МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра електроніки і комп'ютерної техніки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра на тему:

«Розподілена автоматизована система з використанням пристрою шифрування методом Віженера»

Завідувач кафедри: А. С. Опанасюк

Керівник
кваліфікаційної роботи: О. В. Бережна

Консультант
з техніко-економічної частини: О. М. Маценко

Виконав студент
гр. ЕС.м-91: О. О. Сальніков

Суми 2020 р.

Сумський державний університет
Кафедра_«Електроніки і комп'ютерної техніки»
Спеціальність 8.171.00.10 «Електроніка»
Освітня програма „Електронні системи та компоненти"

Затверджую:
Зав.кафедрою ЕКТ
Опанасюк А.С.
„____"____ 2020 г.

ЗАВДАННЯ

до випускної кваліфікаційної роботи магістра

Сальнікову Олександру Олександровичу

Тема роботи : **«Розподілена автоматизована система з використанням пристрою шифрування методом Віженера»**

затверджена наказом від «06» листопада 2020 р. № 1731-III

Термін виконання роботи: 15 .12. 2020 р.

Початкові дані до роботи: 1) реалізувати систему на базі мікроконтролера; 2) метод шифрування – Віженера; 3) первинний алфавіт розширити за рахунок спеціальних символів.

Зміст розрахунково-пояснювальної записки:

- огляд літератури та поставлення задачі проектування;
- наукова-дослідна частина
- вибір та обгрунтування алгоритму функціонування та структурної схеми системи;
- розробка функціональної схеми системи;
- вибір елементної бази та розробка принципових електричних схем блоків.

Перелік графічного матеріалу: креслення схеми алгоритму; креслення схеми електричної структурної; креслення схеми електричної функціональної; креслення схеми електричної принципової.

Консультанти по проекту (роботі), із зазначенням розділів проекту, що стосуються їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Економічна частина	Маценко О.М.		

Дата видачі завдання _____

Керівник _____ _____

Завдання прийняв до виконання _____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Огляд літератури та постановка задачі проектування	04.11.20-11.11.20	
2	Вибір та обґрунтування алгоритму функціонування та структурної схеми системи	12.11.20-16.11.20	
3	Науково-дослідна частина	17.11.20-25.11.20	
4	Розробка функціональної схеми блоків системи	26.11.20-01.12.20	
5	Вибір елементної бази та розробка принципових електричних схем блоків	02.12.20-14.12.20	
6	Економічна частина	15.12.20-18.12.20	

Студент-дипломник _____

Керівник проекту (роботи) _____

"___"_____2020 р.

РЕФЕРАТ

Пояснювальна записка містить: 89 аркушів, 37 рисунків, 20 таблиць, 14 джерел літератури.

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

Пояснювальна записка містить 7 розділів: огляд літератури, наукова частина, розробку алгоритму функціонування та структурну схему, розробку функціональної та принципової схем пристрою, розроблення кодового забезпечення та економічна частина.

Перший розділ містить загальну інформацію про захист конфіденційної інформації.

Другий розділ містить вибір і обґрунтування варіанта побудови системи чи пристрою, наукова новизна

Третій розділ присвячений розробці алгоритму функціонування та структурної схеми проектованої системи за допомогою пристрою шифрування методом Віженера.

Четвертий розділ присвячений розробці функціональної схеми пристрою.

П’ятий розділ присвячений розробленню принципової електричної схеми.

Шостий розділ містить програмне забезпечення для мікропроцесору.

Сьомий розділ містить розрахування собівартіості та ціни проектованого пристрою.

ЗМІСТ

					ЕЛІТ 8.171.00.10.347ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Сальніков О.О.			Розподілена автоматизована система з використанням пристрою шифрування методом Віженера Пояснювальна записка	Літ.	Арк.	Акрушів
Перевір.		Бережна О.В.					5	89
Реценз.						СумДУ; ЕСм-91		
Н. Контр.		Гапич В.Н.						
Затверд.		Опанасюк А.С.						

ВСТУП

Бурхливий розвиток інформаційних технологій в останні десятиріччя вимагає відповідного розвитку загальноосвітньої інформаційної культури. Захист інформації завжди був необхідним атрибутом інформаційних технологій, що означає, що її необхідно також вивчати – сучасний фахівець з комп'ютерних наук повинен бути знайомий з основами захисту інформації.

Захист інформації перетворюється сьогодні на одну з найактуальніших задач унаслідок надзвичайно широкого розповсюдження як власне різноманітних систем обробки інформації, так і розширення локальних та глобальних комп'ютерних мереж, якими передається величезний обсяг інформації державного, комерційного, приватного характеру.

Зрозуміло, що усю перелічену інформацію треба захищати. Принципи захисту повинні бути різними залежно від того, який тип інформації необхідно захищати. Якщо інформація, що підлягає захисту, належить до одного з класифікованих ступенів секретності, то основні зусилля системи захисту повинні бути зосереджені на захисті конфіденційності [1].

1.ОГЛЯД ЛІТЕРАТУРИ

1.1 Захист конфіденційної інформації: проблеми та шляхи вирішення

На сучасному етапі розвитку економіки і суспільства в цілому інформація, як об’єкт інтелектуальної власності компанії, стає все більш значущим інструментом на її шляху до комерційного успіху. Науково-технічні розробки, економічні та організаційні рішення, які невідомі третім особам, можуть надавати компанії конкурентні переваги і служити основним або додатковим джерелом прибутку. Останнім часом все частіше власники такої інформації почали усвідомлювати необхідність її захисту. У системі забезпечення безпеки підприємницької діяльності все більшого значення набуває комп’ютерна безпека. Це пов’язано із зростаючим об’ємом інформації, що поступає, вдосконаленням засобів її зберігання, передачі і обробки. Переведення значної частини інформації в електронну форму, використовування локальних та глобальних мереж створює якісно нові загрози конфіденційної інформації.

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. Проблема забезпечення інформаційної безпеки є на сьогодні однією з найгостріших не лише в Україні, але і в розвинених країнах світу. Досвід експлуатації інформаційних систем і ресурсів в різних сферах життєдіяльності показує, що існують різні і вельми реальні загрози втрати інформації, що приводять до матеріальних і інших збитків. При цьому забезпечити на 100 % безпеку інформації практично неможливо.

В Україні питання захисту інформації регулюються Цивільним, Господарським кодексами України. Закон України «Про інформацію» ввів поняття « інформація із обмеженим доступом». Ця інформація відповідно до закону поділяється на конфіденційну та таємну. Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб та розповсюджуються за їх бажанням відповідно з передбаченими ними умовами [2].

Чільне місце серед всього різноманіття засобів попередження несанкціонованого доступу до захищеної інформації посідають

криптографічні методи, оскільки вони ґрунтуються на властивостях інформації і не мають слабкостей, що виникають при використанні особливостей вузлів її обробки,середовища передачі, адміністративних засобів.

Криптографія - це наука, що вивчає математичні методи забезпечення автентичності і конфіденційності даних. Для сучасного етапу її розвитку характерним є використання алгоритмів, що припускають реалізацію за допомогою обчислювальних засобів. Основними вимогами до сучасних методів криптографічного захисту є: конфіденційність, цілісність і невідслідкованість. В сучасній криптографії практичне значення мають лише методи захисту з використанням ключа. Їх поділяють на два види: симетричні та асиметричні Симетричні системи шифрування базуються на одному ключі,що використовується і для шифрування, і для дешифрування або ключ дешифрування можливо обчислити за ключем шифрування. Їх перевагами є:

1. Велика пропускна здатність.
2. Відносно короткі ключі.
3. Їх можна використати як основу для створення різних криптографічних механізмів псевдовипадкові генератори чисел та обчислювально-ефективні схеми.
4. Можливість їх комбінування для підвищення криптостійкості.

1.2 Система захисту та засоби захисту конфіденційної інформації

Система захисту конфіденційної інформації показує собою пакет технологічних організаційних, технічних засобів та методів, які запобігають несанкціонованому доступу до конфіденційної інформації. Власник певної конфіденційної інформації особисто визначає зміст цінної інформації, яка потребує захисту, та відповідні способи та засоби захисту. Система захисту конфіденційної інформації зобов’язана бути багаторівневою з ієрархічним доступом до даної інформації, гранично конкретизованою і прив'язаною до специфіки фірми по структурі методів та засобів захисту, що використовуються, відкритою для оновлення, надійною як в звичайних, так і в різних екстремальних ситуаціях. Вона не повинна створювати співробітникам фірми серйозні незручності в роботі [3].

Безпека конфіденційної інформації є одним з важливих напрямків комунікаційного менеджменту. Під цим розуміється несанкціонований вихід відомостей інформації за межі кола осіб.

Комплексність системи безпеки досягнутий за рахунок формування з різних елементів:

-технічних

-програмно-математичних

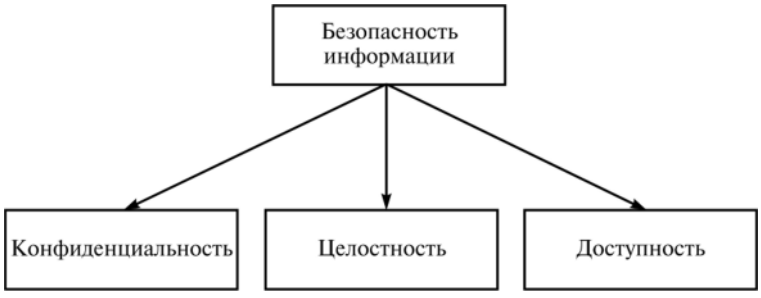
-організаційних.

Ступінь цінності конфіденційної інформації та необхідна надійність її безпеки знаходяться в прямій залежності, та співвідношення елементів їх змісту забезпечують індивідуальність системи безпеки конфіденційної інформації фірми і гарантують її трудність подолання. Співвідношення частин системи, їх склад та взаємозв'язок відображають, індивідуальність та конкретний заданий рівень безпеки з врахуванням цінності конфіденційної інформації. Елемент правової безпеки конфіденційної інформації та елемент організаційної безпеки інформації містить міри управлінського та обмежувального характеру і передбачає:

-регламентацію і регулярне оновлення переліку цінної, конфіденційної інформації, яка підлягає захисту, складання і ведення переліку конфіденційних документів фірми;

-регламентацію технології захисту та обробки конфіденційних документів фірми;

Принципи захисту інформації залежить від того, який тип інформації ми захищатимемо. Якщо інформація, що підлягає захисту, належить до одного з класифікованих ступенів секретності, то основні зусилля системи захисту повинні бути спрямовані на захист конфіденційності.



Цілісність інформації - це здатність інформації (вимога до інформації) зберігати незмінним семантичний зміст (по відношенню до вихідних даних), тобто її стійкість до випадкового або навмисного спотворення або руйнування.

Доступність інформації - це здатність (вимога) об'єкта - інформаційної системи (мережі) - забезпечувати своєчасний безперешкодний доступ авторизованих суб'єктів (користувачів, абонентів) до цікавить їх або здійснювати своєчасний інформаційний обмін між ними.

Суб'єкт - це активний компонент системи, який може стати причиною утворення потоку інформації від об'єкта до суб'єкта або зміни стану системи. Об'єкт - пасивний компонент системи, що обробляє, зберігає, приймає або передає інформацію. Доступ до об'єкту означає доступ до міститься в ньому інформації.

Підкреслимо, що доступ до інформації - можливість отримання і використання інформації, тобто можливість її прийому, ознайомлення з інформацією, обробки, зокрема, копіювання, модифікації або знищення інформації [4].

1.3 Шифрування за допомогою шифру Віженера

Перший документований опис багатоалфавітного шифру було сформульовано Леоном Батіста Альберті в 1467 році, для перемикання між алфавітами використовувався металевий шифрувальний диск. Система Альберті перемикає алфавіти після декількох зашифрованих слів. Пізніше, в 1518 році, Йоганн Трисемуса в своїй роботі "Поліграфія" винайшов центральний компонент шифру Віженера.

Те, що зараз відомо під шифром Віженера, вперше описав Джованні Батіста Беллаз. Він використовував ідею Трисемуса, але додав ключ для перемикання алфавітів шифру через кожну букву.

Шифр Віженера мав репутацію виключно стійкого до злому. Шифр Віженера досить простий для використання в польових умовах, особливо якщо застосовуються шифрувальні диски [5].

Процес шифрування:

Шифр Віженера є багатоалфавітних систему шифрування. Він є

симетричним блоковим шифром заміни.

Будемо вважати, що вихідний текст являє собою рядок

$$S = (x_1, x_2, \ldots, x_L)$$

утворену символами алфавіту

$$A = (a_1, a_2, \ldots, a_N)$$

Довжина тексту - L символів.

При шифруванні тексту використовується секретний ключ - символьний рядок довжиною:

$$K = (k_1, k_2, \ldots, k_l)$$

Чим більше довжина ключового слова, тим складніше зламати шифр, а, значить, тим надійніше захищений текст.

Для шифрування використовується таблиця Віженер, який будується в такий спосіб: зверху і по лівому краю квадрата виписується вихідний алфавіт. У перший рядок квадрата заноситься перестановка з букв алфавіту.

У другому рядку та ж перестановка циклічно зсувається на одну позицію вліво, в третій - на дві. Таким чином, квадрат складається з N перестановок, і кожної з них відповідає та буква вихідного алфавіту, яка записана зліва від неї

У 1518 році в розвитку криптографії був зроблений новий крок завдяки появі в Німеччині першої друкованої книги по криптографії. Система шифрування наступна: перша буква вихідного тексту шифрується по першому рядку, друга по другий і так далі. Після використання останнього рядка наступна буква знову шифрується по першому рядку. У шифрі Трітемія відсутня ключ, секретом є сам спосіб шифрування.

Наступний крок у розвитку запропонованого Трітемія способу шифрування був зроблений італійцем Джовані Белазо. У цьому шифрі ключем є так званий пароль - фраза або слово. Пароль записувався періодично над

буквами відкритого тексту. Буква пароля, що стоїть над відповідною буквою відкритого тексту, вказувала номер рядка в таблиці Трітемія, по якій слід проводити заміну (шифрування) це літери.

В подальшому ідеї Трітемія і Белазо розвинув співвітчизник Белазо Джованні Батіста Порта. Він запропонував відмовитися від алфавітного порядку проходження букв в першому рядку таблиці Трітемія і замінити цей порядок на деякий довільний, який є ключем шифру. Рядки таблиці як і раніше циклічно зсувалися. Порта запропонував біграммний шифр, а також навів опис механічного дискового пристрою, що реалізує біграммную заміну.

Посол Франції в Римі Блез де Віженер, познайомившись з працями Трітемія, Белазо, Кардано, Порта, Альберті, також захопився криптографією. У 1585 році він написав «Трактат про шифри», в якому викладаються основи криптографії.

По суті справи Віженер об'єднав підходи Трітемія, Белазо, Порта до шифрування відкритих текстів, по суті не внісши в них нічого оригінального.

У наш час шифр Віженера, що складається в періодичному продовження ключового слова по таблиці Трітемія, витіснив імена його попередників.

Гілберт Вернам спробував поліпшити зламаний шифр він отримав назву шифр Вернама-Віженера в 1918 році, але, незважаючи на його вдосконалення, шифр так і залишився уразливим до криптоаналізу. Однак робота Вернама в кінцевому підсумку все ж привела до отримання шифру Вернама, який дійсно неможливо зламати [6].

1.4 Канал зв’язку

Канал зв’язку – це сукупність пристроїв і фізичних середовищ, які забезпечуютьпередачу повідомлень з одного місця в інше, або від одного моменту часу до іншого.

Основне завдання відправника- скласти повідомлення і використовувати канал для його передачі таким чином, щоб обидві сторони зрозуміли вихідну ідею. Це буде складно, так як на кожному етапі зміст повідомлення може бути пошкодженим або повністю втрачено.

Якщо канал використовується для передачі дискретних повідомлень, то він називається дискретним каналом, а якщо для передачі неперервних, то неперервними.

Структурна схема системи передачі інформації представлена на рисунку 1.1.

Рисунок 1.1- Структурна схема системи передачі інформації.

Цілі шифру:

-Конфіденційність.

Шифрування використовується для приховування інформації від неавторизованих користувачів при передачі або при зберіганні.

-Цілісність.

Шифрування використовується для запобігання зміни інформації при передачі або зберіганні.

-Ідентифікованість.

Шифрування використовується для аутентифікації джерела інформації та запобігання відмови відправника інформації від того факту, що дані були відправлені саме їм [7].

1.5 Методи проектування розподілених систем автоматизації

Огляд SCADA систем.

SCADA (Supervisory Control And Data Acquisition) – даний програмний пакет, використовується для забезпечення роботи систем обробки, сбору і відображення інформації управління. Розподілені системи спостереження та керування позначаються даним тнрміном. Системи SCADA використовуються для керування фізичними, хімічними або траспортними процесами і також для спостереження цих процесів.

Цей програмний пакет, розроблений для забезпечення роботи в реальному часі систем обробки, збору, архівування, відображення інформації про об'єкт управління або моніторингу. SCADA може бути частиною автоматизованої системи керування, наукового експерименту, системи екологічного моніторингу, автоматизації будівлі і т. д. SCADA-системи використовуються у майже всіх галузях господарства, які потребують забезпечення операторським контролем за технологічними процесами в реальному часі. Дане програмне забезпечення встановлюється на комп'ютери для зв'язку з об'єктом, завдяки використання драйверів введення-виведення або OPC / DDE сервери. Програмний код може бути як написаний на одній з мов програмування, так і згенерований в середовищі проектування.

Іноді SCADA-системи комплектуються додатковим програмним забезпеченням для програмування промислових контролерів. Такі SCADA-системи називаються інтегрованими і до них додається термін SoftLogic.

Термін «SCADA» має двояке тлумачення. Найбільш поширене розуміння SCADA як додатку, тобто даного програмного комплексу, що в даний час забезпечує виконання деяких зазначених функцій, а також інструментальних засобів для розробки програмного забезпечення. Часто під SCADA системою мають на увазі програмно-апаратний комплекс. Розуміння терміна SCADA характерно для розділу телеметрія [8].

Значення терміна SCADA набуло змін разом з розвитком управління технологічними процесами та технологій автоматизації. У 80 - ті роки під SCADA-системами найчастіше використовували програмно-апаратні комплекси збору даних. З 90 - х років термін SCADA використовується більше для позначення тільки програмної частини людино-машинного інтерфейсу автоматизованої системи управління.

SCADA-системи вирішують наступні завдання:

− логічне управління.

− здійснення мережевої взаємодії між SCADA ПК.

− забезпечення зв'язку з зовнішніми додатками.

− обробка інформації в реальному часі

− підготовка та генерування звітів про хід технологічного процесу.

− обмін даними з «пристроями зв'язку з об'єктом».

− відображення інформації на екрані монітора в зручній та зрозумілій для людини формі.

− аварійна сигналізація і управління тривожними повідомленнями.

− ведення бази даних реального часу з технологічною інформацією.

SCADA-системи дозволяють розробляти автоматизовану систему керування як автономні програми, а також в клієнт-серверної або в розподіленої архітектурі.

Термін SCADA відноситься до централізованих систем контролю та управління всією системою, або комплексами даних систем, здійснюваного за допомогою людини. Більша частина керуючих впливів виконується автоматично УСО (RTU) або ПЛК (PLC). Управління процесоми зазвичай забезпечується RTU або PLC, а SCADA забезпечує управління режимами роботи. Наведемо приклад, PLC може управляти потоком води, що виконує охолоджуючу дію всередині частини виробничого процесу, а SCADA система має змогу дозволити операторам змінювати маршрути руху рідини, змінювати уставки для даного потоку, заповнювати ті або інші ємності, а також має змогу стежити за тривожними 20 повідомленнями, такими як – висока температура, втрата потоку, які повинні бути записані та відображені, і на які оператор повинен заздалегідь відреагувати. Цикл управління зі зворотним зв'язком проходить через PLC або RTU, в той час як SCADA система виконує контроль для повного виконання циклу [9].

Збір даних виконується в RTU або на рівні PLC та включає свідчення вимірювального приладу. Після чого, дані збираються та форматуються таким способом, щоб оператор диспетчерської, використовуючи HMI, мав змогу прийняти контролюючі рішення – перервати стандартне управління коштами RTU / PLC або його коригувати. Дані можуть бути записані в архів для створення трендів та іншої аналітичної обробки деяких накопичених даних.

У 90-х роках з'явилися системи SCADA, что працюють в середовіщі Windows. Найвідоміші пакети Genesis 32 («Iconics», USA), Factory Suite («Wonder-ware», USA), Modicon Factory Link («US Data», USA), Genie («Advantech», USA), Cimplicity HMI («GE Fanuc Automation», Японія), WinCC («Siemens AG», Німеччина). У 2014 році українська компанія «НІК» представила свою інноваційну розробку – HMI / SCADA систему «PowerSyS». Такі системи забезпечують: наочно інформацію про Хід виробництва, відображення стану приводів і технологічного устаткування, деталізацію вибраних диспетчером частин процеса, створення архіву аварій, подій і поведінки процесу в часі, захист від недозволеного доступу до збору інформації і управління, розпізнавання передаварійних і аналіз аварійних ситуацій з рекомендаціями послідовності дій диспетчера, розрахунок показників процеса в динаміці і виведення узагальненої інформації у вигляді графіків, таблиць або малюнків, можливість управління виконавчими пристроями об'єкта з пульта диспетчера.

Основні завдання, для SCADA-систем.

SCADA-система зазвичай повинна містить наступні підсистеми:

- програма, що забезпечує обробку даних в межах заданого тимчасового циклу з урахуванням пріоритетів.

− драйвери або сервери введення-виведення

− система реального часу

– програма, що забезпечує автоматичний контроль технологічних подій, віднесення їх до категорії нормальних, що попереджають або аварійних, а також обробку подій оператором або комп'ютером.

- програми, що забезпечують зв'язок SCADA з промисловими контролерами, лічильниками, АЦП і іншими пристроями введення-виведення інформації.

−система управління тривогами

− програма-редактор для розробки людино-машинного інтерфейсу.

− зовнішні інтерфейси - стандартні інтерфейси обміну даними між SCADA та іншими додатками. Зазвичай ODBC DDE OPC, DLL.

− людино-машинний інтерфейс – інструмент, який представляє дані про хід процесу людині оператору, який дозволяє оператору мати змогу контролювати процес та керувати ним.

− система логічного управління - програма, що забезпечує виконання призначених для користувача програм логічного управління в SCADA-системі.

− база даних реального часу - програма, що забезпечує збереження історії процесу в режимі реального часу.

− генератор звітів – програма, що забезпечує створення призначених для користувача звітів про технологічні події. Набір редакторів для їх розробки.

Архітектура SCADA-систем

Зважаючи на вимоги до надійності та складність керованого технологічного процесу, SCADA-системи будуються по одній з наступних архітектур:

Автономні. При даному використанні такої архітектури система складається з однієї або декількох робочих станцій оператора, що не залежать один від одного. Всі функції цієї системи виконуються на єдиній станції.

Переваги даної архітектури:

− простота у використанні.

Недоліки:

− не забезпечується істинність даних (історичні дані можуть відрізнятися між різними станціями).

− низька відмовостійкість;

Клієнт-Серверні. В цьому випадку дана система виконується на сервері, а оператори системи використовують клієнтські станції для управління процесом та моніторингу. Високонадійні системи майже завжди будуються на базі подвійного або потрійного резервування серверів і виконується дублювання клієнтських станцій даного оператора, дублювання здійснюється

підключенням до мережі сервер-сервер і клієнт-сервер. При даній архітектурі вже виконується поділ функцій SCADA системи між серверами. Наприклад, збір даних і управління ПЛК виконується на одному сервері, а взаємодія з клієнтами – на другому, архівування даних – на третьому.

Розподілені. При використанні архітектури розподіленої системи управління дане обчислення здійснюються на декількох взаємопов'язаних обчислювальних пристроях, часто здійснюється з функцією взаємного резервування. Розподілені SCADA-системи з взаємним резервуванням відрізняються високою надійністю [10].

1.6 Постановка задачі

На підставі проведеного літературного огляду задачу проектування сформулюємо наступним чином.

Розробити автоматизовану систему з використанням пристрою захисту конфідеційної інформації за допомогою шифру Віженера.

Розроблювальний пристрій повинен забезпечувати захист інформації в автоматизованій системі керування. Для вирішення поставленого завдання під час дипломного проектування необхідно дослідити особливості шифрування методом Віженера, розробити і обґрунтувати алгоритм функціонування, структурну схему, схему електричну принципову, виконати розрахунок електричних вузлів і блоків пристрою.

2. НАУКОВА-ДОСЛІДНА ЧАСТИНА

2.1 Розподілена автоматизована система як об’єкт технічної інформації

Функціонування розподіленої автоматизованої системи пов’язано із застосуванням розподіленої системи передачі даних (СПД), яка використовує різні технології передачі даних з різним рівнем загроз щодо несанкціонованого доступу до інформації що передається цими каналами зв’язку.

Наведена розподілена автоматизована система призначена для здійснення управління та моніторінгу технологічних параметрів при транспортуванні та розподілу таких життєвоважливих для функціонування виробничої та суспільної інфраструктури транспортування та розподілу енергоресурсів, як вода, газ та електрична енергія. Стан технологічного об’єкту оцінюється за допомогою многофункціональних мікропроцесорних пристроїв таких як лічильники води та газу, лічильник електроенергії SL7000, многофункціональних вимірювачів ПЦ6806, контролери регістрації дискретних сигналів про стан технологічного обладнання (насоси, двигуни, вимикачі та інше).

Крім оцінювання технологічних параметрів процесу транспортування енергоресурсів (сила току, напруга, потужність, коефіцієнт потужності, кількість отриманої чи відданої електроенергії, води, газу) ці пристрої здійснюють керування технологічним обладнанням та мають можливість вмикати та вимикати насоси, двигуни та вимикачі або змінювати режими їх роботи.

Несанкціоноване керування цим технологічним обладнанням несе в себе загрози створення штучних аварійних ситуацій або створення перешкод при ліквідації аварійних ситуацій на об’єктах життєвоважливої інфраструктури. Основними каналами витоку важливої інформації та несанкціонованого втручання в роботу обладнання є канали Інтернет-сервер (АРМи) СПД-лічильник (контролер) та канал СПД-лічильник (контролер).

Многофункціональні мікропроцесорні пристрої інтегруються з верхнім рівнем через систему передачі даних за допомогою послідовних інтерфейсів типу RS485 та RS232, конверторів Ethernet\RS485\RS232, GSM\GPRS та xDSL модемів, комутаторів та маршрутизаторів мережі Ethernet.

Найбільш вразливими для криптоаналітичних атак є безпровідні канали зв’яку, що будуються на базі GSM\GPRS модемів, в які найпростіше додати різні хибні команди шляхом несанкціонованого додавання імітовставок, а найбільш ефективним місцем встановлення апаратних модулів технічного захисту інформації є кінцеві точки інформаційного тракту біля многофункціональних мікропроцесорних пристроїв (лічильників, контролерів та інше), які мають можливість керування технологічними об’єктами.

Застосування в модулях захисту інформації алгоритмів шифрування методом Віженера дозволить з мінімальними апаратними витратами побудувати ефективний технічний захист інформаційних трактів від несанціонованого втручання в роботу технологічного обладнання виробничої інфраструктури.

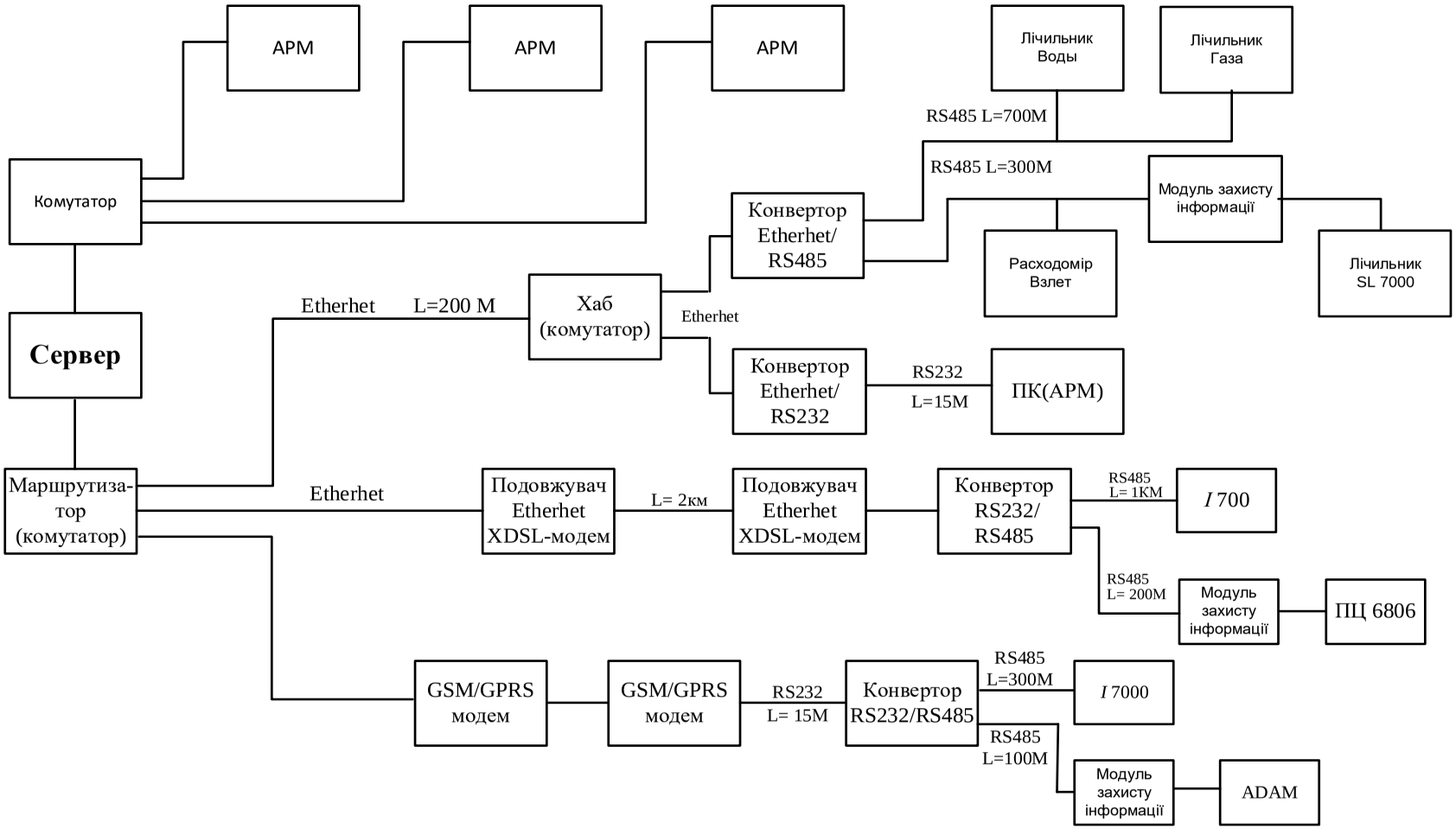


Рисунок 2.1 - Структурна схема телекомунікаційної системи

2.2. Вимоги до криптографічних систем

Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, однак їй властиві і переваги: висока продуктивність, простота, захищеність і т.д. Програмна реалізація більш практична, допускає відому гнучкість у використанні.

Незалежно від способу реалізації для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги:

- стійкість шифру протистояти криптоаналізу повинна бути такою, щоб розтин його міг бути здійснений тільки рішенням завдання повного перебору ключів, і має або виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості організації мережевих обчислень) або вимагати використання дорогих обчислювальних систем;

- криптостійкість забезпечується не секретністю алгоритму, а секретністю ключа (розділяє криптосистеми загального використання (алгоритм доступний потенційному порушнику) і обмеженого використання (алгоритм тримається в секреті));

- зашифроване повідомлення повинно піддаватися читанню тільки при наявності ключа;

- шифр повинен бути стійким навіть в разі, якщо порушнику відомо досить велика кількість вихідних даних і відповідних їм зашифрованих даних;

- незначна зміна ключа або вихідного тексту повинна приводити до істотної зміни виду зашифрованого тексту;

- структурні елементи алгоритму шифрування повинні бути незмінними;

- шифртекст не повинен значно перевищувати за обсягом вихідну інформацію; додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути повністю та надійно сховані в зашифрованому тексті;

- помилки, що виникають при шифруванні, не повинні призводити до спотворень і втрат інформації;

- не повинно бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;

- будь-який ключ з безлічі можливих повинен забезпечувати рівну криптостійкість (забезпечення лінійного (однорідного) простору ключів);

- час шифрування не повинен бути великим;

- вартість шифрування повинна бути узгоджена з вартістю закодованої інформації.

2.3. Криптостійкість і способи її оцінки

Знання деяких положень криптоаналізу необхідно для глибокого розуміння криптографії.

Головною дійовою особою в криптоаналізу виступає порушник (або криптоаналитик). Під ним розуміють особу (групу осіб), метою яких є прочитання або підробка захищених криптографічними методами повідомлень.

Відносно порушника приймається ряд припущень, які, як правило, кладуть в основу математичних чи інших моделей:

1. порушник знає алгоритм шифрування (або вироблення ЕЦП) і особливості його реалізації в конкретному випадку, але не знає секретного ключа.

2. порушнику доступні всі зашифровані тексти. Порушник може мати доступ до деяких вихідних текстів, для яких відомі відповідні їм зашифровані тексти.

3. порушник має в своєму розпорядженні обчислювальні, людські, часові та інші ресурси, обсяг яких виправданий потенційної цінністю інформації, яка буде здобута в результаті криптоаналізу.

Спробу прочитання або підробки зашифрованого повідомлення, обчислення ключа методами криптоаналізу називають кріптоатакою або атакою на шифр. Вдалу криптоатаку називають зломом.

Криптостійкістью називається характеристика шифру, що його стійкість до розшифрування без знання ключа (тобто криптоатаці).

Показник криптостійкості - головний параметр будь-якої криптосистеми. Як показник криптостійкості можна вибрати:

- кількість всіх можливих ключів або ймовірність підбору ключа за заданий час із заданими ресурсами;

- кількість операцій або час (з заданими ресурсами), необхідне для злому шифру із заданою вірогідністю;

- вартість обчислення ключової інформації або вихідного тексту.

Всі ці показники повинні враховувати також рівень можливої криптоатаки.

Однак слід розуміти, що ефективність захисту інформації криптографічними методами залежить не тільки від криптостійкості шифру, але і від безлічі інших чинників, включаючи питання реалізації криптосистем у вигляді пристроїв або програм. При аналізі криптостійкості шифру необхідно враховувати і людський фактор. Наприклад, підкуп конкретної людини, в руках якого зосереджена необхідна інформація, може коштувати на кілька порядків дешевше, ніж створення суперкомп'ютера для злому шифру.

Сучасний криптоаналіз спирається на такі математичні науки як теорія ймовірностей і математична статистика, алгебра, теорія чисел, теорія алгоритмів і ряд інших. Всі методи криптоаналізу в цілому укладаються в чотири напрямки.

1. статистичний криптоаналіз - досліджує можливості злому криптосистем на основі вивчення статистичних закономірностей вихідних і зашифрованих повідомлень. Його застосування ускладнене тим, що в реальних криптосистемах інформація перед шифруванням піддається стиску (перетворюючи вихідний текст в випадкову послідовність символів), або в разі гамування використовуються псевдовипадкові послідовності великої довжини.

2. алгебраїчний криптоаналіз - займається пошуком математично слабких ланок криптоалгоритмів. Наприклад, в 1997 р в еліптичних системах було виявлено клас ключів, що істотно спрощує криптоаналіз.

3. диференціальний (або різницевий) криптоаналіз - заснований на аналізі залежності зміни шифрованого тексту від зміни початкового тексту. Вперше використаний Мерфі, поліпшений Біхемом і Шамір для атаки на DES.

4. лінійний криптоаналіз - метод, заснований на пошуку лінійної апроксимації між вихідним і шифрованим текстом. Як і диференційний аналіз в реальних криптосистемах може бути застосований лише для аналізу окремих блоків криптоперетворень.

Досвід зломів криптосистем показує, що головним методом залишається "лобова" атака - проба на ключ. Також як показує досвід криптосистеми більше страждають від недбалості в реалізації.

Прийнято розрізняти кілька рівнів криптоатаки в залежності від обсягу інформації, доступної криптоаналітикам. Можна виділити три рівні криптоатаки по наростанню складності.

1. атака по шифрованому тексту (Рівень КА1) - порушнику доступні всі або деякі зашифровані повідомлення.

2. атака по парі "вихідний текст - шифрований текст" (Рівень КА2) - порушнику доступні всі або деякі зашифровані повідомлення та відповідні їм вихідні повідомлення.

3. атака за обраним парі "вихідний текст - шифрований текст" (Рівень КА3) - порушник має можливість вибирати вихідний текст, отримувати для нього зашифрований текст і на основі аналізу залежностей між ними обчислювати ключ.

Всі сучасні криптосистеми володіють достатньою стійкістю навіть до атак рівня КА3, тобто коли порушнику є по суті шифрувальний пристрій.

На сучасному етапі розвитку науки і техніки захист інформації перетворюється на одну з найактуальніших задач внаслідок надзвичайно широкого розповсюдження як автоматизованих систем обробки інформації, так і розширення локальних та глобальних комп'ютерних мереж, якими передаються величезні об'єми інформації.

2.4 Концепція захисту інформації

Вразливість інформації в автоматизованих комплексах обумовлена великою концентрацією обчислювальних ресурсів, довгостроковим збереженням великого об'єму даних на магнітних та оптичних носіях, їх територіальною розподіленністю, одночасним доступом до ресурсів багатьох користувачів. У цих умовах необхідність методів захисту, напевно, не викликає сумнівів. Але існують деякі труднощі:

- для забезпечення надійного захисту необхідно розв'язати цілий комплекс технічних і організаційних проблем і розробити відповідну документацію.
- виробники засобів захисту, в основному, пропонують окремі компоненти для рішення приватних задач, залишаючи питання формування системи захисту і сумісності цих засобів на розсуд споживачів;
- немає єдиної теорії захисту систем;

для виконання перерахованих вище труднощів, необхідна координація;

- дій всіх учасників даного інформаційного процесу на підприємстві, та на державному рівні.

Концепція захисту інформації - проблеми інформаційної безпеки та шляхи її рішення з урахуванням всих сучасних тенденцій. Вона є методологічною основою якої є політика розробки практичних заходів для її реалізації. На базі сформульованих задач, заданих цілей і можливих шляхів їх рішення формуються конкретні плани забезпечення інформаційної безпеки.

2.5 Стратегія та архітектура захисту інформації

В основі цього комплексу заходів щодо інформаційної безпеки має бути стратегія захисту інформації. У ній визначаються критерії, мета, принцип і процедури, які необхідні для побудови надійної системи захисту.

Найважливішою особливістю даної загальної стратегії інформаційного захисту є ефективне дослідження системи безпеки. Виділяються два основних напрямки:

- визначення факту вторгнення.
- аналіз засобів захисту;

На основі цієї концепції безпеки інформації розробляється архітектура системи захисту інформації та стратегія безпеки інформації, а далі – політика безпеки інформації (рис.1.1).

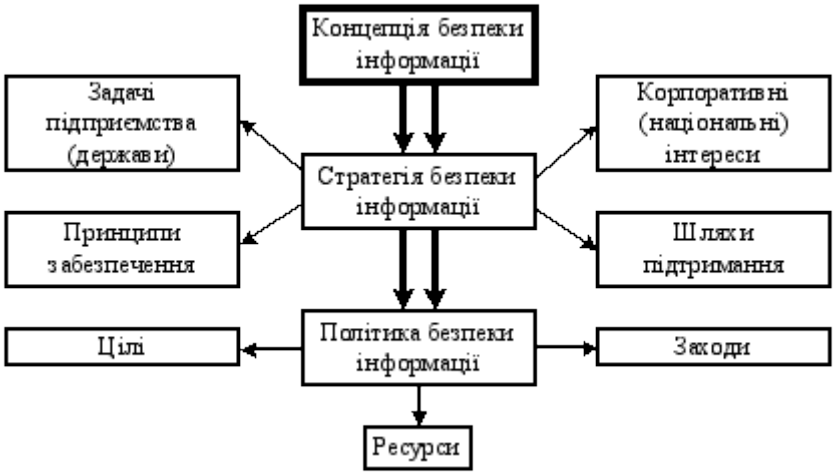


Рисунок 2.2 - Ієрархічний підхід до забезпечення безпеки інформації

Розробку концепції захисту рекомендовано проводити в три етапи (рис. 1.2).

На першому етапі має бути визначена цільова установка захисту, тобто які реальні цінності, програми, виробничі процеси, які масиви даних необхідно захищати. На даному етапі доцільно диференціювати по значимості деякі окремі об'єкти, що потребують захисту.

На другому етапі має бути виеонаний аналіз злочинних дій, що потенційно можуть бути зроблені стосовно об'єкта, що захищається. Також важливо визначити ступінь реальної небезпеки, як крадіжки зі зломом, економічне шпигунство, крадіжки зі зломом, саботаж. Далі потрібно зробити аналіз найбільш ймовірні дії зловмисників стосовно даних основних об'єктів, які мають бути захищені та потребують даного захисту.

Рисунок 2.3 - Етапи розробки концепції захисту інформації

Головною метою третього етапу є аналіз обставин, виробничих процесів, місцевих специфічних умов, уже встановлених технічних засобів захисту.

Концепція захисту має в собі містити перелік технічних, організаційних і інших заходів, що повинні забезпечвати максимальну безпеку при заданому залишковому ризику та мінімальні витрати на їх реалізацію.

Політика захисту - це загальний документ, в якому перераховуються правила доступу, описується базова архітектура середовища захисту та визначаються шляхи реалізації політики.

Документ складається з декількох сторінок тексту. Який формує основу фізичної архітектури мережі, а інформація, яка знаходиться в ньому, визначає вибір продуктів захисту.

Політика захисту повинна обов'язково відображати наступне:

- структура та складові автоматизованих інформаційних систем
- йому не дозволено користуватися);

- контроль доступу (заборона на доступ користувача до матеріалів);
- облік (запис усіх дій користувача в мережі);
- обмін даними (захист усіх комунікацій).
- надійність (запобігання монополізації ресурсів системи одним користувачем);
- ідентифікацію та аутентифікацію (використання паролів або інших механізмів для перевірки статусу користувача);
- акуратність (захист від будь-яких випадкових порушень);
- контрольний журнал (журнал дозволяє визначити, коли і де відбулося порушення захисту);

Один з найпростіших способів реалізації захисту – це обслуговування цієї системи спеціалізованою компанією.

Автоматизована інформаційна система, як і інша будь яка система є складною, вона складається з окремих елементів і організації відносин між ними. В автоматизованій інформаційній системі виділяють найбільше функціональну частину та частину забезпечення**,** які поділяються на простіші елементи - підсистеми, які також припускають подальший поділ.

2.6 Функціональна складова автоматизованої інформаційної системи

Функціональна частина АІС є домінуючою. Вона завжди пов'язана з проблемними сферами і фактично є моделлю системи управління конкретним об'єктом. До функціональної частини належать ті елементи, які визначають її функціональні можливості, а саме: призначення, виконувані управлінські

функції та функції з обробки інформації. Основними елементами функціональної частини автоматизованої інформаційної системи є: функціональні підсистеми, блоки, або комплекси задач та окремі задачі.

Рисунок 2.4 - Загальна структура автоматизованої інформаційної системи

Функціональна підсистема - це відносно самостійна частина системи, виділена за спільністю функціональних ознак управління. В автоматизованих інформаційних системах органів казначейства функціональні підсистеми, як правило, виокремлюють за такими ознаками:

- стадіями управління (прогнозування, планування, облік, звітність, аналіз, контроль тощо);
- видами основної діяльності (доходи, видатки, трансферти тощо);
- організаційною структурою (структурні підрозділи); - функціональною ознакою (виконувані функції).

Серед функціональних підсистем за ознакою управління складовими казначейської діяльності у процесі касового виконання бюджетів можна виділити: управління коштами єдиного казначейського рахунка, управління доходами державного й місцевих бюджетів, управління видатками бюджетів, управління внутрішніми казначейськими операціями, бухгалтерський облік і звітність про виконання бюджетів тощо. Незважаючи на те, що деякі функціональні підсистеми на різних об'єктах можуть мати одне й те саме найменування (наприклад, підсистема бухгалтерського обліку), їх внутрішній зміст щодо різних об'єктів значно відрізняється.

При виділенні функціональних підсистем мають бути визначені такі їх параметри:

- вид керованих ресурсів;
- мета функціонування підсистеми;
- особливості показників, що розраховуються у підсистемі; - підрозділи, які здійснюють управління.

2.7 Криптоалаіз шифра Віженера

Криптографія (від грец. Κρυπτός - прихований і γράφω - пишу) - наука про методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства, а також неможливості відмови від авторства) інформації.

Потреба шифрувати і передавати зашифровані повідомлення виникла дуже давно. Так, ще в V-IV ст. до н. е. греки застосовували спеціальний шифруючий пристрій. Перші придумані шифри ставилися до класу шифрів «проста заміна» або «підстановка». Це «Квадрат Полібія», «Шифр Цезаря». Це такі шифри, в якому кожній букві алфавіту відповідає буква, цифра, символ або якась їх комбінація. Термін "шифр" арабського походження. На початку XV ст. араби опублікували енциклопедію "Шауба Аль-Аща", в якій є спеціальний розділ про шифри. У цій енциклопедії зазначений спосіб розкриття шифру простої заміни. Він заснований на різній частоті повторюваності букв в тексті. У цьому розділі є перелік букв в порядку їх повторюваності на основі вивчення тексту Корану. Зауважимо, що в украньскому тексті найчастіше зустрічається буква "О", потім буква "Е" і на третьому місці стоять літери "І" та "А". Більш точно: на 1000 букв українського тексту в середньому припадає 90 літер "О", 72 літери "Е" і по 60 букв "І" та "А" і т.д.

Незручність шифрів типу "підстановка" ("проста заміна") в разі використання стандартного алфавіту очевидно. Таблиця частот зустрічальності букв алфавіту дозволяє визначити один або кілька символів, а цього іноді достатньо для дешифрування всього повідомлення. Тому зазвичай користуються різними прийомами, щоб утруднити дешифрування. Для цієї мети використовують многобуквенную систему шифрування - систему, в якій одному символу відповідає одна або кілька комбінацій двох і більше символів. Інший

прийом - використання декількох алфавітів. В цьому випадку для кожного символу вживають той чи інший алфавіт в залежності від ключа, який пов'язаний якимось способом з самим символом або з його порядком в переданому повідомленні. У процесі шифрування (і дешифрування) використовується таблиця ("таблиця Віженера"), яка влаштована таким чином: в першому рядку виписується весь алфавіт, в кожної наступної здійснюється циклічний зсув на одну букву. Так виходить квадратна таблиця, число рядків якої дорівнює числу стовпців і дорівнює числу букв в алфавіті.

2.8 Шифр Віженера - метод поліалфавітних шифрування літерного тексту з використанням ключового слова

Цей метод є простою формою многоалфавитной заміни. Шифр Віженера винаходився багаторазово.

Вперше цей метод описав Джован Баттіста Беллазо (італ. Giovan Battista Bellaso) в книзі La cifra del. Sig. Giovan Battista Bellaso в 1553 році, проте в XIX столітті отримав ім'я Блеза Віженер, французького дипломата. Метод простий для розуміння і реалізації, він є недоступним для простих методів криптоаналізу.

Блез Віженер представив свій опис простого, але стійкого шифру перед комісією Генріха III у Франції в 1586 році, і пізніше винахід шифру було присвоєно саме йому. Давид Кан в своїй книзі «Зломщики кодів» відгукнувся про це осудливо, написавши, що історія «проігнорувала важливий факт і назвала шифр ім'ям Віженер, незважаючи на те, що він нічого не зробив для його створення».

Шифр Віженера мав репутацію виключно стійкого до «ручного» злому. Відомий письменник і математик Чарльз Доджсон Доджсон (Люіс Керролл) назвав шифр Віженера невзламиваемим в своїй статті «Алфавітний шифр» англ. The Alphabet Cipher, опублікованій в дитячому журналі в 1868 році. У 1917 році Scientific American також відгукнувся про шифр Віженера, як про не піддається злому. Цю виставу було заперечений після того, як Касіскі повністю зламав шифр в XIX столітті, хоча відомі випадки злому цього шифру деякими досвідченими криптоаналітиків ще в XVI столітті. Шифр Віженера досить простий для використання в польових умовах, особливо якщо застосовуються шифрувальні диски. Наприклад, «конфедерати» використовували мідний

шифрувальний диск для шифру Віженера в ході Громадянської війни.

Опис алгоритма.

У шифрі Цезаря кожна буква алфавіту зсувається на кілька рядків; наприклад в шифрі Цезаря при зсуві +3, A стало б D, B стало б E і так далі. Шифр Віженера складається з послідовності декількох шифрів Цезаря з різними значеннями зсуву. Для зашифровування може використовуватися таблиця алфавітів, звана tabula recta або квадрат (таблиця) Віженера. Стосовно до латинському алфавіту таблиця Віженера складається з рядків по 26 символів, причому кожна наступна рядок зсувається на кілька позицій. Таким чином, в таблиці виходить 26 різних шифрів Цезаря. На різних етапах кодування шифр Віженера використовує різні алфавіти з цієї таблиці. На кожному етапі шифрування використовуються різні алфавіти, які обираються в залежності від символу ключового слова.

Розшифрування проводиться таким чином: знаходимо в таблиці Віженера рядок, відповідну першому символу ключового слова; в цьому рядку знаходимо перший символ зашифрованого тексту. Стовпець, в якому знаходиться даний символ, відповідає першому символу вихідного тексту. Наступні символи

зашифрованого тексту розшифровуються так само.

Якщо букви A-Z відповідають числам 0-25, то шифрування Віженера можна записати у вигляді формули:

$$C_i \equiv (P_i + K_i) \mod 26$$

Росшифровка:

$$P_i \equiv (C_i - K_i + 26) \mod 26$$

Криптоаналіз

Шифр Віженера «розмиває» характеристики частот появи символів у тексті, але деякі особливості появи символів в тексті залишаються. Головний недолік шифру Віженера полягає в тому, що його ключ повторюється. Тому простий криптоаналіз шифру може бути побудований в два етапи:

1. Пошук довжини ключа. Можна аналізувати розподіл частот в зашифрованому тексті з різним проріджування. Тобто брати текст, що включає кожну 2-ю букву зашифрованого тексту, потім кожну 3-ю і т. Д. Як тільки розподіл частот букв буде сильно відрізнятися від рівномірного (наприклад, по ентропії), то можна говорити про знайдену довжині ключа.

2. Криптоаналіз. Сукупність l шифрів Цезаря (де l - знайдена довжина ключа), які окремо легко зламуються.

Теорія криптоаналіза шифру Віженера Розглянемо шифр модульного гамування з рівнянням bi = (ai + yi) mod n, для якого гамма є періодичною послідовністю знаків алфавіту. Така гамма зазвичай виходить періодичним повторенням деякого ключового слова. Наприклад, ключове слово KEY дає гаму KEYKEYKEY .... Розглянемо задачу розкриття такого шифру по тексту однієї криптограми достатньої довжини.

Нехай μ - довжина ключового слова. Зазвичай криптоаналіз шифру Віженера проводиться в два етапи. На першому етапі визначається число μ, на другому етапі - саме ключове слово

Для визначення числа μ застосовується так званий тест Казіскі, названий на честь Ф. Казіскі, що застосував його в 1863 р Тест заснований на простому спостереженні про те, що два однакових відрізка відкритого тексту, віддалених один від одного на відстані, кратному μ, будуть однаково зашифровані. В силу цього в шифр-тексті шукаються повторення довжини, неменшою трьох, і відстані між ними. Звернемо увагу на те, що випадково такі однакові відрізки можуть з'явитися в тексті з досить малою вірогідністю.

Нехай d 1, d2, ... - знайдені відстані між повтореннями і d - найбільший спільний дільник цих чисел. Тоді μ має ділити d. Чим більше повторень має текст, тим більше ймовірно, що μ збігається з d. Для уточнення значення μ, можна використовувати так званий індекс збігу, введений в практику У. Фрідманом в 1920 р.

Для рядка x = (x1, ...,, xm) довжини т, складеної з букв алфавіту А, індексом збіги в x, позначається I c (x) будемо називати ймовірність того, що дві випадково вибрані букви з x збігаються.

Нехай A = {ai, ..., an}. Будемо ототожнювати букви алфавіту з числами, гак що a1 ≡ 0, ..., an-1 ≡ n - 2, a n = n -1. Теорема. Індекс збігу в x обчислюється за формулою:

$$I_C(x) = \frac{\sum_{i=0}^{n-1} f_1(f_i - 1)}{m(m-1)}.$$

Доведення. Будемо обчислювати I з (x) як відношення числа сприятливих результатів до загального числа випадків. Сприятливим є результат, при якому на обраних двох позиціях в x розташовані однакові літери. Загальне число результатів одно, очевидно, C 2 m . Число сприятливих результатів є:

$$\sum_{i=0}^{m-1} C_{f_i}^2$$

Справді, переупорядкувати букви в x таким чином, щоб спочатку йшли f a1 букв a 1 потім - f a2 букв *a 2* і т.д.

$$\underbrace{a_1,\ldots,a_1}_{f_{a_1}} \ldots \underbrace{a_n,\ldots,a_n}_{f_{a_n}}$$

Тепер зауважимо, що при випадковому виборі місць (*i* і *j)* в рядку *x* сприятливими є наступні результати:

$$(a_1)\begin{cases}0\ldots i\ldots j\ldots m-1\\ \ldots a_1\ldots a_1\ldots\end{cases}$$

$$(a_2)\begin{cases}0\ldots i\ldots j\ldots m-1\\ \ldots a_2\ldots a_2\ldots\end{cases}$$

$$\overline{\qquad\qquad}$$

$$(a_n)\begin{cases}0\ldots i\ldots j\ldots m-1\\ \ldots a_n\ldots a_n\ldots\end{cases}$$

Таким чином, загальне число сприятливих результатів виражається величиною, а індекс збігу в *x* – формулою

$$I_c(x)=\frac{\sum_{i=0}^{m-1} C_{f_i}^2}{C_m^2}$$

Нехай *x* - рядок осмисленого тексту (наприклад, англійської). Припустимо, як і раніше, що букви в *x* з'являються на будь-якому місці тексту з відповідними

можливостями *p 0 , ..., p n-1* незалежно один від одного, де *p i* - ймовірність появи

букви *i* в осмисленому тексті, і Z n У такій моделі відкритого тексту ймовірність

того, що дві випадково вибрані букви з *x* збігаються з *i,* Z n дорівнює *p 2i,* отже

$$I_c(x)\approx\sum_{i=0}^{n-1} p_i^2$$

Взявши за основу значення ймовірностей *p i* для відкритих текстів англійською мовою, отримуємо наближення:

$$\sum_{i=0}^{25} p_i^2 \approx 0{,}066$$

Тим самим для англійських текстів *x* можна користуватися наступним наближенням для індексу збігу:

I з (x) ≈ 0,066.

Аналогічні наближення можна отримати і для інших мов. Так, для української мови отримуємо наближення:

I з (x) ≈ 0,053.

Наведемо значення індексів збіги для ряду європейських мов:

Язык	Русский	Алгл.	Франц.	Нем.	Итал.	Испан.
$I_c(x) \approx$	0,0529	0,0662	0,0778	0,0762	0,0738	0,0775

Таблиця 2.1 – Індекси збігу для європейських мов

Міркування, використані при виведенні формули, залишаються, очевидно, справедливими і в разі, коли *x* результат шифрування деякого відкритого тексту простою заміною. В цьому випадку ймовірності *p i* переставляються місцями, але сума $\sum_{i=0}^{n-1} p_i^2$ залишається незмінною.

Припустимо, що *x* - реалізація незалежних випробувань випадкової величини, що має рівномірний розподіл на Z *n* . Тоді індекс збігу обчислюється за формулою:

$$I_c(x) = \sum_{i=0}^{n-1} \frac{1}{n^2} = n \cdot \frac{1}{n^2} = \frac{1}{n}$$

Повернемося до питання про визначення числа μ.

Нехай у = *y 1* у *2* ... у *n* - даний шифр-текст. Випишемо його з періодом μ:

$Y_1^{\downarrow}$	$Y_2^{\downarrow}$	...	$Y_\mu^{\downarrow}$
y_1	y_2	...	y_μ
$y_{\mu+1}$	$y_{\mu+2}$	...	$y_{2\mu}$
$y_{2\mu+1}$	$y_{2\mu+2}$	...	$y_{3\mu}$
...	...	...	...

і позначимо стовпці вийшла таблиці через $Y\downarrow 1$, ..., $Y\downarrow \mu$. Якщо μ це справжня довжина ключового слова, то кожен стовпець $Y\downarrow i$, *i 1*, μ , являє собою

ділянку відкритого тексту, зашифрований простою заміною, яка визначається підстановкою

$$\begin{pmatrix} 0 & 1 & 2 & \dots & n-s & \dots & n \\ s & s+1 & s+2 \dots & & 0 & \dots & s-1 \end{pmatrix}$$

для деякого s 0, nl (числа беруться по модулю n).

В силу сказаного вище, (для англійської мови) *I з (Y ↓i)* ≈ 0,066 при будь-якому *i* . З іншого боку, якщо *μ* відмінно від довжини ключового слова, то стовпці *Y ↓i* будуть більш "випадковими", оскільки вони є результатом зашифрування фрагментів відкритого тексту деяким багатоалфавітних шифром. Тоді *I з (Y ↓i)* буде ближче (для англійської мови) до числа 1/28 ≈ 0,038

Помітна різниця значень *I з (x)* для осмислених відкритих текстів і випадкових послідовностей літер (для англійської мови - 0,066 і 0,038, для російської мови - 0,053 і 0,030) дозволяє в більшості випадків встановити точне значення *μ.*

Припустимо, що на першому етапі ми знайшли довжину ключового слова *μ.*

Розглянемо тепер питання про знаходження самого ключового слова. для його знаходження можна використовувати так званий *взаємний індекс збігу.*

Нехай *x = (x] , ..., x n), y = (y 1 , ..., y m)* - два рядки букв алфавіту А. Взаємним індексом збіги *x і y,* позначається *MI з (x, y),* називається ймовірність того, що випадково обрана буква з *x* збігається з випадково обраної буквою з *y.*

Нехай *f 0 f 1 ... f n* і *f 0 f 1 ... f n-1* - числа входжень букв алфавіту в *x і y* відповідно.

Теорема. *Взаємний індекс збігу в x і y визначається за формулою* (ця теорема доводиться точно так же, як і попередня теорема.

$$MI_c(x,y) = \frac{\sum_{i=0}^{n-1} f_i \cdot f_i^1}{m \cdot n'}$$

Нехай k = (*k 1* , ..., *k μ* ,) - справжнє ключове слово. спробуємо оцінити індекси *MI c (Y ↓i , Y ↓j)*

Для цього нагадаємо, що $Y\downarrow 3$ є результатом зашифрування фрагмента відкритого тексту простою заміною, яка визначається підстановкою при деякому s. Імовірність того, що $Y\downarrow i$ і $Y\downarrow j$ довільна пара букв дорівнює 0, має вигляд $p\ nsi * p\ n\text{-}sj$ (де $p\ a$ - ймовірність появи букви а у відкритому тексті); ймовірність того, що обидві літери є 1, дорівнює $p\ n\text{-}si + 1 * p\ n\text{-}sj + 1$ і так далі. На підставі цього отримуємо:

$$MI_c(Y_i^{\downarrow}, Y_j^{\downarrow}) \approx \sum_{h=0}^{n-1} p_{h-s_i} \cdot p_{h-s_j} = \sum_{h=0}^{n-1} p_h \cdot p_{h+(s_i-s_j)}$$

Зауважимо, що сума в правій частині останнього рівності залежить тільки від різниці $(s\ i - s\ j)\ mod\ n$, яку назвемо *відносним зсувом* $Y\downarrow i$ і $Y\downarrow j$. Зауважимо також, що:

$$\sum_{j=0}^{n-1} p_j \cdot p_{(j+s) \bmod n} = \sum_{j=0}^{n-1} p_j \cdot p_{(j-s) \bmod n}$$

тому $Y\downarrow i$ і $Y\downarrow j$ з відносними зрушеннями s і $n\text{-}s$ мають однакові взаємні індекси збіги. Наведемо таблицю значень сум для англійської мови:

Сдвиг s	*0*	*1*	*2*	*3*	*4*	*5*	*6*
$MI_c(x,y) \approx$	0,066	0,039	0,032	0,034	0,044	0,033	0,036
Сдвиг s	*7*	*8*	*9*	*10*	*11*	*12*	*13*
$MI_c(x,y) \approx$	0,039	0,034	0,034	0,038	0,045	0,039	0,043

Таблиця 2.2 Значення сум для англійської мови

Звернемо увагу на те, що ненульові "зрушення" дають взаємні індекси збіги, що змінюються в межах від 0,032 до 0,045, в той час як при нульовому зсуві індекс *MI c (x, y)* близький до 0,066. Це спостереження дозволяє визначити величини відносних зрушень $s\ i - s\ j$ стовпців $Y\downarrow i$ і $Y\downarrow j$. Для цього зауважимо, що при деякому значенні $s\ (i,\ j)$ 0, n-1столбец $Y\ s\ (i,\ j)\downarrow j$, отриманий з $Y\downarrow j$ додатком до кожного його елементу числа $S\ (i,\ j)$ (по модулю n), має нульовий відносний зрушення з $Y\downarrow$

Нехай $Y\ 0\downarrow j$, $Y\ 1\downarrow j$, ..., $Y\ n\text{-}1\downarrow j$ - результати шифрування $Y\downarrow j$ кожної з простих замін. Нескладно обчислити взаємні індекси:

$$MI_c(Y_i^{\downarrow}, Y_j^{\downarrow}), \quad 0 \le s \le n-1, \quad 1 \le i < j \le \mu$$

всього, таким чином, є $C\ 2\mu\ n$ значень. Для цього скористаємося формулою, отриманої з

$$MI_c(Y_i^{\downarrow}, Y_j^{s\downarrow}) = \frac{\sum_{h=0}^{n-1} f_h \cdot f_{h-s}^1}{m \cdot m'}$$

Якщо s одно *s i - s j* - (відносного зсуву *Y ↓i* і *Y ↓j*), то взаємний індекс впадання повинен бути (для англійської мови) близький до 0,066, так як відносний зсув *Y ↓i* і *Y ↓j* дорівнює нулю. Якщо ж s не дорівнює *s i - s j* то взаємний індекс збігу повинен коливатися в межах 0,032 - 0,045.

Використовуючи викладений метод, ми зможемо пов'язати системою рівнянь відносні зрушення різних пар стовпців *Y ↓i* і *Y ↓j* . В результаті залишиться 26 (Для англійської мови) варіантів для ключового слова, з яких можна вибрати найкращий варіант (якщо ключове слово є осмисленим). Слід зазначити, що запропонований метод буде ефективним для занадто великих значень μ. Це пояснюється тим, що для хороших зближень індексів збігу потрібні тексти досить великої довжини.

3.РОЗРОБЛЕННЯ АЛГОРИТМУ РОБОТИ ТА СТРУКТУРНОЇ СХЕМИ ПРИСТРОЮ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

3.1 Розроблення алгоритму роботи пристрою захисту конфіденційної інформації

В даному розділі ми розробили блок схему алгоритму роботи пристрою. Також представлені таблиці Віженера, для шифрування даної інформації.

Алгоритм роботи пристрою:

Крок 1.Введення ключового слова чи символа. Блок 1.

Крок 2. Вибір строки або введення символів, які потрібно зашифрувати і запис в блок пам’яті. Блок 12.

Крок 3. Перевірка тексту на символи. Блок 3.

Крок 4. Визначення мови тексту якого потрібно зашифрувати. Блок 10.

Крок 5. Виконується виправлення даного тексту. Блок 5.

Крок 6. Виконується генерація квадрата Віженера, для шифрування. Блок 11.

Крок 7. Виконується шифрування даного тексту. Блок 13

Крок 8. Формування рядка, в якому записується результат шифрування. Блок 14.

Крок 9. Вказується чи потрібно шифрувати нову строку.

	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
а	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
б	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а
в	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б
г	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в
ґ	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г
д	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ
е	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д
є	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е
ж	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є
з	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж
и	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з
і	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и
ї	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і
й	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї
к	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й
л	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к
м	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л
н	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м
о	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н
п	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о
р	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п
с	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р
т	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с
у	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т
ф	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у
х	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ь	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ю	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
я	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю

Рисунок 3.1 - Табличне представлення шифру Віженера для Української мови

Дана таблиця призначена для шифрування інформації українського алфавіту.

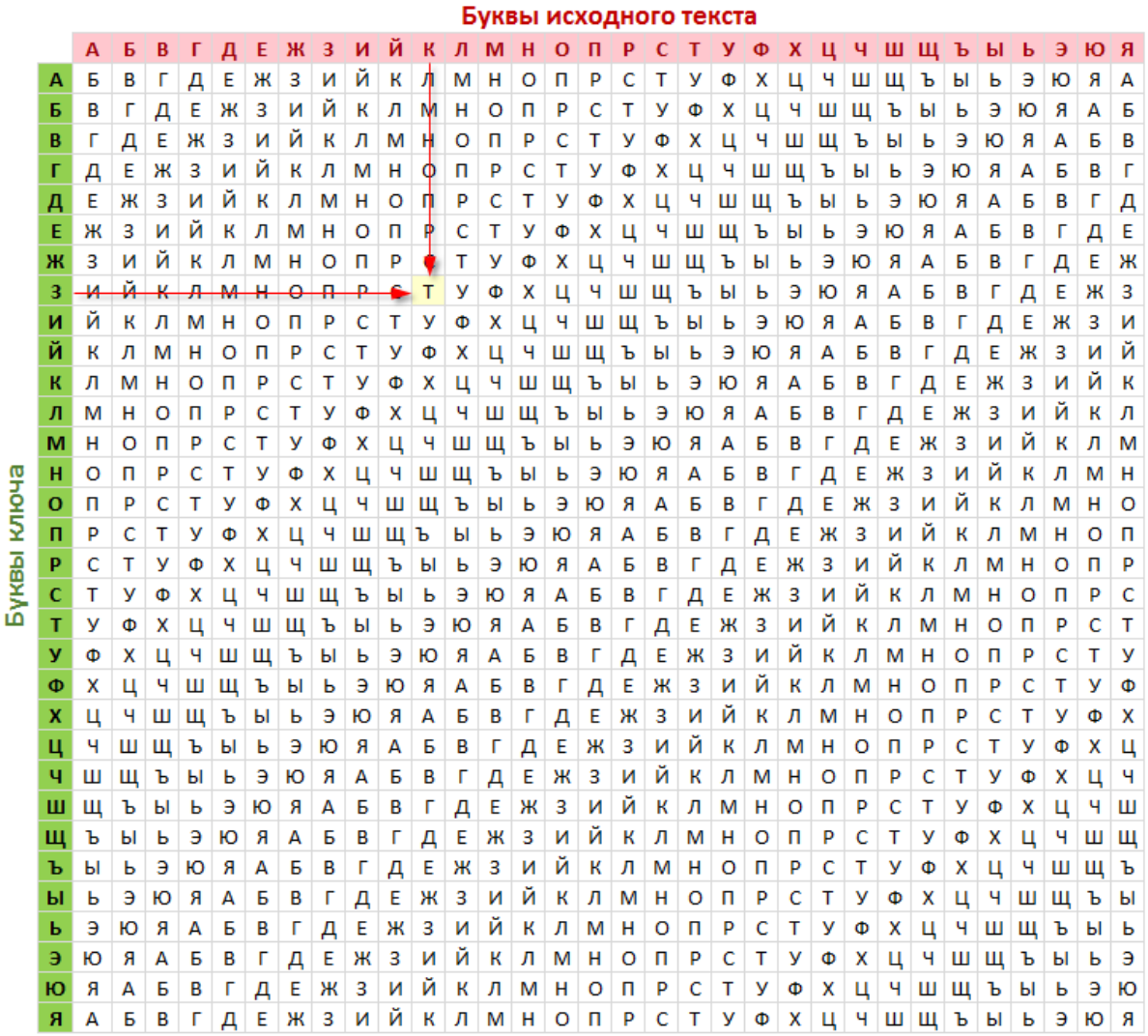


Рисунок 3.2- Табличне представлення шифру Віженера для Російської мови

Дана таблиця призначена для шифрування інформації російського алфавіту.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Рисунок 3.3 - Табличне представлення шифру Віженера для Англійської мови

Дана таблиця призначена для шифрування інформації англійського алфавіту.

	0	1	2	3	4	5	6	7	8	9	.	,	:	;	«	»	[	]
0	0	1	2	3	4	5	6	7	8	9	.	,	:	;	«	»	[	]
1	1	2	3	4	5	6	7	8	9	.	,	:	;	«	»	[	]	0
2	2	3	4	5	6	7	8	9	.	,	:	;	«	»	[	]	0	1
3	3	4	5	6	7	8	9	.	,	:	;	«	»	[	]	0	1	2
4	4	5	6	7	8	9	.	,	:	;	«	»	[	]	0	1	2	3
5	5	6	7	8	9	.	,	:	;	«	»	[	]	0	1	2	3	4
6	6	7	8	9	.	,	:	;	«	»	[	]	0	1	2	3	4	5
7	7	8	9	.	,	:	;	«	»	[	]	0	1	2	3	4	5	6
8	8	9	.	,	:	;	«	»	[	]	0	1	2	3	4	5	6	7
9	9	.	,	:	;	«	»	[	]	0	1	2	3	4	5	6	7	8
.	.	,	:	;	«	»	[	]	0	1	2	3	4	5	6	7	8	9
,	,	:	;	«	»	[	]	0	1	2	3	4	5	6	7	8	9	.
:	:	;	«	»	[	]	0	1	2	3	4	5	6	7	8	9	.	,
;	;	«	»	[	]	0	1	2	3	4	5	6	7	8	9	.	,	:
«	«	»	[	]	0	1	2	3	4	5	6	7	8	9	.	,	:	;
»	»	[	]	0	1	2	3	4	5	6	7	8	9	.	,	:	;	«
[	[	]	0	1	2	3	4	5	6	7	8	9	.	,	:	;	«	»
]	]	0	1	2	3	4	5	6	7	8	9	.	,	:	;	«	»	[

Рисунок 3.4 - Табличне представлення шифру Віженера для цифр та символів.

Дана таблиця призначена для шифрування інформації яка складається з цифр та символів.

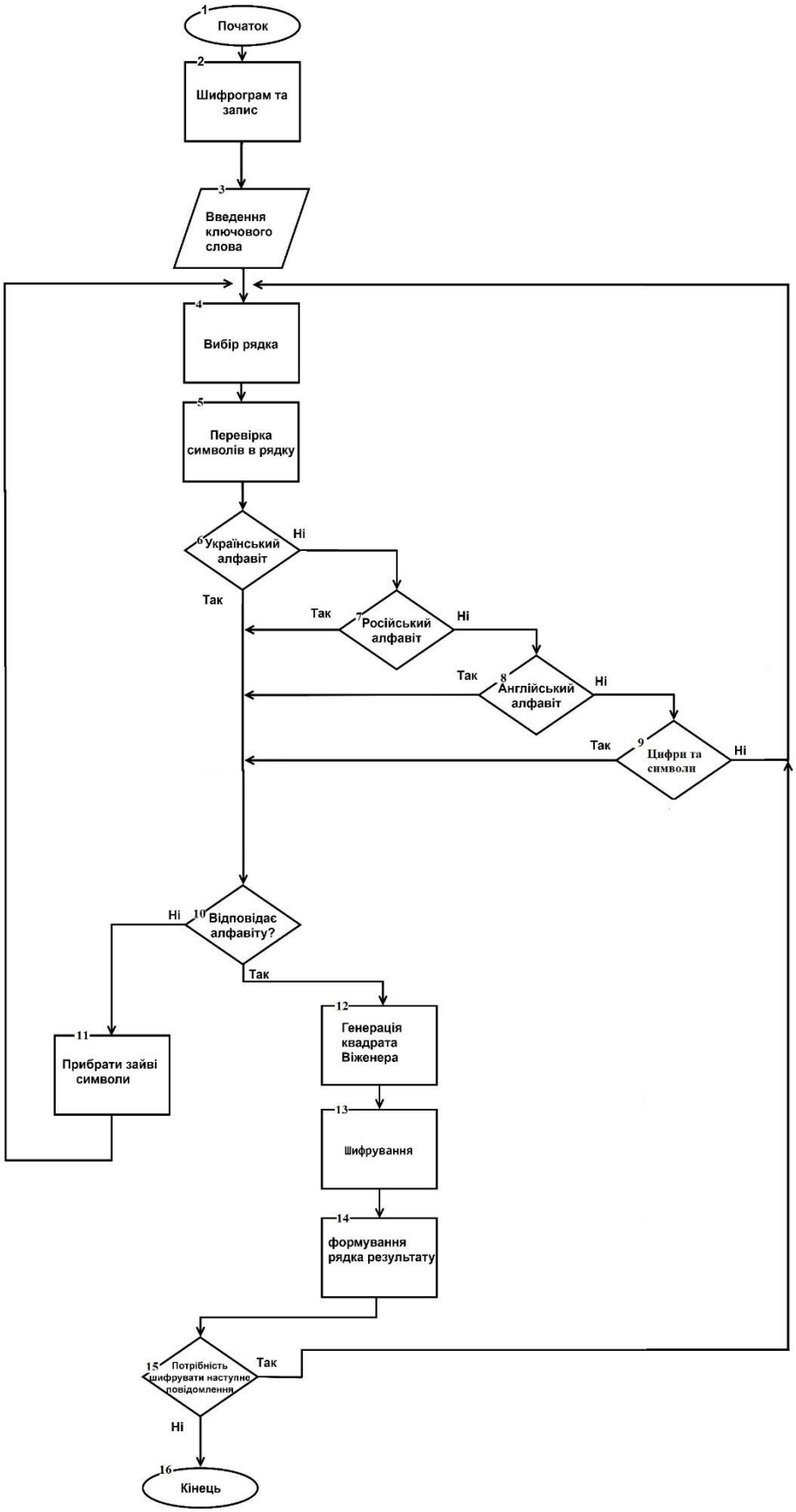


Рисунок 3.5 - Схема алгоритму роботи

3.2 Розроблення структурної схеми пристрою захисту конфіденційної інформації

На основі алгоритму функціонування розробляється структурна схема пристрою. Вона являє собою сукупність блоків з відображенням відповідних зв'язків між ними. На рис 3.6. представлена структурна схема пристрою.

До складу пристрою захисту інформації в залежності від виконання певної функції входять наступні блоки та вузли:

- блок формування ключа, який призначений для введення ключа для шифрування даного рядка;
- блок вибору рядка, який призначений для вибору рядка, в якому знаходяться вказаний текст чи символи для шифрування;
- блок перевірки символів в рядку для виявлення помилки у рядку;
- блок аналізу символів, який призначений для визначення типу даних для шифрування;
- блок заміни символів для виправлення помилок у рядку;
- блок керування, що видає керуючі сигнали, необхідні для коректної роботи всіх блоків;
- блок формування квадрата Віженера, який призначений для формування квадрата Віженера, для визначеної мови чи символів в рядку;
- блок пам'яті для запису та зберігання інформації;
- формувач шифрограм, який виконує шифрування даного тексту та надає зашифрований текст у вигляді шифрограмми.

Принцип роботи ПЗКІ полягає в наступному:

1. Виконується введення ключа для шифрування даного тексту, чи символів.

2. Проводиться аналіз на помилки в тексті для подальшого шифрування.

3. За допомогою управляючих команд виконується генерація квадрата Віженера, та виконується шифрування даного тексту чи символів.

4. Отримана шифрограма записуюється до блоку пам'яті, для очікування наступних команд.

5. Принцип шифрування детальніше наведений при поясненнях до алгоритму роботи пристрою.

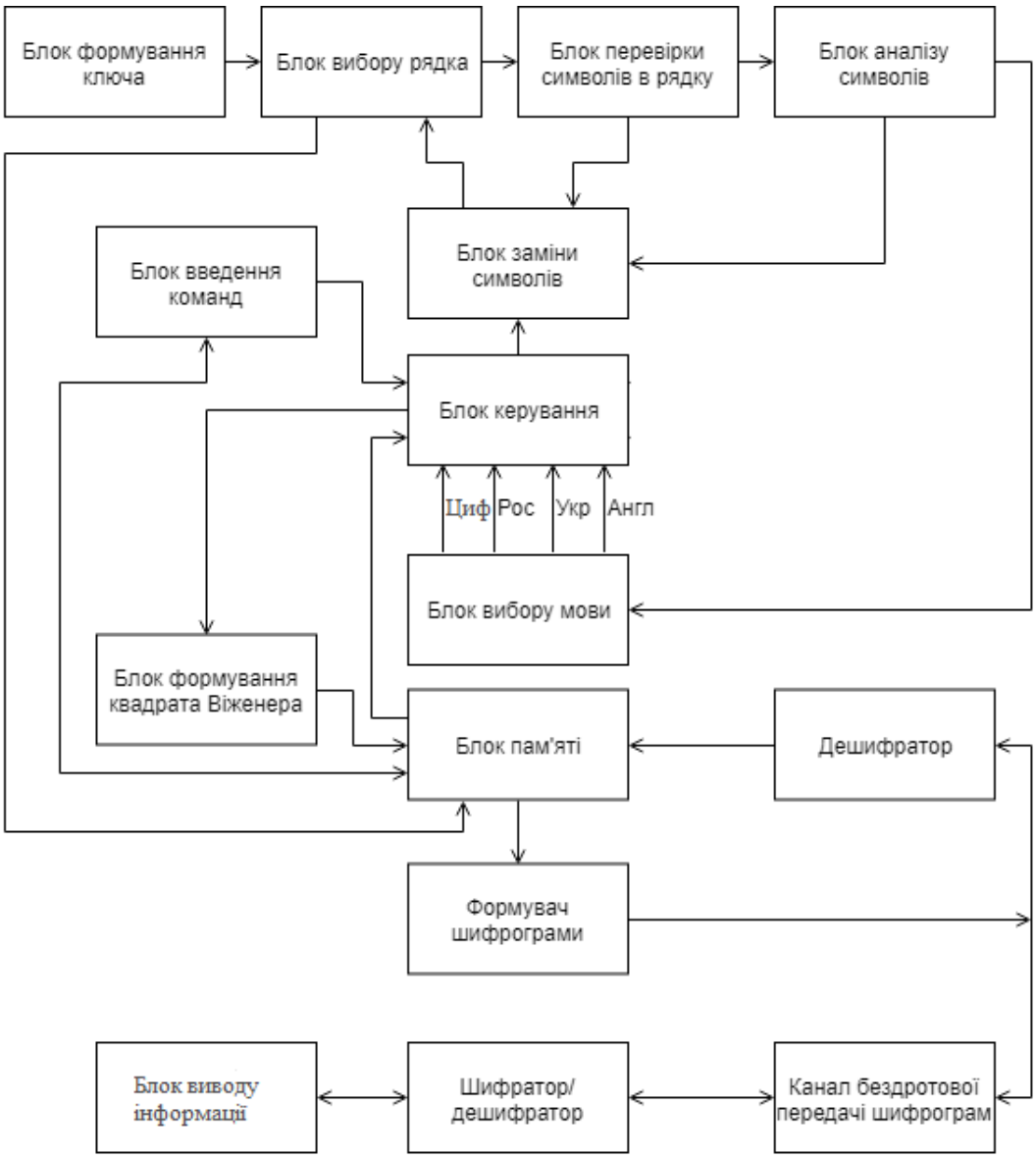


Рисунок 3.6 - Структурна схема пристрою захисту конфіденційної інформації

4. РОЗРОБЛЕННЯ СХЕМИ ЕЛЕКТРИЧНОЇ ФУНКЦІОНАЛЬНОЇ ПРИСТРОЮ

4.1 Розробка блока управління.

Центральний процесорний модуль є основним блоком шифрування. Він забезпечує управління і синхронізацію роботи всього пристрою, забезпечує прийом, видачу, зберігання і обробку даних, що надходять з системної шині.

До складу мікропроцесорного блоку (МПБ) входять процесор, буферний регістр, двонаправлений системний контролер, зовнішній резонатор, схема формування скидання.

Мікропроцесор (МП) - обробляє і керуючий пристрій виконане з використанням технології БІС, на одному або декількох кристалах і володіє здатністю під програмним управлінням виконувати обробку інформації.

У таблиці 3.1 наведено призначення виводів МП.

Таблица 4.1 - Призначення виводів процессора

Выводы	Призначення виведення
X1,X2	Вихід для підключення кварцового резонатора.
AD0-AD7	Шина адрес / даних
A8-A15	ША
ALE	Дозвіл захоплення адреси
RD	Управління зчитуванням
WR	Управління записом
IO/M	Покажчик введення-виведення / пам'ять
READY	Виклик стану очікування
HOLD	Запит захоплення
HLDA	Підтвердження стану захоплення
RESI	Скидання мікропроцесора

На рисунку 4.1 представлено позначення МП на функціональній схемі.

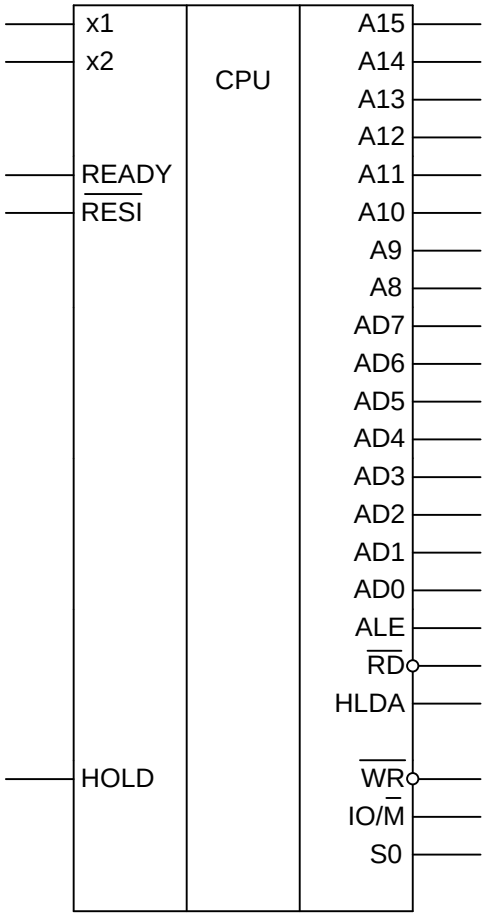


Рисунок 4.1 – Позначення на функціональній схемі мікропроцесора

У мікропроцесорний блок також входить буферний регістр. Він використовується для реалізації схеми фіксації, буферизації і мультиплексування в мікропроцесорних системах. В даному блоці буферний регістр використовується для формування сигналів шини адреси МП.

На рисунку 4.2 представлено позначення буферного регістра на функціональній схемі.

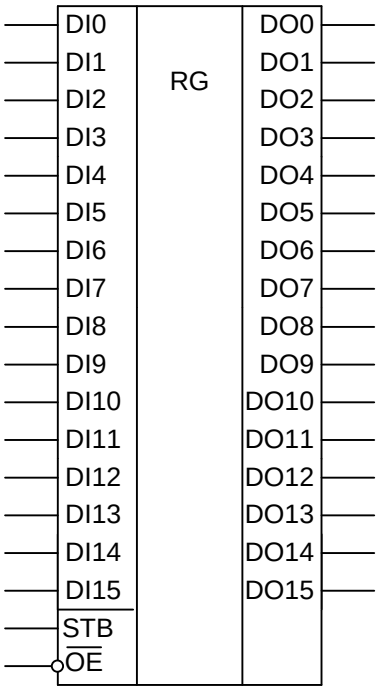


Рисунок 4.2 - Позначення на функціональній схемі буферного регістра

В таблиці 4.2 наведено призначення виводів буферного регістра

Таблиця 4.2 - Призначення виводів буферного регістра

Позначення	Призначення
DO0- DO15	Інформаційна шина
DI0- DI15	Інформаційна шина
STB	Строб сигнал
OE	Дозвіл передачі даних

Запис вхідних даних в регістр проводиться при переході сигналу STB з H - рівня в L - рівень. При H - рівень сигналу OE виходи буферних регістрів знаходяться в високоімпедансном стані.

Також до мікропроцесорній комплекту входить системний контролер. Він призначений для формування сигналів. Таких як INTA, MEMR, MEMW, IO / R, IO / W і передачі даних від МП і до нього.

На рисунку 3.3 представлено позначення системного контролера на функціональній схемі.

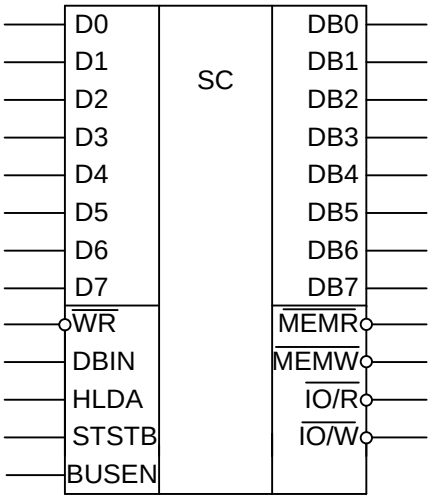


Рисунок 4.3 - Позначення на функціональній схемі системного контролера

У таблиці 4.3 наведено призначення виводів системного контролера.

Таблиця 4.3 - Призначення виводів системного контролера

Позначення виводу	Призначення
D(7-0)	Входи / виходи даних
STSTB	Строб стану від ГТВ
DBIN	Вхід сигналу «прийом» від МП
WR	Вхід сигналу «видачі» від МП
HLDA	Вхід сигналу «підтвердження захоплення» від МП
DB(7-0)	Входи / виходи інформаційної системної шини
MEMR	Читання пам'яті
MEMW	Запис в пам'ять
I/OR	Читання з ВУ
I/OW	Запис в ВУ
BUSEN	Дозвіл роботи шини

Інформація від МП в пам'ять, до зовнішнього пристрою і навпаки надходить через виводи D (7-0), DB (7-0) системного контролера. А також системний контролер перетворює сигнали процесора в сигнали читання / запису пам'яті і зовнішніх пристроїв - MEMR, MEMW, I / OR, I / OW.

На рисунку 4.4 представлено позначення МПБ на функціональній схемі.

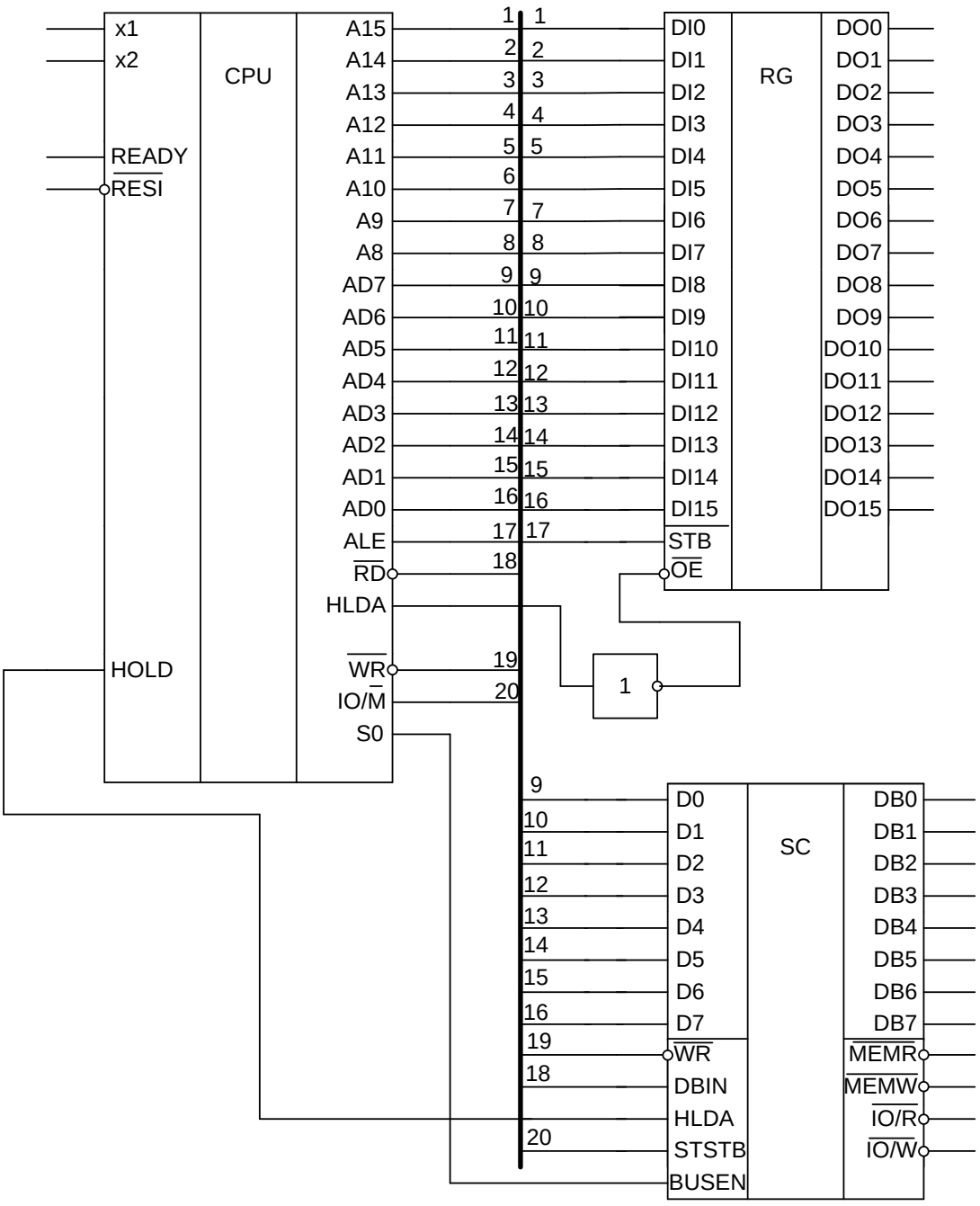


Рисунок 4.4 - Позначення на функціональній схемі МПБ

4.2 Розробка блока памяті

У мікроконтролері проектованого блок пам'яті складається з ПЗУ, ОЗУ і селектора адрес пам'яті.

Постійна пам'ять (ПЗУ) - призначена для зберігання кодів програми, що управляє роботою всього мікроконтролера. Оскільки керуюча програма не велика, то і обсяг ПЗУ потрібен невеликий. Рекомендований обсяг ПЗУ 2 кб. Пам'ять програм (ПЗУ) розділена на дві частини: резидентна програмна пам'ять

об'ємом 4К і зовнішня програмна пам'ять. Якщо адреса вибірки команди виходить за межі резидентної пам'яті, то автоматично підключається зовнішня пам'ять.

Оперативна пам'ять (ОЗУ) - призначена для збереження вихідних даних, що надходять від зовнішніх пристроїв і вихідні дані, які будуть виведені на зовнішній пристрій. Дані вводяться і ті, які виводяться потребують як мінімум в 300 КБ пам'яті, тому рекомендований обсяг ОЗУ 512 Кбайт. Пам'ять даних (ОЗУ) розбита на два банки регістрів загального призначення (Рзн).

Селектор адрес пам'яті - призначений для активізації ПЗУ або ОЗУ, в залежності який вихідний сигнал буде на адресному виході мікропроцесора А11.

На рисунку 4.5 представлено позначення ROM на функціональній схемі.

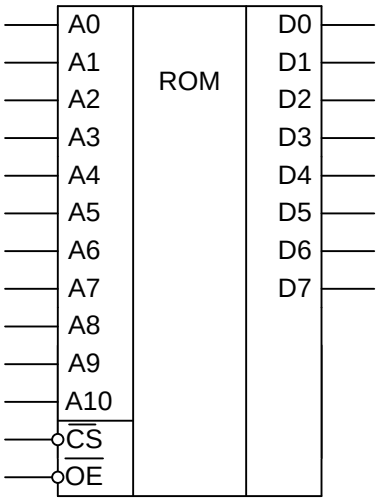


Рисунок 4.5 - Позначення на функціональній схемі ПЗУ

В таблиці 4.4 наведено призначення виводів ПЗУ.

Таблиця 4.4 - Призначення виводів постійної пам'яті

Позначення	Призначення
A0-A10	Шина адрес
CS	Вибір мікросхеми
OE	Дозвіл передачі
D0-D7	Мультиплексована шина даних

На входи A0-A10 надходить від МП адресу тієї комірки пам'яті, в якій зберігається код команди необхідної для управління роботою всього пристрою.

З виводів D0-D7 в мікропроцесор надходить необхідна команда для управління роботою всього пристрою. CS необхідний для активації мікросхеми, я OE - щоб дозволити надсилання даних.

На рисунку 4.6 представлено позначення RAM на функціональній схемі.

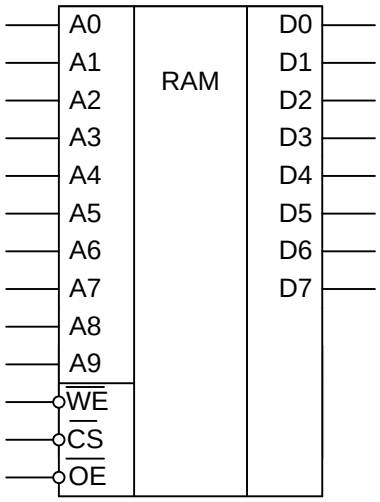


Рисунок 4.6 - Позначення на функціональній схемі ОЗУ

В таблиці 4.5 наведено призначення виводів ОЗУ.

Таблиця 4.5 – Призначення виводів ОЗУ

Позначення	Призначення
A0-A9	Адресні входи
CS	Вибір мікросхеми
WR	Запис / читання
D0-D7	Входи / виходи даних
OE	Сигнал дозволу зчитувати

4.3 Розробка інтерфейсного блоку

Так як в мікропроцесорних системах можливо три варіанти введення – виведення (програмне введення - виведення, введення - виведення з перериванням, введення - виведення в режимі прямого доступу до пам'яті), то необхідно вибрати якийсь один. Розглянемо кожен з методів більш детально.

При програмному здійсненні введення виведення ініціатором обміну є мікропроцесор. Він проводить опитування зовнішніх пристроїв на готовність їх до обміну і якщо отримує підтвердження реалізує обмін.

До складу паралельного інтерфейсу входять:

а) двонаправлений 8-розрядний буфер даних, що з'єднує лінії даних інтегральної мікросхеми з системною шиною даних;

б) блок управління читанням / записом, що забезпечує управління зовнішньої і внутрішньої передачею даних і керуючих слів;

в) три восьми розрядні порти вводу-виводу (PA, PB, PC), призначені для обміну інформацією при чому порт 3 поділений на 4-розрядні полупорти: C` (PC7-PC4), і C`` (PC3-PC0).

На рисунку 4.8 представлено позначення паралельного інтерфейсу на функціональній схемі.

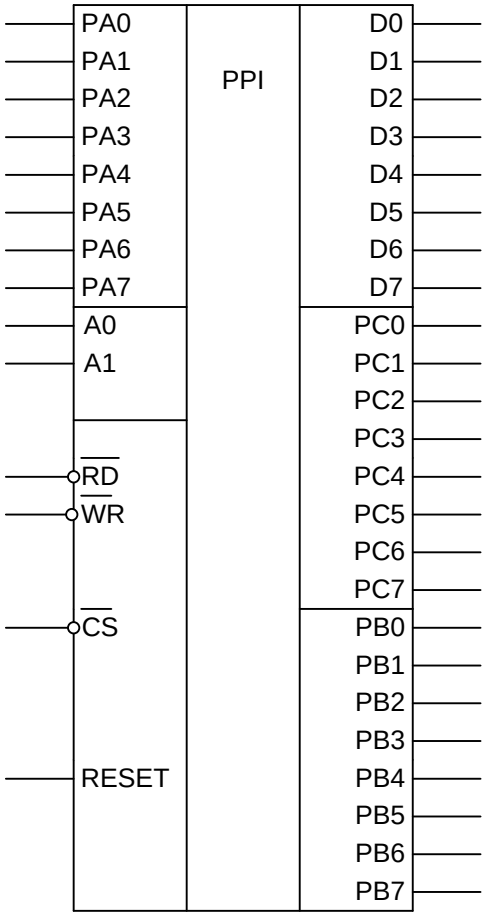


Рисунок 4.8 - Позначення на функціональній схемі паралельного інтерфейсу

Напрямок передачі даних визначає комбінація сигналів на адресних входах A0, A1 і входах читання RD і запису WR за умови вибірки мікросхем (CS = 0). При CS = l входи - виходи D0 - D7, PA0 - PA7, PB0 - PB7, PC0 - PC7 знаходяться в Z-стані. Канал А використовується для прийому вхідної інформації. Канал В використовується для виведення вихідної інформації, а канал С - для видачі керуючих сигналів на буферні регістри блоку індикації.

Призначення входів і виводів паралельного інтерфейсу наведено в таблиці 4.6.

Таблиця 4.6 - Призначення виводів паралельного інтерфейсу

Позначення	Призначення
D0-D7	Входи / виходи даних
PA0-PA7	Канал А
PB0-PB7	Канал В
PC0-PC7	Канал З
RESET	Скидання
A0,A1	Входи для адресації внутрішніх регістрів
RD	Читання
WR	Запис
CS	Вибір мікросхеми

4.4 Розробка блоку відображення інформації

Блок відображення інформації призначений для виведення даних на цифрові індикатори. У блок відображення інформації входять: індикатор, дешифратор, буферний регістр.

На рисунку 4.9 представлено позначення семисегментний індикатора на функціональній схемі.

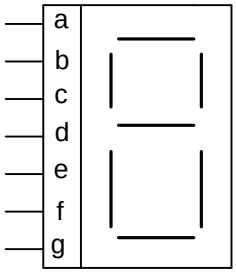


Рисунок 4.9 - Позначення на функціональній схемі семисегментного індикатора.

На індикатори виводиться наступна інформація: код помилки, яка могла виникнути при виконанні шифрування інформаці або зображення; розмір вхідного зображення і вже зашифрований. Для реалізації виведення даної інформації необхідний семисегментний індикатор.

Вибір сегмента здійснюється за допомогою дешифратора.

На рисунку 4.10 представлено позначення дешифратора на функціональній схемі.

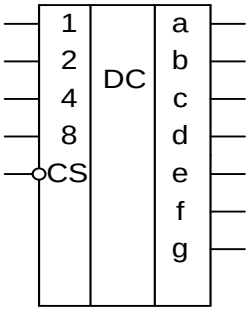


Рисунок 4.10 - Позначення на функціональній схемі дешифратора

Призначення входів і виходів дешифратора приведено в таблиці 3.7.

Таблиця 4.7 - Призначення виводів дешифратора

Позначення виводів	Функціональне призначення виводів
Г	Активація мікросхеми
1,2,4,8	Дані
a-g	Вихідний код

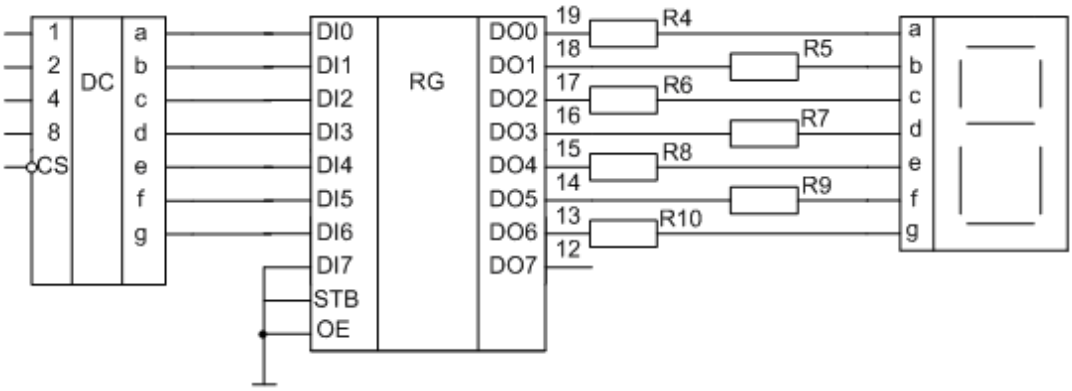


Рисунок 4.11 - Позначення на функціональній схемі

Залежно від того який код прийшов на входи 1,2,4,8, такий код буде на виходах a-g, т.с. які будуть активні сегменти на індикаторі.

Для того щоб зберігати дані, що надходять від процесора до блоку відображення інформації необхідно використовувати буферні регістри.

4.5 Опис роботи пристрою

Після виконання програми тестування всіх основних вузлів пристрою шифрування інформації чи зображення, МП починає проводити опитування зовнішніх пристроїв на готовність їх до обміну і якщо отримує підтвердження, реалізує обмін даними.

При отриманні сигналу готовності від паралельного інтерфейсу (ПІ), МП перемикається на роботу з ним. МП активізує паралельний інтерфейс подавши на вхід CS сигнал логічного нуля і налаштовує його на режим прийому інформації. МП подає на вивід ПІ A0, A1 адреса порту А і налаштовує його на прийом даних подавши на вхід RD ПІ сигнал логічного нуля.

Після того як інформація чи зображення було зашифровано, його необхідно зберегти в ОЗУ. Для цього МП видає через буферні регістри на ША адресу першого осередку пам'яті, куди буде записано зображення. Паралельно з цими діями МП формує сигнал запису в ОЗУ - MEMW і за допомогою селектора адрес активізує мікросхему ОЗУ, подавши на входи CS і OE даної мікросхеми сигнал логічного нуля. Після цього МП починає передавати зашифровану інформацію чи зображення по ШД в ОЗУ.

Після виконання налаштувань ОЗУ видає на ШД кодове відображення зашифрованого зображення, яке надходить в паралельний інтерфейс, а з нього на зовнішній пристрій.

МП періодично опитує зовнішні пристрої на готовність їх обміну з МП. Якщо пристрої готові то пристрій знову виконує всі операції описані вище.

5. РОЗРОБЛЕННЯ ПРИНЦИПОВОЇ ЕЛЕКТРИЧНОЇ СХЕМИ ПРИСТРОЮ

5.1 Мікропроцесорний блок

Центральний модуль є основним блоком контролера, що забезпечує управління та синхронізацію роботи пристрою, забезпечує видачу інформації, зберігання даних та обробку даних.

До складу мікропроцесорного блоку (МПБ) входять процесор КР1821ВМ85А, два буферних регістра КР580ІР82, двонаправлений системний контролер КР580ВК28, зовнішній резонатор (ZQ, С1), схема формування скидання (R1, С2, S).

Саме від вибору процесора залежить швидкодія системи в цілому, точність обробки даних, а також зручність розробки програмного забезпечення. Оптимальним для розроблюваного курсового проекту буде мікропроцесор КР1821ВМ85А, перевагами якого є:

- низька вартість;
- орієнтування на роботу в складі мікроконтролерів;
- програмна сумісність з мікропроцесором КР580ВМ80А;
- наявність одного джерела живлення +5 В;
- наявність вбудованого генератора тактових імпульсів;
- вбудований системний контролер;
- вбудований контроллер переривання.

Однак, поряд з перерахованими перевагами, у КР1821ВМ85А є і деякі недоліки:

- низька швидкодія (тривалість одного машинного такту - 0,5 мкс);
- час виконання однієї команди - 7-8 мкс);
- розрядність оброблюваних даних 8 біт;
- відсутність команди ділення в наявному складі команд.

Для стабілізації частоти системного генератора до виводів Х1 і Х2 БІС КР1821ВМ85А підключають кварцовий резонатор з номінальною частотою 18500кГц. При цьому тривалість машинного такту буде дорівнює 0,486 мкс. Конденсатор С2 - використовується для регулювання частоти системного

генератора в невеликих межах. Ланцюжок R1C1 служить для короткочасного формування імпульсу з негативним переднім фронтом тривалістю не менше 1,5

мкс (3 машинних такти).

На рисунку 4.1 представлено позначення МП КР1821ВМ85А на принциповій схемі.

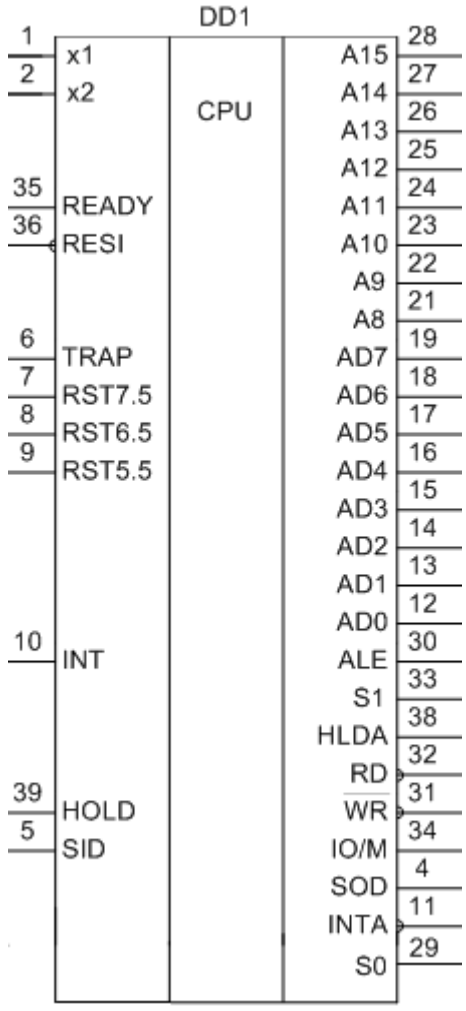


Рисунок 5.1 - Позначення на принциповій схемі мікропроцесора КР1821ВМ85А

У таблиці 5.1 наведено призначення виводів МП КР1821ВМ85А

Таблиця 5.1 – Призначення виводів процессора КР1821ВМ85А

Виводи	№ контакта	Призначення виводів
X1,X2	1,2	Вихід для підключення кварцового резонатора.
AD0-AD7	12-19	Шина адрес / даних
A8-A15	21-28	ША

ALE	30	Дозвіл захоплення адреси
RD	32	Управління зчитуванням
WR	31	Управління записом
IO/M	34	Покажчик введення-виведення / пам'ять
S0,S1	29,33	Покажчик стану шини
RESI	36	Скидання мікропроцесора
READY	35	Виклик стану очікування
SID	5	Введення послідовних даних
SOD	4	Висновок послідовних даних
HOLD	39	Запит захоплення
HLDA	38	Підтвердження стану захоплення
INT	10	Запит на переривання
TRAP	6	Запит немаскірованного переривання
RST	7,8,9	Запит апаратного векторного переривання
INTA	11	Підтвердження запиту на переривання
Vcc	40	Живлення
GND	20	Земля

Також до мікропроцесорній блоку повинен входити буферний регістр. Повністю спільний з мікропроцесором КР1821ВМ85 буферний регістр КР580ІР82. Це восьми розрядний адресний буферний регістр, який призначений для зв'язку процесора з системною шиною. Має підвищені навантажувальні можливості. Призначення виводів регістра в таблиці 4.2.

Таблиця 5.2 - Призначення виводів буферного регістра КР580ІР82

№ вивода	Позначення	Призначення
19-12	DO0- DO7	Інформаційна шина
1-8	DI0- DI7	Інформаційна шина
11	STB	Строб сигнал
9	OE	Дозвіл передачі даних
20	Ucc	Напруга живлення
10	GND	Земля

На рисунку 5.2 представлено позначення буферного регістра КР580ІР82 на принциповій схемі.

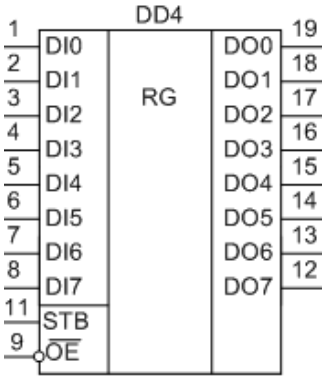


Рисунок 5.2 - Позначення на принциповій схемі буферного регістра КР580ІР82

Основні електричні параметри мікросхеми КР580ІР82:

Вихідна напруга логічного нуля U0L, В ..... ≤ 0,5

Вихідна напруга логічного одиниці U0H, В ..... ≥ 2,4

Вхідна напруга логічного нуля U1L, В ..... ≤ 0,8

Вхідна напруга логічного одиниці U1H, В .....≥ 2,0

Струм споживання від джерела живлення ICC, мА. ...≤ 160

Вихідний струм витоку I0Z, мкА. .....≤ 50

Час затримки tI0, нс .....≤ 40

Також до мікропроцесорній комплекту входить системний контролер. Так як мікропроцесор КР1821ВМ85 спільний з комплектом КР580, то підходить системний контролер КР580ВК28. Він призначений для формування сигналів. Таких як INTA, MEMR, MEMW, IO / R, IO / W і передачі даних від МП і до нього.

У таблиці 5.3 наведено призначення виводів системного контролера КР580ВК28.

Таблиця 5.3 - Призначення виводів системного контролера КР580ВК28

Позначення виводу	Номер контакту	Призначення виведення
D(7-0)	8,21,19,6, 10,12,17,15	Входи / виходи даних
STSTB	1	Строб стану від ГТВ

DBIN	4	Вхід сигналу «прийом» від МП
WR	3	Вхід сигналу «видачі» від МП
HLDA	2	Вхід сигналу «підтвердження захоплення» від МП
DB(7-0)	7,20,18,5, 9,11,16,13	Входи / виходи інформаційної системної шини
MEMR	24	Читання пам'яті
MEMW	26	Запис в пам'ять
I/OR	25	Читання з ВУ
I/OW	27	Запис в ВУ
BUSEN	22	Дозвіл роботи шини
Ucc	28	Напруга живлення
GND	14	Земля

Основні електричні параметри мікросхеми КР580ВК28:

Вихідна напруга L-рівня U0L, В:

- на шині D (7-0) .....≤ 0,45
- на всіх інших виходах ..... ≤ 0,45

Вихідна напруга H-рівня U0H, В:

- на шині D (7-0) .....≥ 3,6
- на всіх інших виходах .....≥ 2,4

Струм споживання від джерела живлення ICC, мА. .....≤ 190

Прямий вхідний струм Ib, мкА:

- на вході STSTB .....≤ 500
- на всіх інших виходах .....≤ 250

Зворотний вхідний струм II, мкА:

- на вході STSTB .....≤ 100
- на всіх інших виходах .....≤ 100

На малюнку 4.3 представлено позначення системного контролера КР580ВК28 на принциповій схемі.

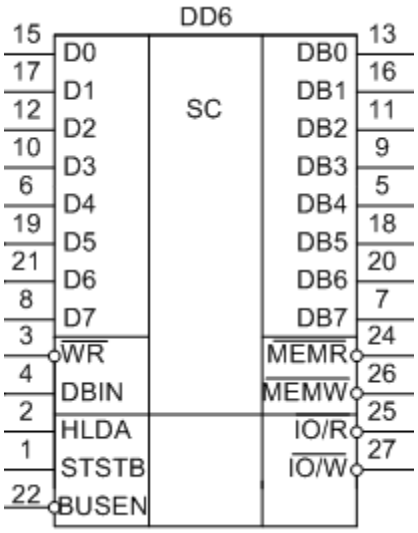


Рисунок 5.3 - Позначення на принциповій схемі системного контролера КР580ВК28

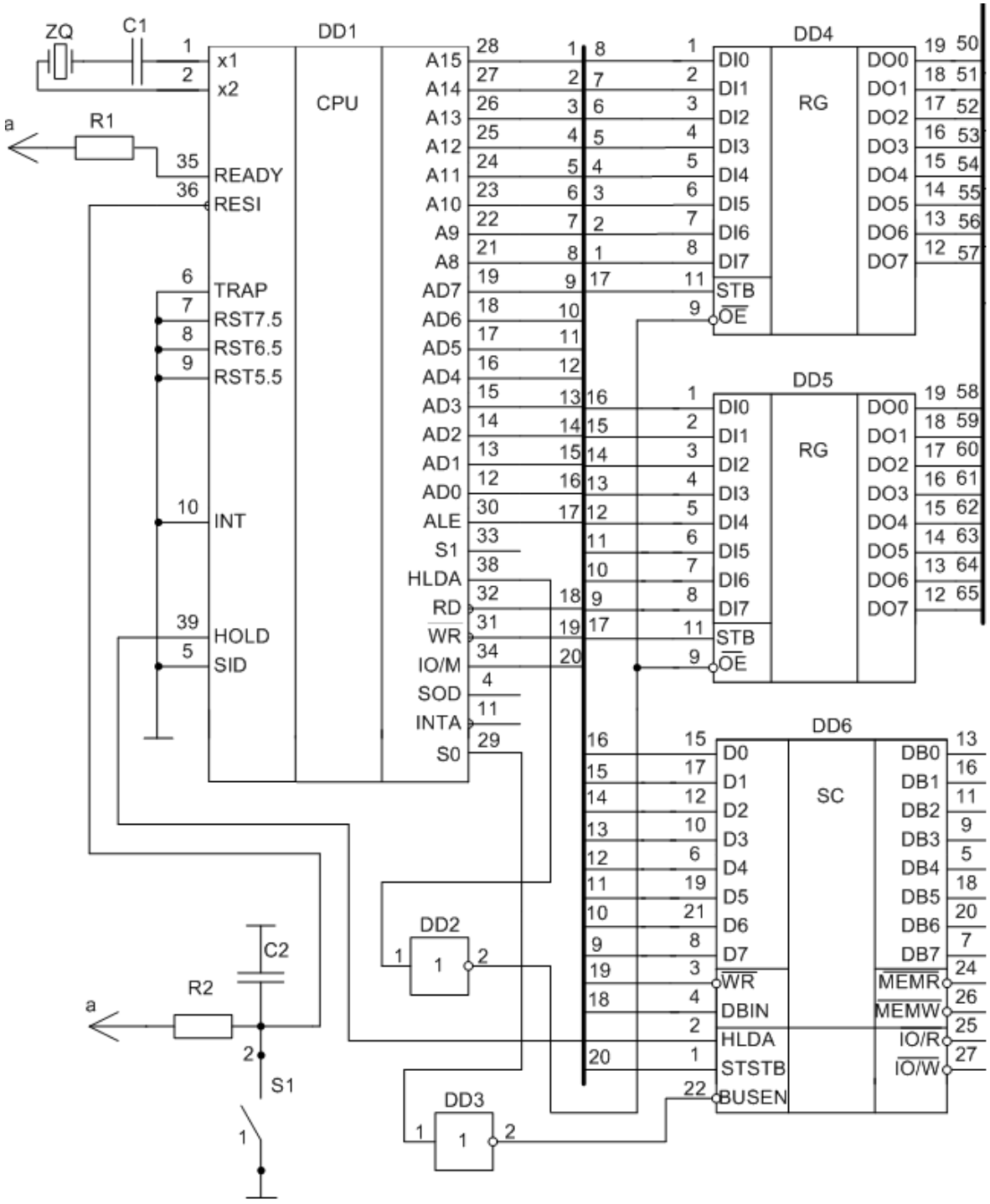


Рисунок 5.4 - Позначення на принциповій схемі МПБ

5.2 Блок пам’яті

Обсяги ПЗУ, який необхідній для реалізації поставлених завдань - невеликий, і тому може буть реалізовано на базі однієї мікросхеми пам'яті типу К573РФ5, який має організацію 2к * 8.

У таблиці 5.4 наведено призначення виводів ПЗУ К573РФ5

Таблиця 5.4 - Призначення виводів ПЗУ К573РФ5

№ виведення	Позначення	Призначення
8-1,23,33,19	A0-A10	Шина адрес
18	CS	Вибір мікросхеми
20	OE	Дозвіл передачі
9-16	D0-D7	Мультиплексована шина даних
24	Ucc	Напруга живлення

На рисунку 5.5 представлено позначення ПЗУ К573РФ5 на принциповій схемі.

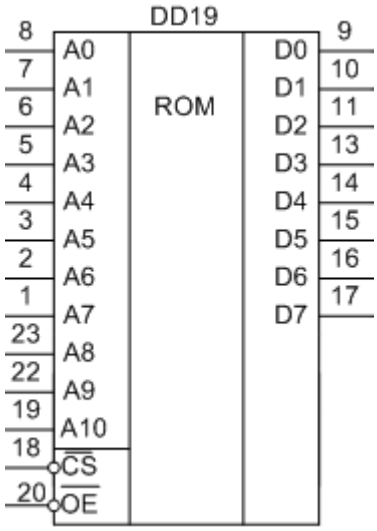


Рисунок 5.5 – Позначення на принциповій схемі ПЗУ К573РФ5.

Для зберігання одного зашифрованого 8-ми розрядного зображення розміром 640 * 480 необхідно ОЗУ розміром 300 Кбай. Повністю підходить по умові і параметрам мікросхема ОЗУ КМ185РУ8. Вона має обсяг 512Кбайт, і повністю сумісна з МП комплектом.

Рисунку 5.6 - Представлено позначення ОЗУ КМ185РУ8 на принциповій схемі.

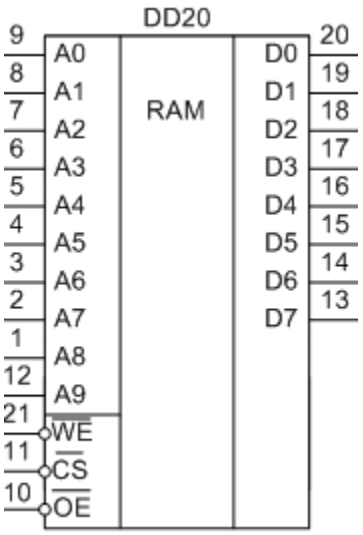


Рисунок 5.6 – Позначення на принциповій схемі ОЗУ КМ185РУ8

У таблиці 5.5 наведено призначення виводів КМ185РУ8

Таблиця 5.5 - Призначення виводів мікросхеми КМ185РУ8

№ виводу	Позначення	Призначення
9-1, 12	A0-A9	Адресні входи
11	CS	Вибір мікросхеми
21	WR	Запис / читання
20-13	D0-D7	Входи / виходи даних
10	OE	Сигнал дозволу зчитувати
24	Ucc	Напруга живлення
23	GND	Земля

Селектор адрес пам'яті побудований на таких елементах: логічне додавання (АБО), логічне множення (І), логічне заперечення додавання (АБО-НЕ) і логічне заперечення множення (І-НЕ).

На рисунку 5.7 представлено позначення селектора адрес пам'яті на принциповій схемі.

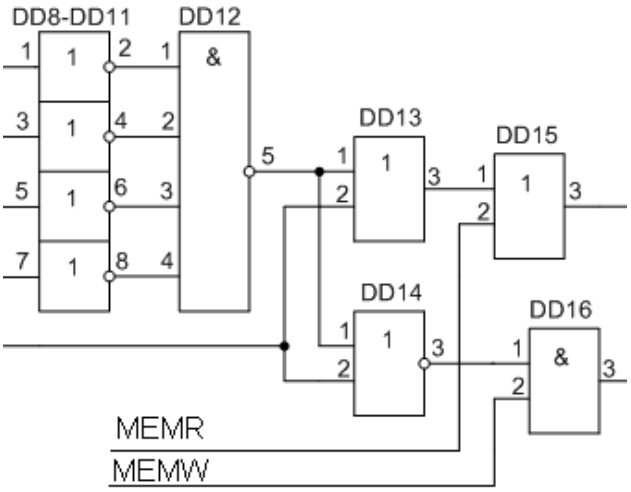


Рисунок 5.7 – Позначення на принциповій схемі селектора адрес пам'яті

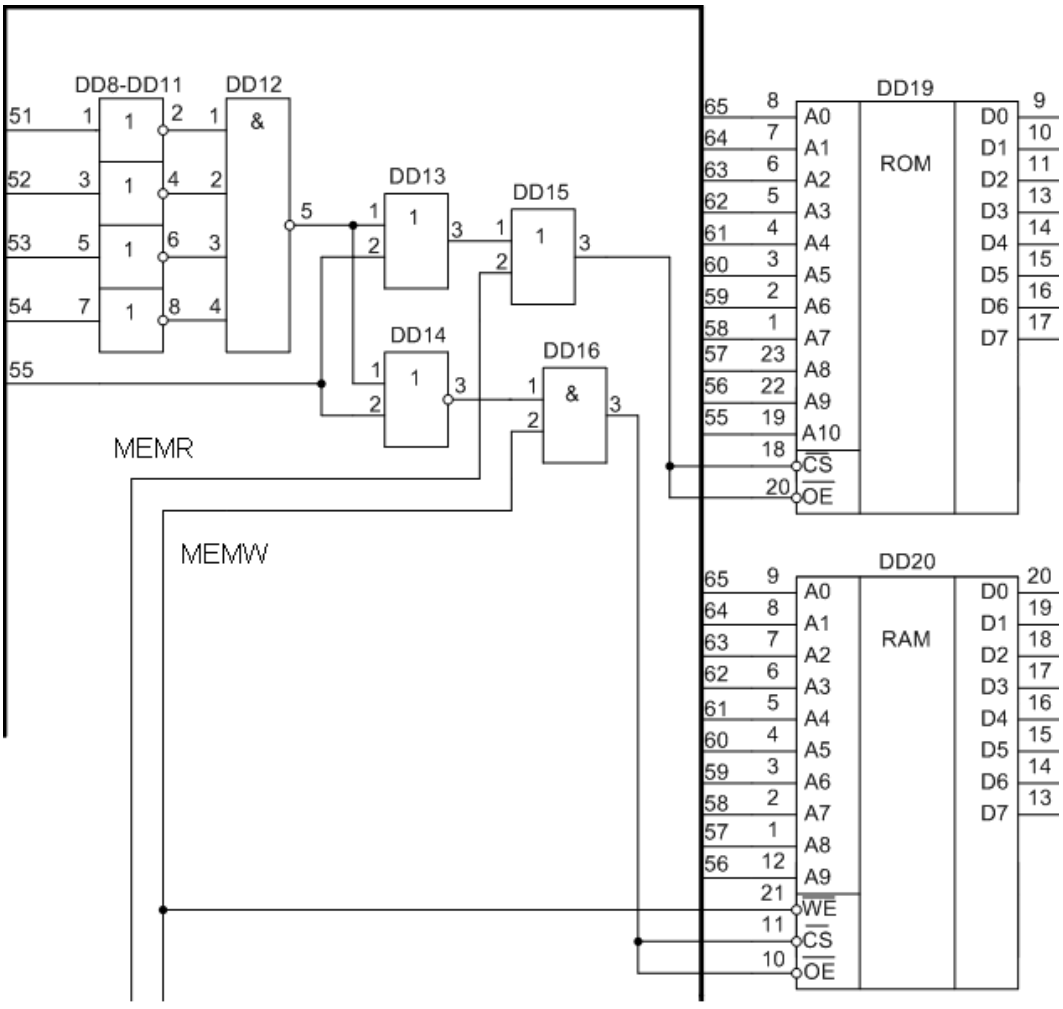


Рисунок 5.8 – Позначення на принциповій схемі блоку пам'яті

5.3 Інтерфейсний блок

Для реалізації інтерфейсного блоку можна використовувати інтегральну мікросхему паралельного інтерфейсу КР580ВВ55.

Програмований паралельний інтерфейс КР580ВВ55 призначенний для запровадження виводу паралельної інформації різного формату, що дозволяє реалізувати більшість відоміх протоколів обміну по паралельних каналах.

На рисунку 4.9 представлено позначення КР580ВВ55 на принциповій схемі.

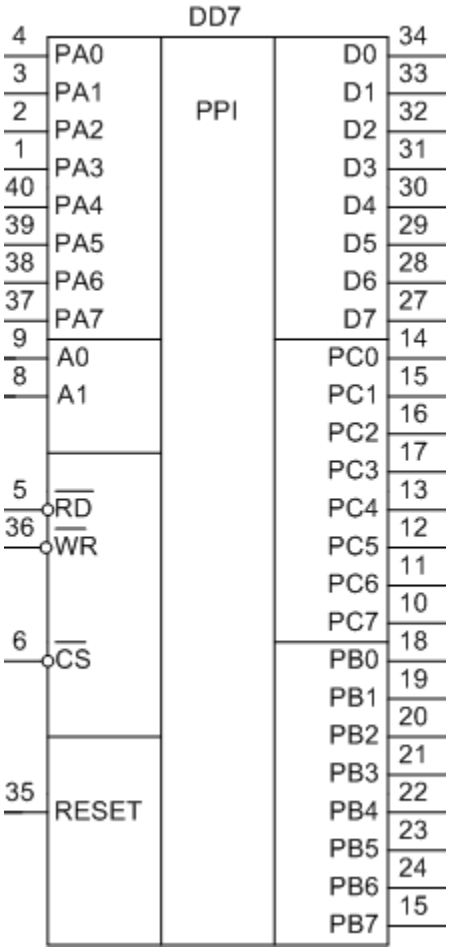


Рисунок 4.9 – Позначення на принциповій схемі КР580ВВ55

До складу паралельного інтерфейсу входять:

а) двонаправлений 8-розрядний буфер даних, що з'єднує лінії даних інтегральної мікросхеми з системною шиною даних;

б) блок управління читанням / записом, що забезпечує управління зовнішньої і внутрішньої передачею даних і керуючих слів;

в) три восьми розрядні порти вводу-виводу (РА, РВ, РС), призначені для обміну інформацією при чому порт З поділений на 4-розрядні полупорти: С` (РС7-РС4), і С`` (РС3-РС0). Основні електричні параметри мікросхеми КР580ВВ55

Вихідна напруга логічного нуля U0L, В ..... ≤ 0,4

Вихідна напруга логічної одиниці U0H, В ..... ≥ 2,4

Струм споживання від джерела живлення ICC, мА.....≤ 60

Вихідний струм витоку I0Z, мкА.....≤ 50

Час затримки tI0, нс ..... .≤ 40

Струм витоку каналів А, В, С, D при невибраному режимі II0Z, мкА - 100

Струм витоку на керуючих входах IIL, мкА ....- 10, ... 10

Призначення входів і виходів мікросхеми КР580ВВ55 наведено в таблиці 4.6.

Таблиця 4.6 - Призначення виводів паралельного інтерфейсу на базі мікросхеми КР580ВВ55.

№ виводу	Позначення	Призначення
27-34	D0-D7	Входи / виходи даних
37-40,1-4	PA0-PA7	Канал А
15,18-24	PB0-PB7	Канал В
10-17	PC0-PC7	Канал З
35	RESET	Скидання
8,9	A0,A1	Входи для адресації внутрішніх регістрів
5	RD	Читання
36	WR	Запис
6	CS	Вибір мікросхеми
26	Ucc	Напруга живлення
7	GND	Земля

У таблиці 4.7 представлені керуючі сигнали

Таблиця 4.7 - Операції задаються керуючими сигналами

Операція	Сигнали управління				
Запис керуючого слова з МП	0	1	0	1	1
Запис в канал А	0	1	0	0	0
Запис в канал В	0	1	0	0	1
Запис в канал З	0	1	0	1	0
Читання з каналу А	0	0	1	0	0
Читання з каналу У	0	0	1	0	1
Читання з каналу З	0	0	1	1	0
Відключити від D (7-0)	1	X	X	X	X

5.4 Блок відображення інформації

Для проектування блоку відображення інформації (БВІ) треба визначитися з наступними параметрами:

а) число L знакомісць (кількість десяткових розрядів індикатора).

б) мінімальна сила світла елемента індикатора;

в) мінімальна висота h елемента відображення інформації.

В якості індикаторів я використовував 7-ми сегментні індикатори АЛС324, що складається з семи лінійних сегментів, розташованих у вигляді цифри вісім, Включаючи необхідний сегмент в коло проходження струму, відбувається його засвічення, якщо ж засвітити групу сегментів, можна згенерувати зображення певного символу. Лінійні шкали виконані на основі інтегральних світлодіодів і являють собою мікросхеми утворені послідовно з'єднаними світлодіодними сегментами, які включаються пристроєм управління.

На рисунку 4.10 представлено позначення семисегментний індикатора АЛС324.

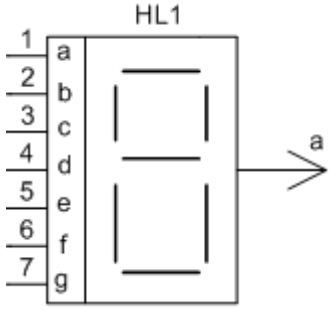


Рисунок 4.10 – Позначення на принципіальній схемі АЛС324

В таблиці 4.8 наведені технічні параметри мікросхеми АЛС324

Таблиця 4.8 – Параметри семисегментний індикатора АЛС324

Колір світіння	Красний
Довжина Хвилі, нм	660
Мінімальна сила світла Iv хв., Мкд	0.15
Максимальна сила світла Iv макс., Мкд	0.45
При струмі Iпр., МА	20
Кількість сегментів	7
Кількість розрядів	1
Схема включення	Общ.анод
Висота знака, мм	7.5
Максимальна пряма напруга, В	2.5
Максимальна зворотна напруга, В	5
Максимальний прямий струм, мА	25
Максимальний імпульсний прямий струм, мА	300
Робоча температура, С	-60…70

Вибір сегмента здійснюється за помощью дешифратора. Для реалізації цієї функції повністю підходить дешифратор К514ИД2. Він может працювати зі світлодіодними індикаторами при напрузі 9-12 вольт.

На рисунку 4.11 представлено позначення дешифратор К514ИД2.

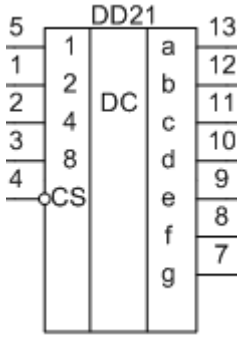


Рисунок 4.11 – Позначення на принциповій схемі ДШ К514ИД2

Основні електричні параметри мікросхеми ДШ К514ИД2:

Струм навантаження на кожному виході, мА 22

Напруга джерела живлення. В, не більше 5,25

Вихідна напруга. В, не більше 5,25

Напруга на кожному виході, В 6

Призначення виводів дешифратора К514ІД2 приведено в таблиці 4.9.

Таблиця 4.9 - Призначення виводів дешифратора К514ІД2

№ вивода	Позначення виводів	Функціональне призначення виводів
4	CS	Активація мікросхеми
7,1,2,6	1,2,4,8	Дані
13,12,10,9,16,15	a-g	Вихідний код

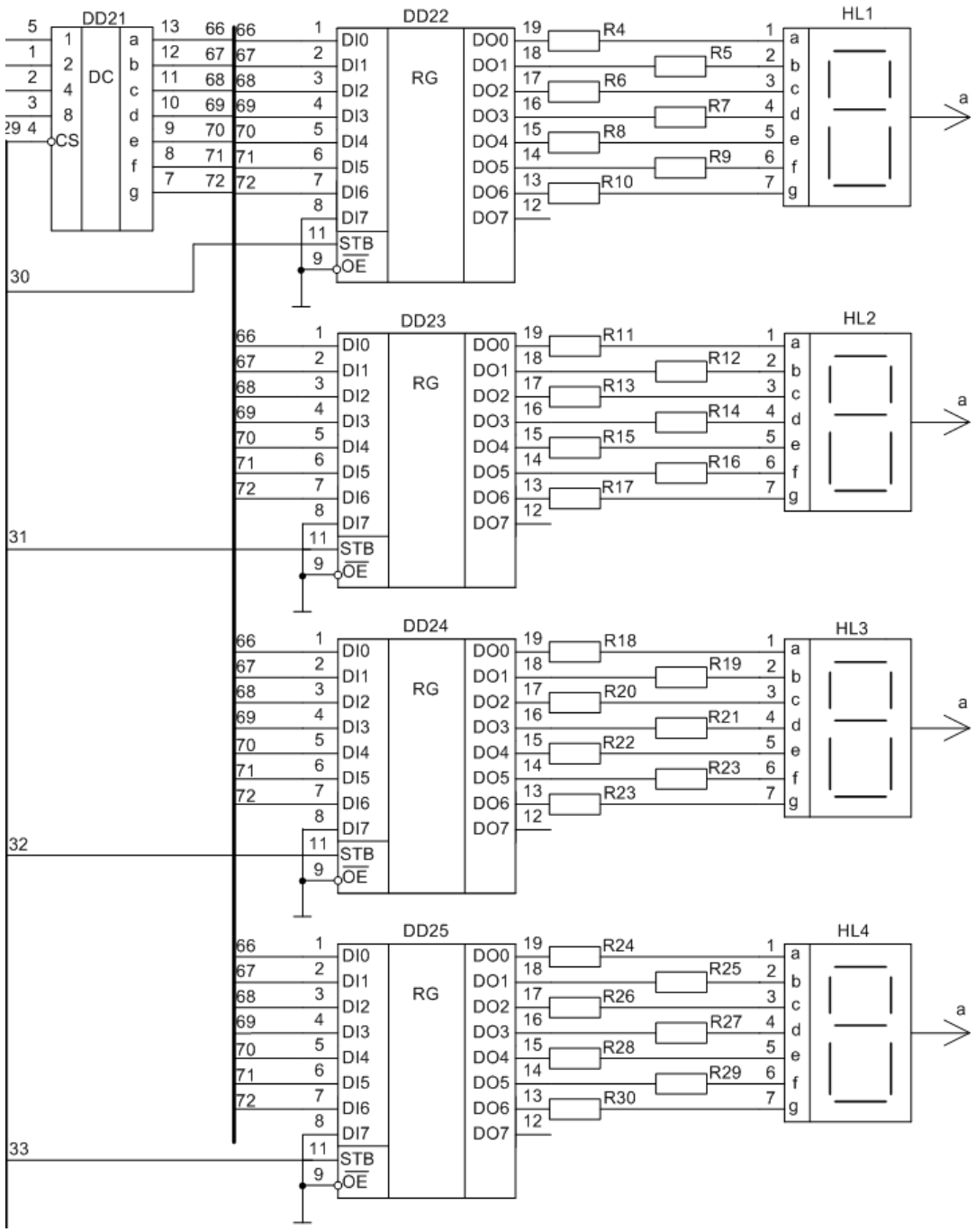


Рисунок 4.12 - Позначення на принциповій схемі

6.РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРИСТРОЮ

6.1 Розроблення алгоритму багатобайтового складання

Алгоритм програми багатобайтового складання.

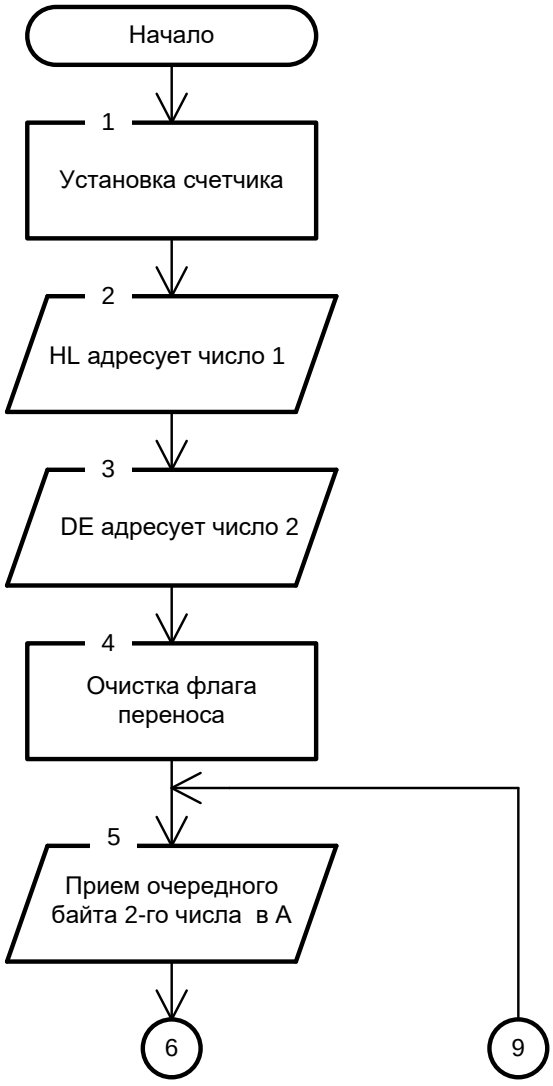
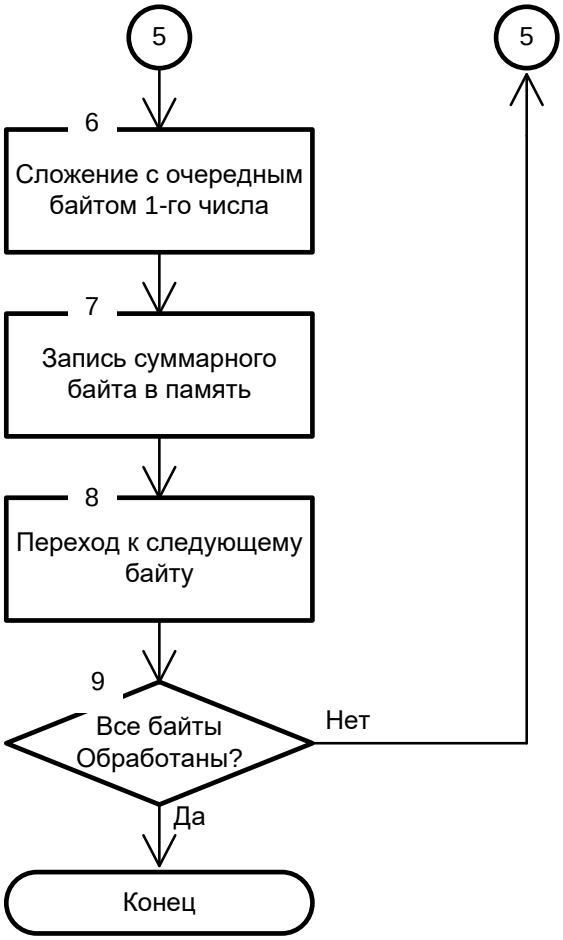


Рисунок 6.1 – Алгоритм програми багатобайтового складання



Продовження рисунка 6.1 - Алгоритм програми багатобайтові складання

6.2 Опис програми багатобайтові складання.

Етап 1 - відбувається встановлення лічильника, в регістр завантажується кількість пікселів зображення, яке необхідно зашифрувати.

Етап 2 - в реєстрову пару HL завантажується перший піксель.

Етап 3 - в реєстрову пару DE завантажується перший піксель.

Етап 4 - очищається вміст акумулятора.

Етап 5 - починається цикл складання, і в акумулятор завантажується другий піксель.

Етап 6 - додавання другого пікселя з першим і перенесення від складання попередніх пікселів.

Етап 7 - збереження результату в пам'ять.

Етап 8 - перехід до наступного пікселя для виконання операції додавання.

Етап 9 - виконується перевірка умови чи пікселі оброблені. Якщо умова не

виконується, то програма переходить до виконання пункту 5, а якщо виконується, то програма завершує роботу в підпрограмі багатобайтові складання.

6.3 Частина лістингу програми

Підпрограма багатобайтові складання:

```
; початкові установки
MSUM:   MVI B,N     ; установка лічильника
        LXI H,C1    ; HL адресує число 1
        LXI D,C2    ; DE адресує число 2
        XRA A       ; очищення флага переносу

; цикл складання
M1:     LDAX D      ; прийом чергового байта 2-го числа в A
        ADC M       ; складання з черговий байтом 1-го числа
                    ; і перенесенням від складання попередній байт
        MOV M,A     ;  запис сумарного байта в пам'ять
        INX H       ; перехід до наступного байту
        INX D
        DCR B       ; всі байти оброблені?
        JNZ M1      ; ні – продовжить работу
        RET         ; да – кінец.
```

Підпрограма перетворення до семіразрядний числу

```
lda Result                  ; прочитать мол. байт результата;
mov c, a                    ; сохранить цого в C;
lda Result+1                ; прочитать ст. байт результата;
                Continue:
rrc                         ; здвиг аккумулятора вправо;
jnc NoShift                 ; якщо не було переноса – перейти на
```

```
                                    ; NoShift
mov d, a                            ; сохранить ст. байт в D;
mov a, c                            ; загрузить мол. байт;
rrc                                 ; здвиг мол. байта;
ori 10000000B                       ; установить старший біт;
mov c, a                            ; вернуть в C;
mov a, d                            ; восстановить ст. байт в A;
                    NoShift:
cpi 0                               ; провірить A на 0;
jnz  Continue                       ; якщо A ≠ 0 перейти на  Continue;
                    Exit:
mov a, c                            ; записать в A мол. байт результата;
rrc                                 ; здвинуть вправо;
```

7. ЕКОНОМІЧНА ЧАСТИНА

7.1 Розрахунок собівартості та оптової ціни пристрою, що розроблюється

7.1 Розрахунок собівартості. В процесі виробництва будь-якого виробу споживаються різні матеріали, комплектуючі вироби, використовуються різні види обладнання та інструменти, проводиться велика кількість технологічних операцій [18]. У зв'язку з цим для обліку фактичних витрат на виробництво та для обґрунтування собівартості необхідна певна класифікація цих витрат. Для розрахунку собівартості одиниці певного виду продукції, що випускається, застосовується класифікація за калькуляційними статтями витрат. У плануванні та в обліку собівартості продукції застосовується наступне типове групування за статтями калькуляції:

- основна заробітна плата;
- додаткова заробітна плата;
- відрахування від заробітної плати;
- матеріали та комплектуючі;
- витрати на утримання та експлуатацію обладнання;
- виробничі витрати;
- адміністративні витрати;
- позавиробничі витрати (комерційні витрати) [18].

Групування витрат по калькуляційних статтях витрат дозволяє визначити рівень собівартості виробу, а відповідно й рівень його ціни. Вона характеризує місце виникнення витрат та їх цільове призначення.

Вихідними даними для складання калькуляції собівартості на проектований пристрій є стаття калькуляції на покупні та комплектуючі вироби. Необхідно врахувати вартість напівфабрикатів, що йдуть на виготовлення друкованої плати.

Дані по цій статті витрат приведені в таблиці 7.1

Таблиця 7.1 - Дані на покупні та комплектуючі вироби

Найменування комплектуючих	Кількість	Ціна однієї одиниці,(грн.)	Сума на один виріб (грн.)
1	**2**	**3**	**4**
Мікросхеми			
КР1821ВМ85А	1	170	170
КР580ИР82	2	40	80
КР580ВК28	1	65	65
КР580ВВ55	1	60	60
К573РФ5	1	35	35
RM185РУ8	1	140	140
К514ИД2	1	70	70
КР580ИР82	4	130	520
Конденсатори			
К50-6 25В 100мкФЖО.464.031ТУ	3	15	45
Резистори			
МЛТ-0.125-'7500м+5%ГОСТ7113-83	1	2	2
МЛТ-0.125-1.5кОм+5%ГОСТ7113-83	1	4	4
МЛТ-0.5-7500м+5%ГОСТ7113-83	1	2	2
МЛТ-0,125-2200м+5%ГОСТ7113-83	27	2	54
Індикатор			
АЛС324	1	190	190
Витратні матеріали			
Гетінакс(двосторонній)	100 $см^2$	40	40
Розєм 2РМГе0.364.126ТУ	2	30	60
Припой, флюс і др.		20	20
Загальна вартість, (грн.)			**1557**

Витрати на основну заробітну плату (Зо):

$$З_о = Т * Г * К * А, \quad (7.1)$$

де Т – сумарна трудомісткість розробки продукту (годин), яка визначається експертним шляхом виходячи з фактично витраченого часу на виробництво та налаштування продукту, Т = 8 (годин);

Г – середня годинна тарифна ставка одного робітника задіяного у виробництві продукту, грн. / год, Г = 60 грн. / год;

К – коефіцієнт трудової участі (розрядності), К = 1,3;

А – кількість працівників задіяних у виробництві, А = 2.

Тоді

$$З_о = Т * Г * К * А = 8*60*1,3*2 = 1248 \text{ (грн.)}.$$

Додаткова заробітна плата (10 – 30% від $З_о$):

$$З_д = З_о * К_д/100, \quad (7.2)$$

де $К_д$ – відсоток додаткової заробітної плати, $К_д$ = 10%.

$$З_д = З_о * К_д/100 = 1248*(10\%/100) = 124,80 \text{ (грн.)}.$$

Нарахування на заробітну плату – єдиний соціальний внесок у розмірі 22%.

$$Н_в = (З_о + З_д) * 22/100. \quad (7.3)$$

$$Н_в = (1248+124,8) * 22/100 = 302,02 \text{ (грн.)}.$$

Витрати на утримання та експлуатацію обладнання.

Оренда машинного часу ($О_м$):

$$О_м = М_в * Ч_м, \quad (7.4)$$

де $М_в$ – величина машинного часу, необхідного для розробки та налагодження продукту, годин, $М_в$ = 1дн * 8ч = 8 годин;

$Ч_м$ – вартість оренди машинного часу, грн. / год:

$$Ч_м = Ц_{еом} / Н_р * 259 * 8, \quad (7.5)$$

де $Ц_{еом}$- ціна обладнання, задіяного при виробництві виробу,

$Ц_{еом}$ = 35000 грн;

$Н_р$ – термін ефективної роботи, $Н_р$ = 5;

259 – кількість робочих днів;

8 – тривалість зміни.

$$Ч_м = 35000/5*259*8 = 3,40 \text{ (грн./ч).}$$

Тоді

$$О_м = М_в * Ч_м = 8*3,4 = 27,20 \text{ (грн.).} \quad (7.6)$$

7.2 Загальновиробничі витрати.

Являють собою витрати, що пов'язані з управлінням підрозділом, витрати на службові відрядження співробітників підрозділу, амортизаційні відрахування від вартості основних фондів загальноцехового призначення і т.д.

Загальновиробничі витрати ($В_{зв}$) визначаються в розмірі 130-250% від основної заробітної плати.

$$В_{зв} = З_о * \% В_{зв} = 1248 * 1,3 = 1622,40 \text{ (грн.).} \quad (7.7)$$

Визначимо виробничу собівартість:

$$В_с = З_о + З_д + Н_в + М + О_м + В_{зв} =$$
$$= 1248 + 124,80 + 302,02 + 1557 + 27,20 + 1622,40 = 4881,42 \text{ (грн.).} \quad (7.8)$$

Адміністративні витрати можуть містити:

- витрати, пов'язані з управлінням підприємством;
- витрати на службові відрядження адміністрації підприємства;
- витрати на пожежну і сторожову охорону;
- витрати, пов'язані з підготовкою (навчанням) і перепідготовкою кадрів;
- витрати на перевезення працівників до місця роботи і назад;
- витрати на оплату відсотків за фінансові кредити, а також відсотків за товарні і комерційні кредити;
- витрати, пов'язані з оплатою відсотків за користування матеріальними цінностями, взятими в оренду (лізинг);
- витрати, пов'язані з оплатою послуг комерційних банків та інших кредитно-фінансових підприємств;
- податки, відрахування.

Адміністративні витрати ($В_а$) визначаються в розмірі 140 - 200% від основної заробітної плати.

$$В_а = З_о * \% В_а = 1248 * 1,4 = 1747,20 \text{ (грн.)}. \quad (7.9)$$

Витрати на збут ($В_з$). Включають витрати на рекламу і предреализационная підготовку пристрою. Орієнтовно ці витрати визначаються в розмірі 5 - 10% від виробничої собівартості.

Тоді

$$В_з = В_с * (5 – 10)\% = 4881,42 * 0,05 = 244,07 \text{ (грн.)}. \quad (7.10)$$

Повна собівартість пристрою (С):

$$С = В_с + В_а + В_з . \quad (7.11)$$

$$С = 4881,42 + 1747,20 + 244,07 = 6872,70 \text{ (грн.)}.$$

Калькуляція собівартості виробу зводиться в таблицю 7.2.

Таблиця7.2 - Калькуляція собівартості виробу, що розробляється

Найменування статей калькуляції	Величина, грн.
1. Основна заробітна плата	1248
2. Додаткова заробітна плата	124,80
3. Нарахування на заробітну плату	302,02
4. Матеріали та комплектуючі	1557
5. Оренда машинного часу	27,20
6. Загальновиробничі витрати	1622,40
7. Адміністративні витрати	1747,20
8. Витрати на збут	244,07
Разом повна собівартість	6872,70

7.3 Розрахунок ціни пристрою.

Розрахунок оптової ціни виробу проведемо за схемою «собівартість плюс прибуток»:

$$Ц_{опт} = С + П, \quad (7.12)$$

де С – собівартість пристрою;

П – величина прибутку.

Прибуток визначається виходячи з нормативу рентабельності виробництва продукції:

$$R = (П / С) * 100\%, \quad (7.13)$$

де R - рентабельність продукції (продукту), приймається в розмірі до 35%.

R = 10%.

Тоді оптова ціна:

$$Ц_{опт} = С + (R * С / 100) = 6872,70 +0,1*6872,70 = 7560 \text{ (грн.)}. \quad (7.14)$$

Визначимо роздрібну ціну розробленого виробу:

$$Ц_{розн} = Ц_{опт} * 1,2 = 7560 * 1,2 = 9072 \text{ (грн.)}, \quad (7.15)$$

де 20% ПДВ.

Позитивні сторони даної методики полягають в її простоті, комплексної очевидності такої функції ціни як відшкодування витрат на виробництво та забезпечення прибутковості від створення та реалізації пристрою. Недолік даної методики полягає в тому, що вона недостатньо враховує ринкові чинники ціноутворення й, перш за все, попит. Однак, у реальній перехідній економіці існують ситуації, коли підприємствам доцільно її застосовувати: в умовах відсутності конкуренції (монополії), при обмеженні рентабельності продукції з боку держави, виконанні одноразових замовлень, при виготовленні оригінальної продукції.

Необхідно відзначити, що для встановлення реальної ціни, яка б відповідала умовам існуючого ринку, необхідні відповідні маркетингові дослідження.

ВИСНОВКИ

У даному проекті було розроблено пристрій для захисту конфіденційної інформації, також описали актуальність даного пристрою в наш час.

Було розроблено алгоритм функціонування пристрою.

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

Розроблено електричну функціональну схему пристрою під розробкою функціональної схеми розуміється: визначення функціонального складу, що входить в мікропроцесорний контролер.

Для розроблення електричної принципової схеми оптимальним для розроблюваного проекту буде мікропроцесорний блок до якого входять процесор КР1821ВМ85А, два буферних регістра КР580ІР82, двонаправлений системний контролер КР580ВК28 , перевагами якого є:

- низька вартість;
- орієнтування на роботу в складі мікроконтролерів;
- програмна сумісність з мікропроцесором КР580ВМ80А;
- вбудований системний контролер;

ЛІТЕРАТУРА

1. Бережна О.В. Про особливості побудови адаптивних систем передачі інформації / О.В. Бережна, В.В. Арбузов, О.О. Сальніков, Д.В. Гриненко// Фізика, електроніка, електротехніка (ФЕЕ-2020). Матеріали та програма науково-технічної конференції. – Суми: СумДУ, 2020. - С.°136.
2. http://studfiles.net/preview/5993348
3. http://fotocom.at.ua/publ/ucheba/zakhist_konfidencijnikh_...ogo_dostupu/2-1-0-74
4. http://znaimo.com.ua/%D0%A8%D0%B8%D1%84%D1%80%20%D0%92%D1%96%D0%B6%D0%B5%D0%BD%D0%B5%D1%80
5. Журнал «Радиолюбитель» №5, 2002г.
6. Усатенко С. Т., Каченюк Т.К., Терехова М.В. Выполнение электрических схем по ЕСКД: Справочник – М.; Издательство стандартов, 1989.
7. Зубчук В.И. и др.: Справочник по цифровой схемотехнике.— К.: Техника, 1990.— 448 с.: ил.
8. Разработка и оформление конструкторской документации радиоэлектронной аппаратуры: Справочник Э. Т. Романычевой, - М.; Радио и связь, 1989.
9. http://robotrends.ru/pub/1812/roboty-ploho-zashisheny-ot-hakerov-i-eto-opasno-2018
10. Автоматизация производства и промышленная электроника. Том 1. Главные редакторы А.И. Берг и В.А. Трапезников. (Москва: Издательство «Советская Энциклопедия», 1962. – Серия «Энциклопедия современной техники. Энциклопедия. Словари. Справочникик»)
11. Автоматизированные ынформационные системы Под ред В.А. Ильина. М., изд. ВЗПИ, 1970. 359с.
12. http://allbest.ru/otherreferats/law/00165045_0.html
13. http://referat.co/ref/56100/read?p=8
14. https://knowledge.allbest.ru/programming/2c0b65635b2ac78b4d53b89521316d27_0

ДОДАТОК А

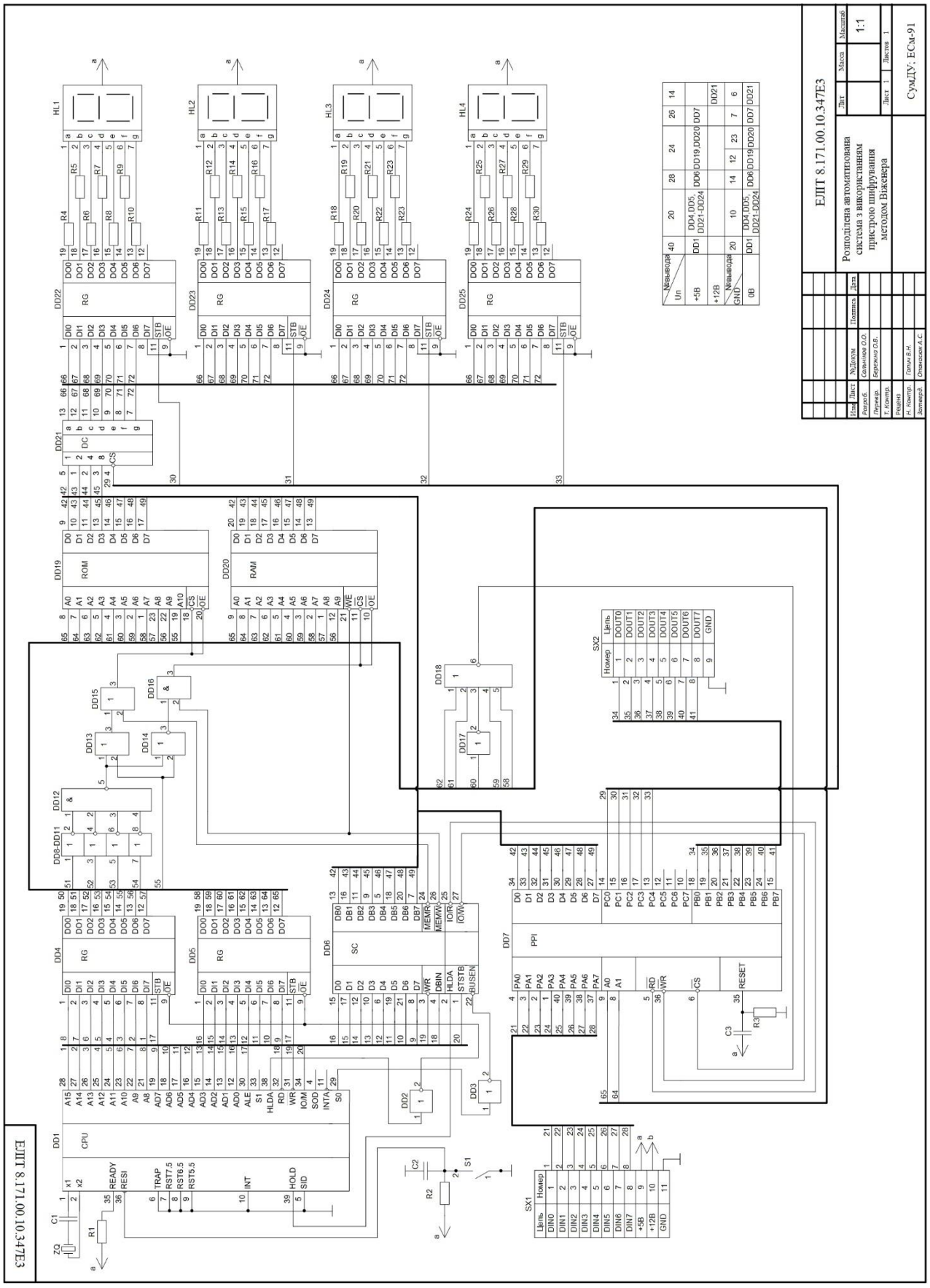


Рисунок 8.1 -Принципіальна схема пристрою

ДОДАТОК Б

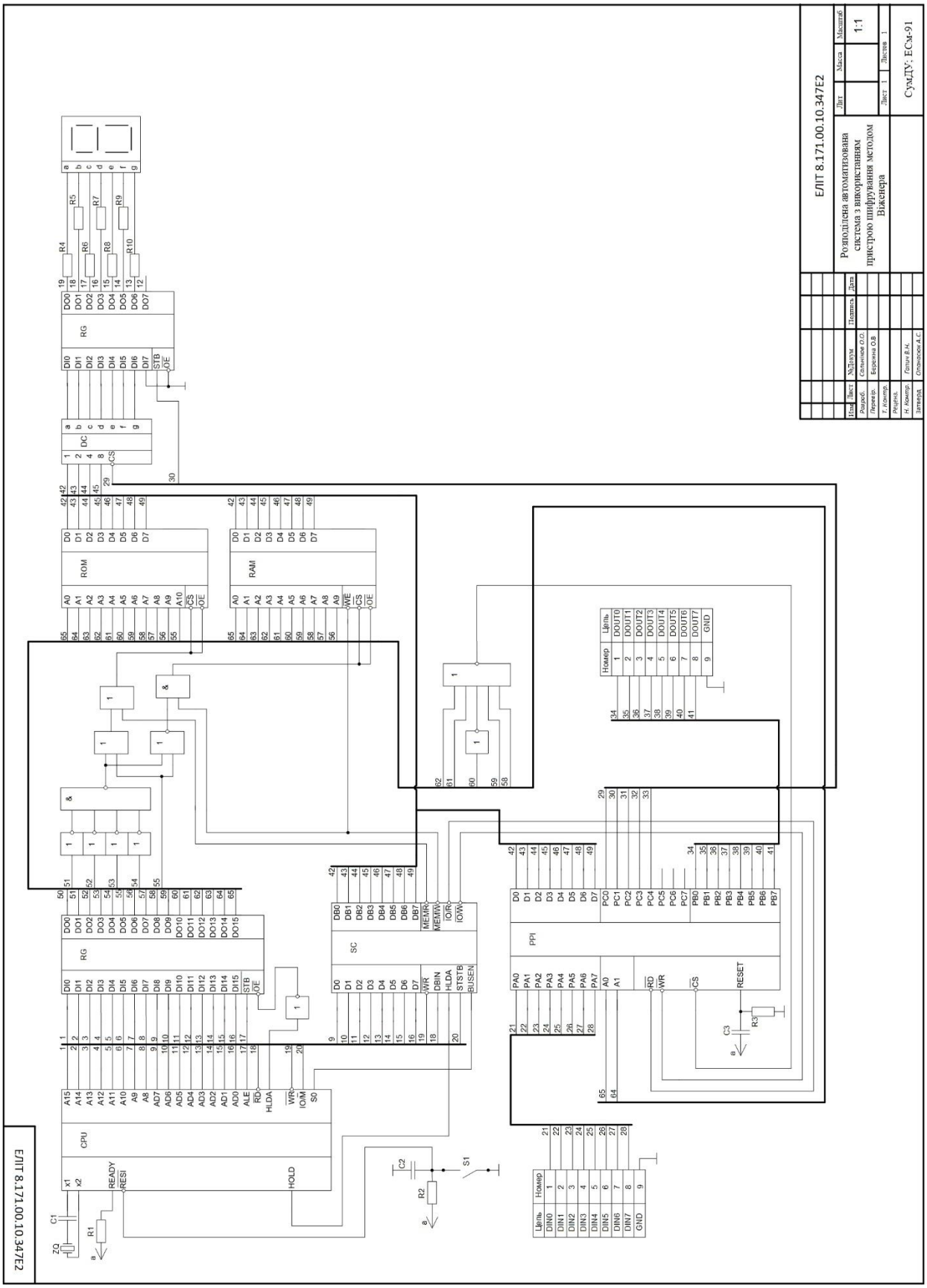


Рисунок 8.2 -Функціональна схема пристрою

ДОДАТОК В

Про особливості побудови адаптивних систем передачі інформації

Бережна О.В.[1], *доцент*; Арбузов В.В.[2], *генеральний директор*; Сальніков О.О.[1], *студент*; Гриненко Д.В.[1], *студент*
[1]Сумський державний університет, м. Суми, Україна
[2]Енергосервісне підприємство «Преобразователь», м. Суми, Україна

Найбільш важливими завданнями при побудові розподілених інформаційно-вимірювальних систем є забезпечення високої швидкості та достовірності інформації, що передається. З іншого боку, для індустріальних систем є характерним високий рівень спотворень в каналах зв'язку. Високий ступінь апріорної невизначеності та зміни в часі характеру та параметрів спотворень інформації ускладнюють застосування систем передачі інформації із заздалегідь визначеною структурою та параметрами. У такому випадку найбільш доцільним є використання адаптивних систем передачі інформації.

У роботі пропонується при виборі стратегії досягнення оптимальних параметрів передачі інформації застосовувати математичну модель системи передачі інформації з використанням алгоритмів оптимального оцінювання стану каналів зв'язку.

Дослідження та аналіз різних типів моделей спотворень та режимів передачі інформації показали, що при побудові узагальненої моделі системи передачі інформації на основі векторного перезапиту в умовах як стаціонарного, так і нестаціонарного каналу зв'язку доцільно застосовувати кусочно-стаціонарну модель потоку помилок зі змінними параметрами та біноміальним законом розподілу. Основною метою контролю стану каналу зв'язку є визначення номера та тривалості і-го стаціонарного стану каналу зв'язку з характерною для нього моделлю спотворення. Кожному і-му стану каналу приводиться у відповідність і-я ефективна структура системи передачі інформації з оптимальними параметрами.

Використовуючи результати проведених досліджень був розроблений алгоритм оцінювання стану каналу зв'язку, який дозволяє більш повно використовувати можливості адаптивної системи передачі інформації з векторним перезапитом та здійснювати передачу інформації з вибором вирішальної функції, яка мінімізує ризик, що виникає.