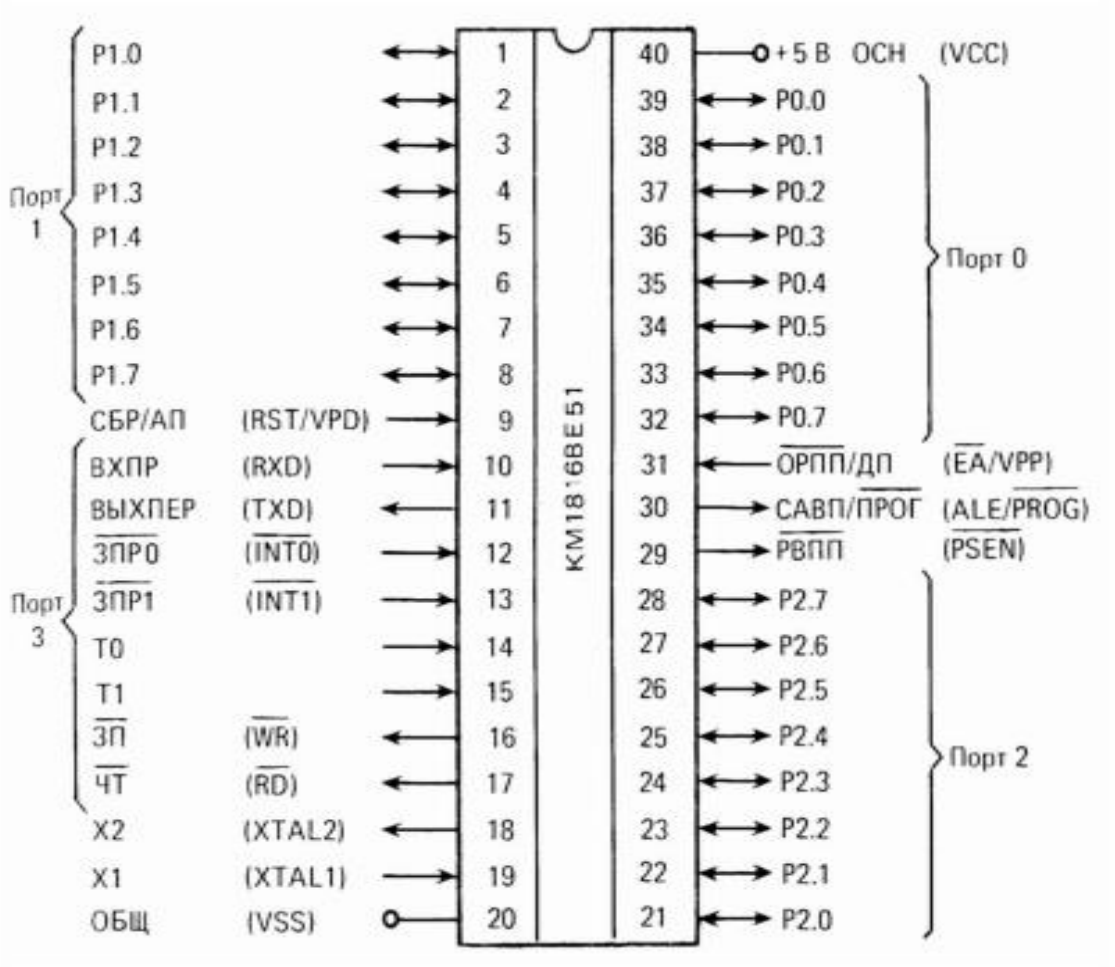

Рисунок 3.1 – Корпус мікросхеми МК51 і найменування виводів

Назва виводів і значення вхідних і вихідних рівнів приводяться нижче:

ТТЛ: Uin ≥ 2,0В Uil ≤ 0,8 В – вхідні рівні;

Uoh ≥ 2,4В Uol ≤ 0,4В – вихідні рівні;

СБР (RST) – керуючий сигнал скидання;

ВхПр(RxD) вхід приймача універсального приймача-передавача (УАПП);

ВихПер(TxD) – вихід передавача УАПП;

ЗПр(INT) – запит переривання;

Т0,Т1– таймер/лічильник подій;

Х1, Х2 – входи кварцевого резонатора;

ЗП(WR) – керуючий сигнал запису;

ЧТ(RD) – керуючий сигнал читання;

ОРПП(EA) – керуючий сигнал відключення резидентної пам'яті програм;

САВП(ALE) – керуючий сигнал скидання адреси зовнішньої пам'яті;

ПРОГ(PROG) – керуючий сигнал програмування РПП;

ДЗПП(PSEN) – дозволи зовнішньої пам'яті програм;

ОБЩ(VSS) – потенціал землі;

+5В(VCC) – напруга живлення

+5В; X1(XTAL1) – вхід для підключення виведення кварцевого резонатора або вхід для сигналу від зовнішньої початкової сигналізації;

X2(XAL2) вхід для підключення другого виводу резонатора.

Основу складає внутрішня двонаправлена 8-бітова шина, яка зв'язує між собою осоновні вузли і пристрої.

До них відносяться:

- 8-розрядний центральний процесор (ЦП) (включає АЛУ, акумулятор з розширювачем, регістр слова стану, блок регістрів спеціальних функцій, пристрій управління і синхронізації), розміщені на кристалі (всередині);
- пам'ять програм – ПЗП місткістю 4 кбайта і пам'ять даних – ОЗП місткістю 128 байт, які складають резидентну пам'ять;
- 32 лінії чотирьох паралельних портів (P0, P1, P2, P3) вводу- виводу (ВВ);
- канал послідовного порту ВВ;
- два 16-розрядні таймери/лічильники і логіку дворівневої системи переривань з п'ятьма або шістьма джерелами запитів.

Всі ці засоби утворюють резидентну частину МК, розміщену безпосередньо на кристалі. Окрім цього, є можливість реалізувати поза кристалом пам'ять програм і пам'ять даних до 64 кбайт кожну, шляхом підключення зовнішніх ВІС. Для скорочення ширини фізичного інтерфейсу більшість логічних ліній поєднуються. Так, при зверненнях до зовнішньої пам'яті порт P0 виконує роль суміщеної шини адреси даних, а P2–шини старшої частини адреси. Всі лінії порту P3 можуть виконувати альтернативні функції ліній управління [4].

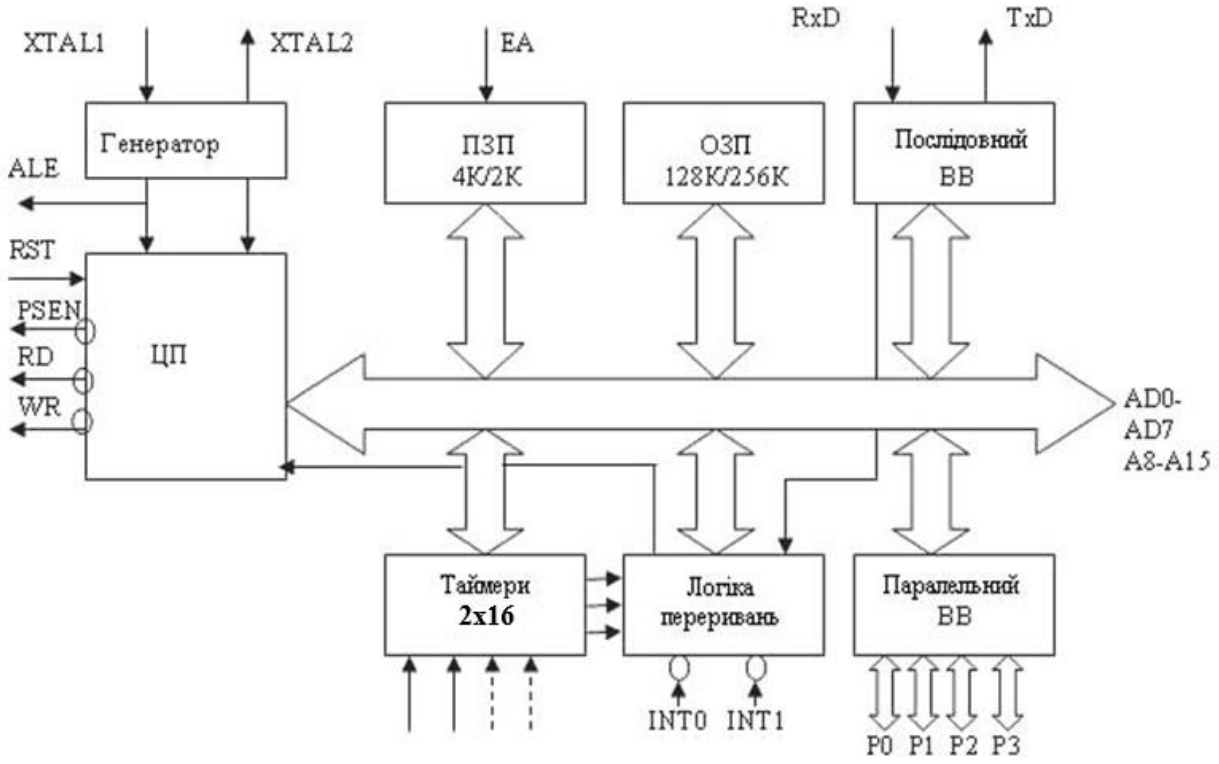

Рисунок 3.2 – Узагальнена структурна схема МК51

У архітектурі МК51 використаний принцип незалежності середовищ для зберігання програм і даних, тобто принцип Гарвардської архітектури.

Резидентна пам'ять. Пам'ять програм і пам'ять даних, розміщені на кристалі ВЕ51, фізично і логічно розділені, мають різні механізми адресації, працюють під управлінням різних сигналів і виконують різні функції.

Пам'ять програм (ПЗП або СППЗУ) має місткість 4Кбайта і призначена для зберігання команд, констант, слів ініціалізації, таблиць перекодування вхідних змінних і т.п., керована РПП має 16-бітову шину адреси, через яку забезпечується доступ з лічильника команд або з регістра покажчика даних (РПД).

Пам'ять даних (ОЗП) призначена для зберігання змінних в процесі виконання прикладної програми, адресується одним байтом і має місткість 128 байт. До адресного простору РПД примикають адреси регістрів спеціальних функцій (РСФ), РПП, РПД. Організація

доступу до них представлена на рис. 5.3. Набір програмно доступних регістрів приведений на рис. 5.4. Оскільки структура відноситься до класу акумуляторних, з банками перемикачів робочих регістрів, то центральним регістром набору вважається акумулятор.

Акумулятор А – 8-розрядний регістр, виконує звичайні функції основного арифметичного регістра, є джерелом операнда і приймачем (місцем фіксації) результату арифметичних і логічних операцій, а також ряду операцій передачі даних. Тільки з використанням акумулятора можуть бути виконані операції зсуву, перевірки на нуль, з прапором паритету і ін.

Регістр В – 8-розрядний, служить розширенням акумулятора А, необхідний для здійснення операцій множення і ділення, де виступає як джерело і приймач операндів. У всіх інших операціях регістр В виконує функції, які визначені користувачем. При скиданні А і В встановлюють в нуль.

Контролер МК51 може виконувати безліч команд без участі акумулятора. Дані можуть бути передані з будь-якої комірки РПД в будь-який регістр, останній може бути завантажений безпосередньо операндом і т.д.

3.3 Буферний регістр– KR580ИР82

Введення та виведення інформації виконується за допомогою портів введення/виведення, які являють собою 8- або 16-розрядні регістри зі схемами вибирання та керування читанням/записуванням. Використання регістра КР580ИР82 для з’єднання з пристроєм введення та пристроєм виведення показано на рисунку 3.3. Якщо регістр використовується як порт введення, то дані від пристрою введення надходять у регістр по лініях DI7-DI0 і записуються за стробом STB. Вихідні дані DO7-DO0 порту надходять у МПС по шині даних. Мікропроцесор формує також сигнал керування читанням і вибиранням порту, який надходить на вхід OE .

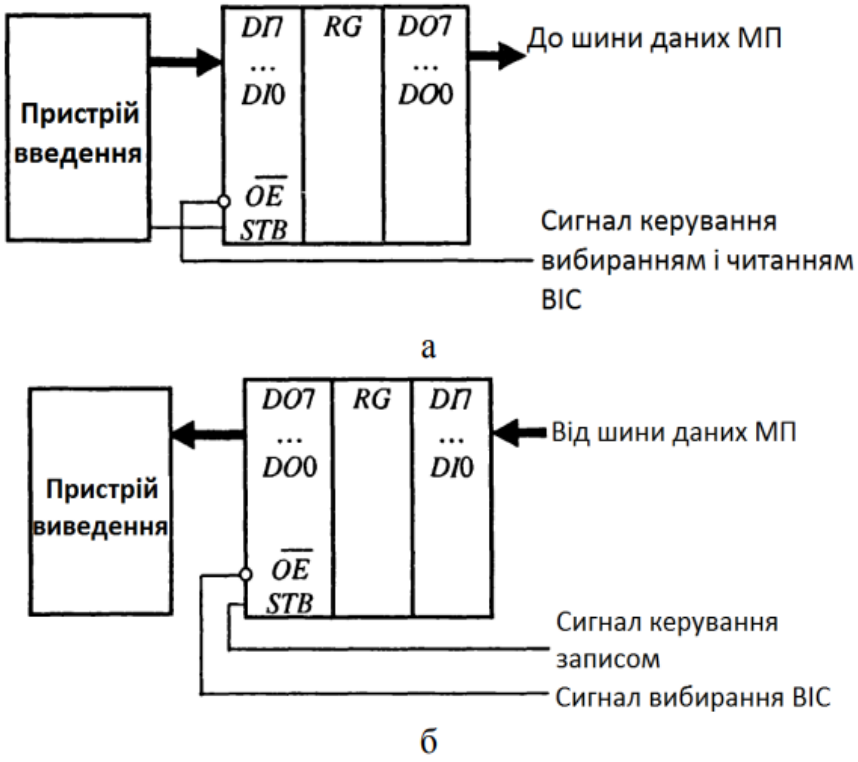

Рисунок 3.3 – Використання регістра КР580ИР82 для з’єднання:
а – з пристроєм введення;
б – з пристроєм виведення

Якщо регістр використовується як порт виведення, то дані від МП надходять по шині даних на входи DI7-DI0 порту і супроводжуються сигналами керування записуванням і вибиранням ВІС. Вихідні дані D07-DO0 порту надходять у пристрій виведення. Введення або виведення даних можна здійснювати двома способами:

- з використанням окремого адресного простору ПВВ;
- з використанням спільного з пам’яттю адресного простору, тобто з відображенням на пам’ять [6].

3.4 Пам’ять постійного зберігання – КР573РФ2

Мікросхема КР573РФ2 є перепрограмованим постійним пристроєм, що запам'ятовує, зі стиранням інформації ультрафіолетовим випромінюванням

ємністю 2048 байт. Умовно графічне зображення мікросхеми наведено рисунку 3.4.

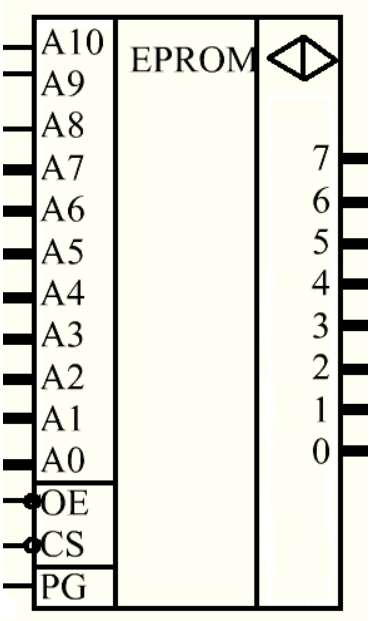

Рисунок 3.4 - КР573РФ2

Дані з пам'яті ячейки, адреса якої присутня на адресних входах протягом всього циклу, зчитуються при подачі сигналів нульового рівня на вхід вибору кристала CS і вхід дозволу виходу CEO.

3.5 Пам’ять з довільним зберіганням – КР537РУ10

Мікросхема КР537РУ10 є оперативним запам'ятовуючим пристроєм статичного типу, виготовленим за КМОП технологією. Умовно графічне зображення мікросхеми наведено на рисунку 3.5.

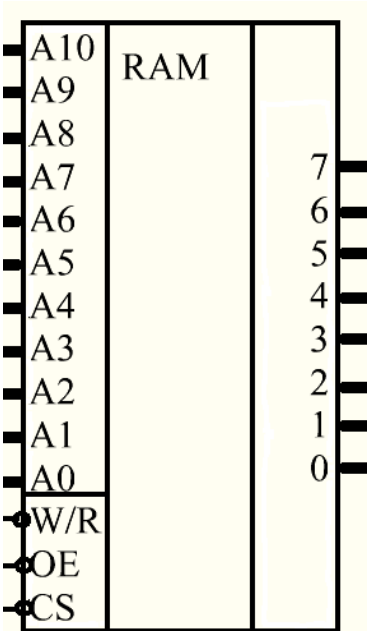

Рисунок 3.5 - КР537РУ10

Інформаційна ємність мікросхеми 2048×8 біт. На адресні входи подається код повної адреси необхідної пам'ятної комірки (а не окремі адреси рядка і стовпця як у попередньому випадку) і утримується протягом усього циклу. Вхід CS є входом вибору кристала. Мікросхема здійснює цикл запису чи читання лише за нульовому рівні сигналу цьому вході. Вхід OE є входом роздільної здатності виходу. При подачі на цей вхід сигналу нульового рівня виходи даних мікросхеми виходять з високоімпедансного стану і на них з'являються дані із осередку, адреса якої в даний момент присутня на адресних входах. Запис даних у мікросхему здійснюється за позитивним перепадом сигналу на вході WR/RD при одиничному рівні сигналу на вході OE та нульовому – на вході CS [7].

3.6 Програмований контролер паралельного вводу-виводу – КР580ВВ55

Програмований контролер паралельного вводу-виводу КР580ВВ55 призначений для введення-виведення паралельної інформації у 8-байтовому форматі, що дозволяє реалізувати більшість відомих протоколів обміну по паралельних каналах. Може використовуватись для з’єднання МП зі стандартним периферійним устаткуванням (дисплеєм, телетайпом,

накопичувачем, тощо). Структурну схему ВІС КР580ВВ55 показано на рисунку 3.6.

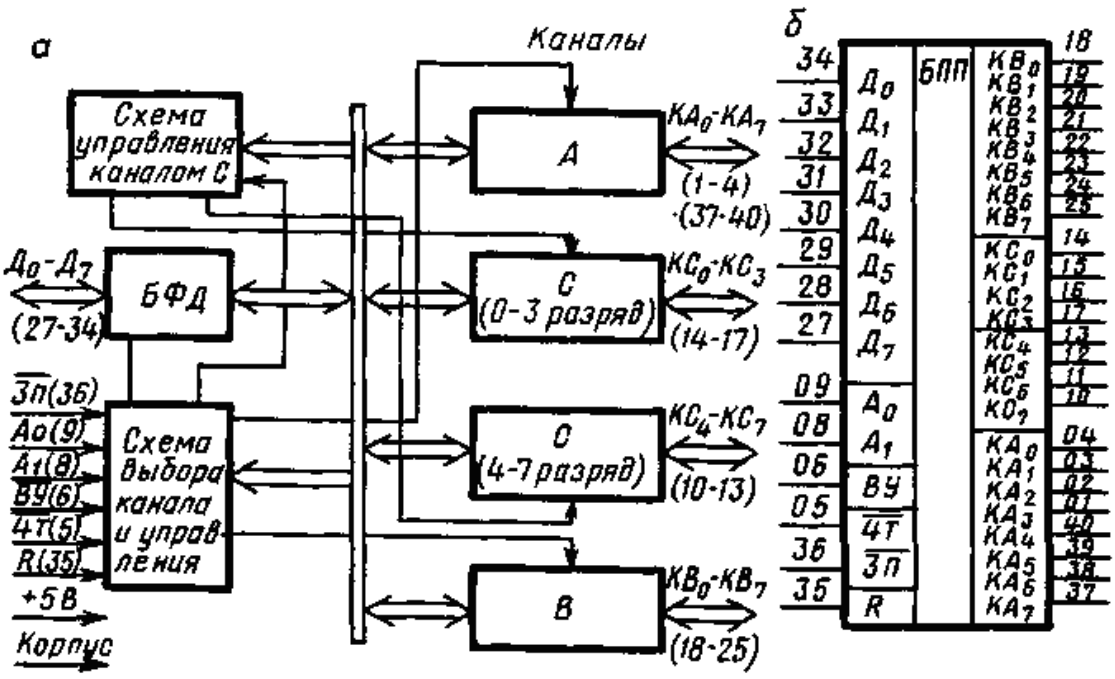

Рисунок 3.6 - Спрощена схема програмованого паралельного інтерфейсу КР580ВВ55 (а) та його умовне позначення (б)

До складу контролера входять:

- блок керування читанням/записом ReadlWrite Control Unit (RWCU), що забезпечує керування зовнішнім і внутрішнім передаванням даних і керувальних слів;
- двонапрямлений 8-розрядний буфер даних Bufer of Data(BD), що з'єднує лінії даних ВІС із системною шиною даних;
- три 8-розрядні порти введення-виведення (Port A, Port B, Port C) для обміну інформацією, при чому порт С поділений на два 4-розрядні: С' (РС7-РС4) і С"(РС3-РС0). Порти А і С' об'єднані у групу А, порти В і С" – у групу В.

Схема ВІС містить також блоки керування групою А Control Unit A (CUA) та групою В (CUB), що формують сигнали керування для відповідних груп.

Блок RWCU містить регістр керувального слова, який зберігає керувальні слова, що надходять від МП.

Призначення виводів ВІС КР580ВВ55:

─D7-D0 – вхід/вихід даних;

─RD – читання: L-рівень сигналу дозволяє зчитуванняінформації з регістра, що адресується розрядам A0, A1 на лінії D7-D0;

─WR – запис: L-рівень сигналу дозволяє запис інформації із шини D7-D0 у порт паралельного інтерфейсу, що адресується розрядам A0, A1;

─ A0, A1 – входи для адресування внутрішніх регістрів ППІ;

─RESET – скидання: H-рівень сигналу скидає регістр керувального слова і встановлює всі порти в режим уведення;

─CS – вхід вибірки мікросхеми: L-рівень сигналу з'єднує шину даних D7- D0 ВІС із системною шиною;

─PA7-PA0 – вхід/вихід порту A;

─PB7-PB0 – вхід/вихід порту B;

─PC7-PC0 – вхід/вихід порту C;

─Ucc – вивід напруги живлення +5 В;

─GND – спільний вивід 0 В.

3.7 Розробка програмного забезпечення для контролера КР580ВВ55

Одним из головних елементів схеми є контролер паралельного вводу-виводу–КР580ВВ55 яка може адресувати сигнал із шини даних на три зовнішні об'єкти за допомогою трьох 8-розрядних каналів даних (PortA, PortB, PortC), які можуть працювати як на вхід, так і на вихід. Ось приклад програми на асемблері для роботи з контролером. У цій програмі реалізоване читання входів, перевірка стану певного біта та установка певного виводу залежно від результату.

```
ORG 100H   ; Початкова адреса програми

START:
  MOV AL, 80H  ; Встановлюємо біт введення/виведення (IN/OUT)
```

```
    OUT 80H, AL  ; Записуємо в регістр даних

    MOV AL, 0FFH  ; Встановлюємо всі виводи в стан "1"
    OUT 81H, AL  ; Записуємо в регістр виводів

LOOP:
    IN AL, 82H  ; Зчитуємо стан входів
    MOV DL, AL  ; Зберігаємо зчитане значення в регістрі DL

    ; Перевіряємо стан нульового біту в регістрі DL
    TEST DL, 01H  ; Перевіряємо біт 0
    JZ SET_OUTPUT  ; Якщо біт 0 дорівнює 0 (стан низького рівня), переходимо до установки певного виводу
    JMP LOOP  ; Якщо біт 0 дорівнює 1 (стан високого рівня), продовжуємо цикл

SET_OUTPUT:
    MOV AL, 7FH  ; Встановлюємо біт 7 в "0", інші біти залишаються "1"
    OUT 81H, AL  ; Записуємо в регістр виводів

    ; Далі проводяться операції з установкою певного виводу

    JMP LOOP  ; Повертаємося до початку циклу

END  ; Кінець програми
```

Ця програма зчитує стан входів та перевіряє стан нульового біту в регістрі DL. Якщо нульовий біт дорівнює 0 (стан низького рівня), програма переходить до установки певного виводу та виконує відповідні операції. Якщо нульовий біт дорівнює 1 (стан високого рівня), програма продовжує цикл та повторює процес.

ВИСНОВКИ

Метою данного проекту був пристрій захисту інформації.

Причиною стала проблема захисту конфіденціальної інформації в наш час и необхідність надійних методів захисту.

Була проведенна аналітична робота, завдяки якій були визначенні основні плюси та мінуси різних типів шифрування інформації.

На основні аналізу був обранний метод книжкового гамування завдяки високій криптостійкості.

Розробленно алгоритм функціонування пристрою, структурна схеми.

Для розроблення електричної принципової схеми оптимальним для розроблюваного проекту буде мікроконтролер КР1816ВЕ51 завдяки низькій вартості, доступності, універсальності та зручності використання.

СПИСОК ЛІТЕРАЛУРИ

1. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. Київ, 2020. – 78с.
2. Шифрування: типи і алгоритми. URL:https://hostpro.ua/wiki/ua/security/encryption-types-algorithms (дата звернення: 16.07.2020).
3. Гапак О. М. Захист інформації в комп'ютерних системах: підручник. Ужгород, 2021. – 86с.
4. Касянчук М. М., Якименко І. З., Свистун М. Ю. Фінанси : навч. посіб. Тернопіль – 2020 – 7с.
5. Грищук Ю.С. Мікропроцесорні пристрої: Навчальний посібник. – Харків: НТУ "ХПІ", 2007.– 280с.
6. Огородник К. В., Книш Б. П.. Мікропроцесорна техніка : навчальний посібник – Вінниця : ВНТУ, 2018. – 106 с.
7. Принципова схема. URL:https://studfile.net/preview/10041830/page:2/ (дата звернення: 24.11.2019).
8. Вибір додаткових елементів схеми URL:https://studfile.net/preview/7052480/page:5/ дата звернення: 31.10.2018).
9. Бирин О.О. Захист інформації на базі методу книжкового гамування в інфокомунікаційних системах / Бережна О.В., Борисенко О.А., Горішняк А.О., Савченко Д.С.,// Фізика, електроніка, електротехніка (ФЕЕ-2022). Матеріали та програма науково-технічної конференції. – Суми: СумДу, 2023. – С.73.