МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Кафедра електроніки і комп’ютерної техніки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи бакалавра на тему:

«Пристрій захисту конфіденційної інформації»

Завідувач кафедри А.С. Опанасюк

Керівник роботи О.В. Бережна

Студент групи О.О. Сальніков

Суми
2019 р.

РЕФЕРАТ

Пояснювальна записка містить: 37 аркушів, 19 рисунків, 12 джерел літератури.

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

Пояснювальна записка містить п’ять розділів: огляд літератури, розробку алгоритму функціонування пристрою та структурну схему, розробку функціональної та принципової схем пристрою та розроблення кодового забезпечення.

Перший розділ містить загальну інформацію про захист конфіденційної інформації.

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

Третій розділ присвячений розробці функціональної схеми пристрою.

Четвертий розділ присвячений розробленню принципової електричної схеми пристрою.

П’ятий розділ містить кодове забезпечення для мікропроцесору.

ЗМІСТ

					ЕЛІТ 6.05080202.347ПЗ		
Змн.	*Арк.*	*№ докум.*	*Підпис*	*Дата*			
Розроб.		*Сальніков О.О.*			Пристрій захисту конфіденційної інформації Пояснювальна записка	*Літ.*	*Арк.* 3 / *Акрушів* 37
Перевір.		*Бережна О.В,*					
Реценз.						СумДУ; ЕС-51	
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.

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 [2].

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.

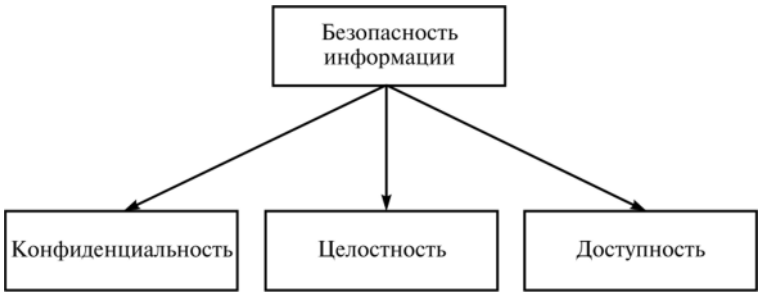

Рисунок 1.1 - Принцип захисту інформації

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.

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 [3].

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:

$$K = (k_1, k_2, ..., k_l)$$

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.

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 1.2.

Рисунок 1.2 - 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.

1.5 Захист промислових роботів від злому

Автоматизація виробництва - сучасний тренд, до 2018 року кількість роботів на фабриках в усьому світі досягне 1,3 мільйона. Однак експерти попереджають: промислові роботи практично беззахисні перед атакою хакерів. Зловмисники можуть без проблем зламати систему, що призведе до виходу з ладу в продукції, що виготовляється, зупинці виробництва або іншим серйозних наслідків.

Наукові співробітники Міланського технічного університету та японського розробника ПЗ для кібербезпеки Trend Micro провели дослідження того, наскільки сучасні роботи захищені від хакерів. Вони опитали 50 експертів робототехніки та безпеки, серед яких інженери ABB, KUKA, Comau, представники Industrial Robotics group в EU Robotics і інші.

Роботи стали найбільш уразливими з кількох причин:

- роботизовані системи підключили до корпоративних мереж;

- збільшилася кількість спільних роботів, які підключені до інтернет-мереж;
- багато операторів не усвідомлюють небезпеку кібератак і не приймають ніяких дій, щоб від них захиститися.

Щоб захистити роботів від злому потрібно проаналізувати всі варіанти кібератак, знайти в системі всі потенційні дірки безпеки. Організація TÜV Rheinland, яка займається технічним наглядом, привела список вимог для забезпечення безпеки роботів:

- перевірка системи безпеки робота;
- аналіз ризиків кібератак і моделювання загроз;
- створення Матриці відповідності вимог;
- огляд програмного забезпечення для безпеки;
- тестування робота для виявлення вразливих місць;
- виявлення компонентів, які можуть привести до злому системи;
- огляд ключових елементів управління безпекою;
- формування плану дій при кібератаки;
- правова і нормативна оцінка;
- оновлення програмного забезпечення і аналіз виправлень;
- огляд вразливих елементів конструкції.

Вхідні дані:

- шифр Віженера;
- три мови відкритого тексту - українська, російська, англійська;
- довжина шифрограми L - не більше ніж 124 символи;
- довжина ключа K - не менше ніж 32 символи.

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

2.1 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. Блок 1.

Крок 2. Введення команд для керування роботом. Блок 6.

Крок 3. Керування кроковим двигуном. Блок 9.

Крок 4. Місцезнаходження робота. Блок 8.

Крок 5. Вибір строки або введення символів, які потрібно зашифрувати і запис в блок пам’яті. Блок 12.

Крок 6. Перевірка тексту на символи. Блок 3.

Крок 7. Визначення мови тексту якого потрібно зашифрувати. Блок 10.

Крок 8. Виконується виправлення даного тексту. Блок 5.

Крок 9. Виконується генерація квадрата Віженера, для шифрування. Блок 11.

Крок 10. Виконується шифрування даного тексту. Блок 13

Крок 11. Формування рядка, в якому записується результат шифрування. Блок 14.

Крок 12. 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 2.1 - Табличне представлення шифру Віженера для Української мови

Дана таблиця призначена для шифрування інформації українського алфавіту.

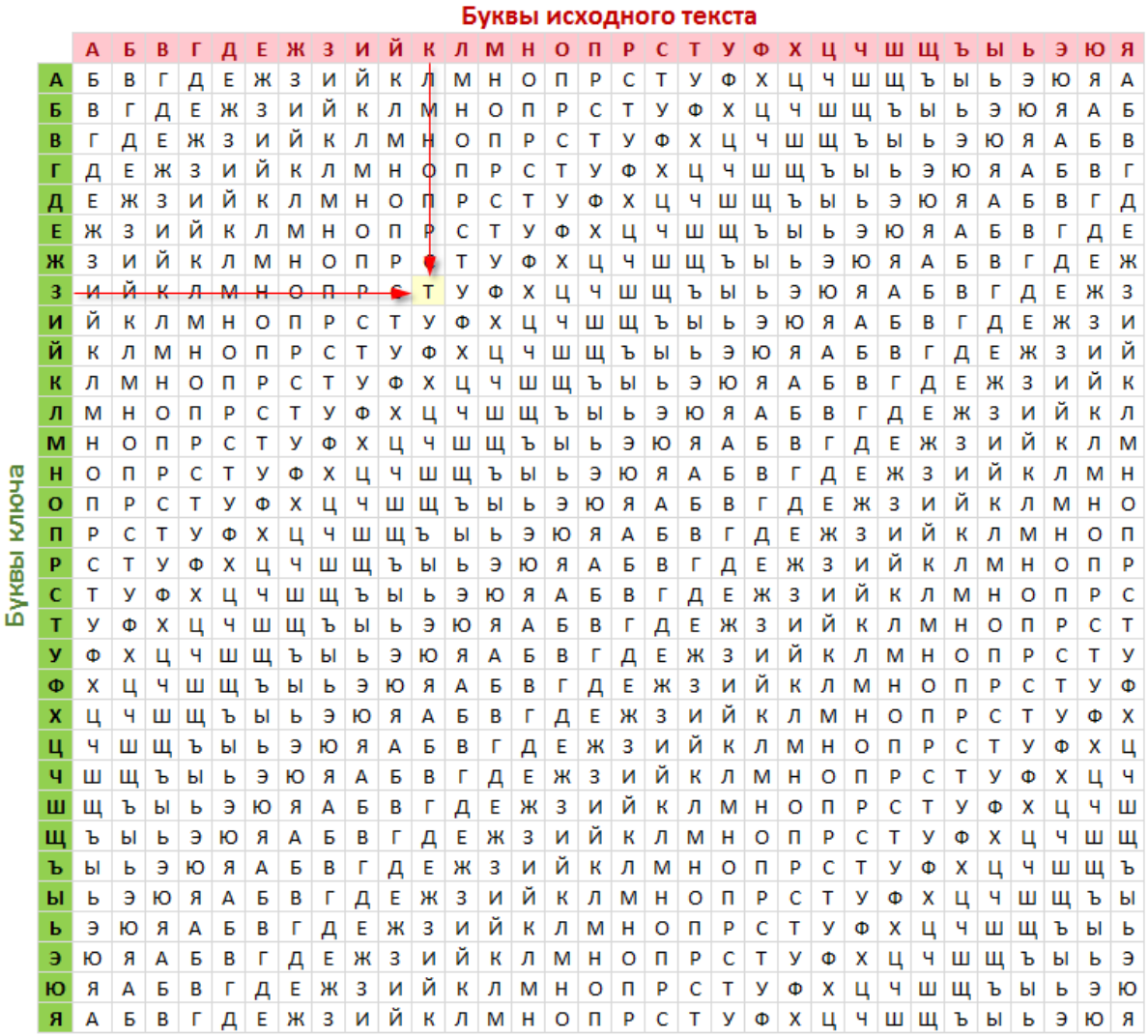

Рисунок 2.2- Табличне представлення шифру Віженера для Російської мови

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 2.3 - Табличне представлення шифру Віженера для Англійської мови

Дана таблиця призначена для шифрування інформації англійського алфавіту.

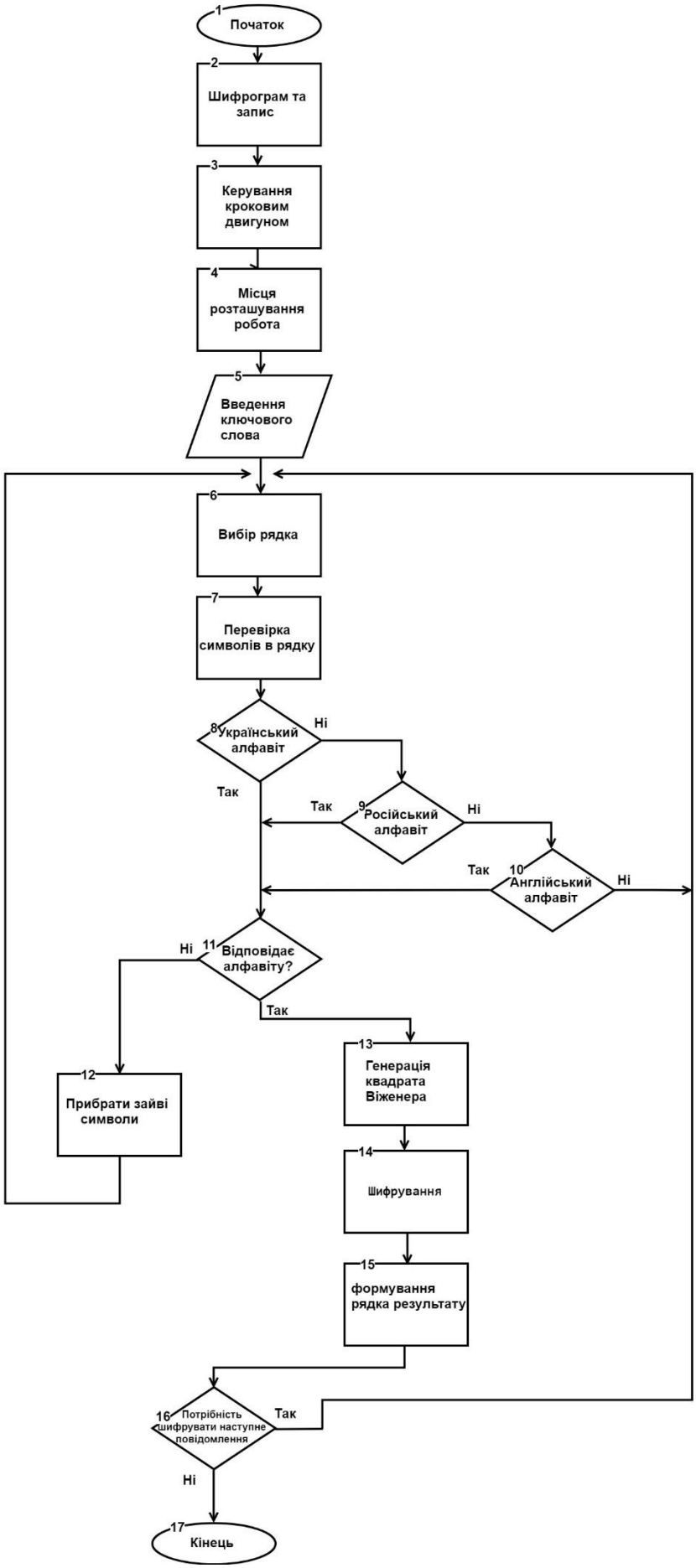

Рисунок 2.4 - Схема алгоритму роботи

2.2 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 2.5. представлена структурна схема пристрою.

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

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

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

Місце розташування робота - призначення місця для розташування робота.

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

Перевірка символів в рядку - блок, який виявляє помилки у рядку.

Аналіз - визначення мови, для тексту в рядку.

Заміна символів - блок, який виправляє помилки у рядку.

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

Керування кроковим двигуном - даний блок видає керуючі сигнали на кроковий двигун.

Квадрата Віженера - блок призначений для формування квадрата Віженера, для визначеної мови в рядку.

Пам'ять - блок призначений для запису інформації.

Шифрування - блок, який виконує шифрування даного тексту.

Шифрограмма - зашифрований текст.

Принцип роботи пристрою захисту конфіденційної інформації полягає в наступному:

1.Керування роботом здійснюється за допомогою пульта дистанційного керування роботом, який формує відповідні команди керування, шифрує їх за допомогою шифру Віженера та передає до робота за допомогою бездротового каналу зв'язку.

2. Отримані роботом зашифровані команди дешифруються за допомогою дешифратора, записуються до блоку пам’яті та через блок введення команд подається до виконання до блоку керування.

3. Блок керування забезпечує переміщення роботу за допомогою блока керування кроковими двигунами та блоку контролю місця розташування роботу.

4. Команди, що отримуються роботом, геометричні параметри приміщення, що експериментально визначаються роботом при первоначальному налаштуванні, маршрути переміщення робота мають статус конфіденційної інформації та підлягають шифруванню за допомогою шифру Віженера при передачі та зберіганні цієї інформації.

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

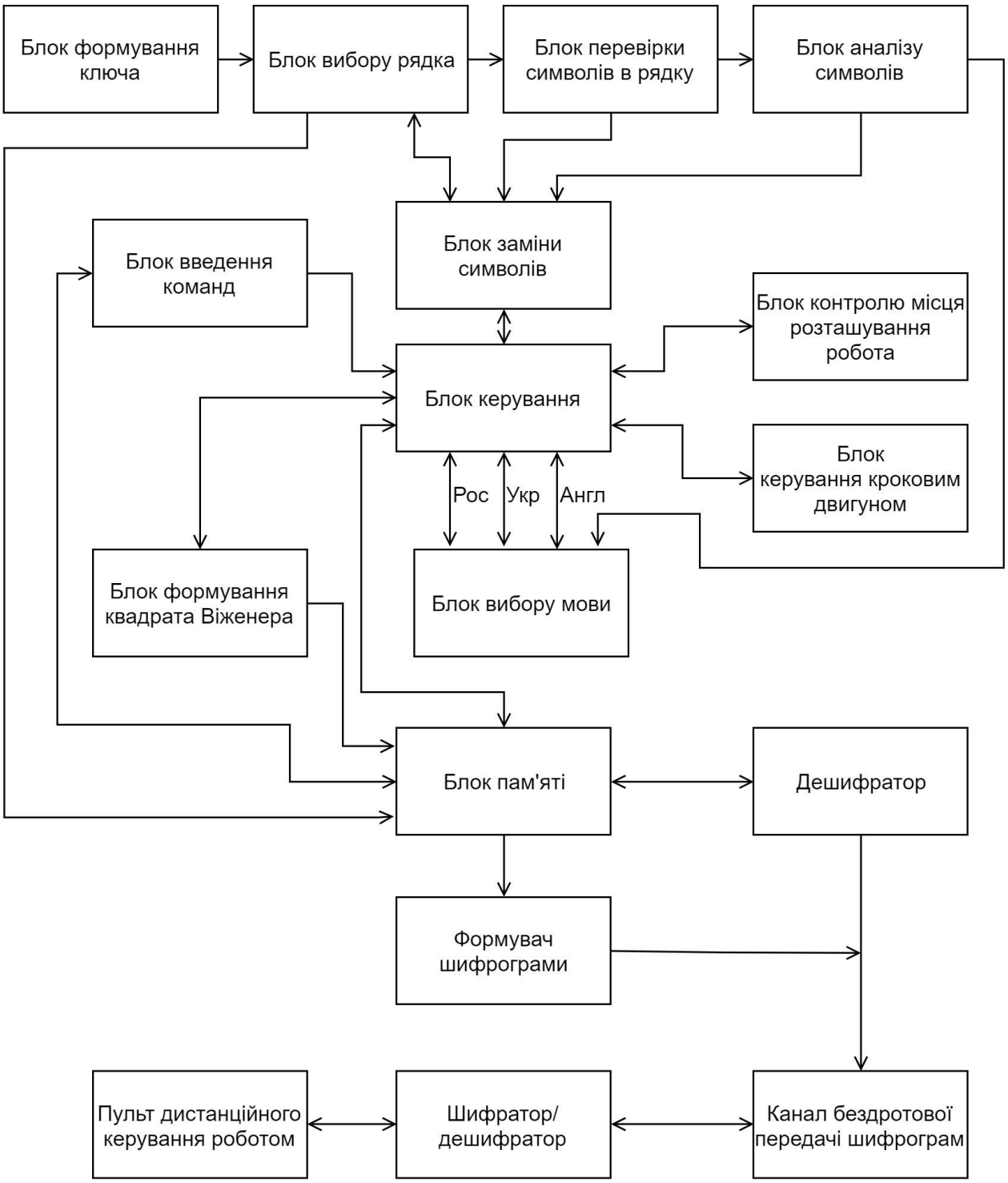

Рисунок 2.5 - Структурна схема пристрою захисту конфіденційної інформації

3. РОЗРОБЛЕННЯ СХЕМИ ЕЛЕКТРИЧНОЇ ФУНКЦІОНАЛЬНОЇ ПРИСТРОЮ

Під розробкою функціональної схеми розуміється: визначення функціонального складу, що входить в мікропроцесорний контролер; розрахунок і обгрунтування технічних вимог до вказаних блоків і встановлення необхідних електричних зв'язків між ними.

Мікроконтролер координує роботу всіх пристроїв цифрової системи за допомогою шини управління.

Для управління процесом перетворення і обчислення до складу проектованого пристрою повинен входити мікропроцесор.

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

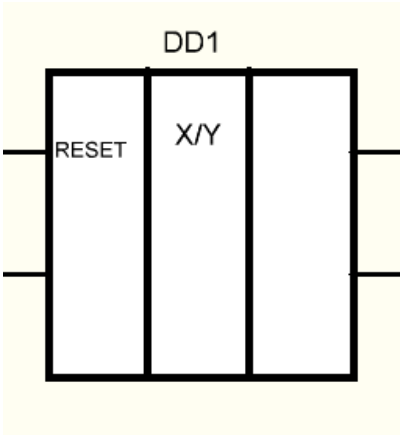

Рисунок 3.1 - Блок встановлення в початковий стан

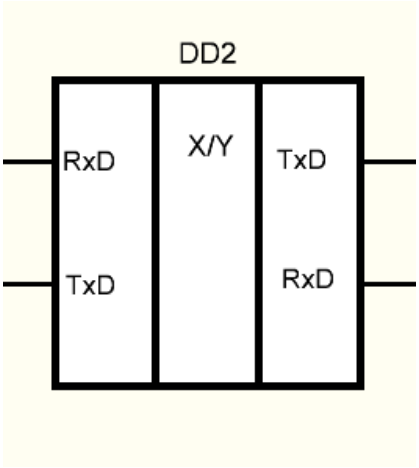

Рисунок 3.2 - Блок передачі команд

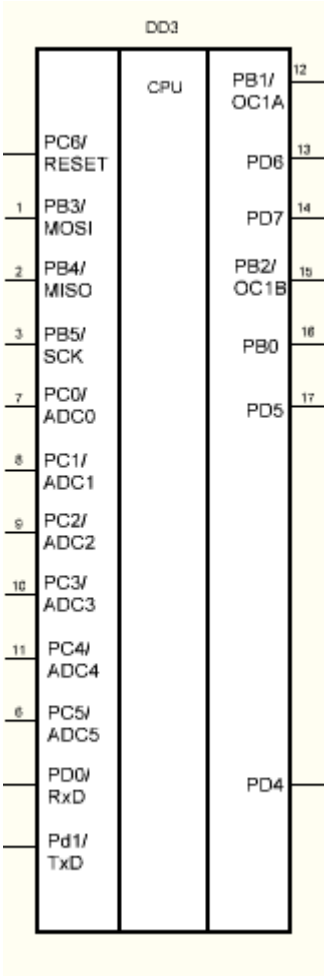

Рисунок 3.3 - Мікроконтролер

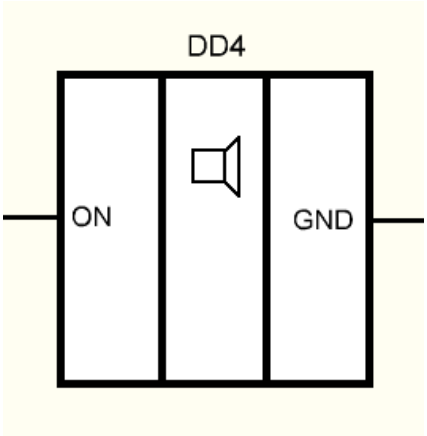

Рисунок 3.4 - Блок звукового сповіщення

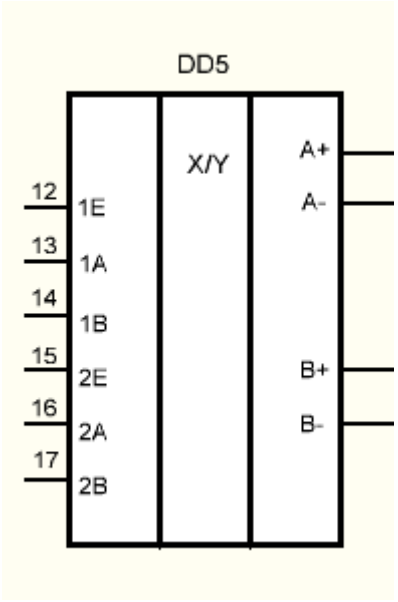

Рисунок 3.5 - Блок керування шаговим двигуном

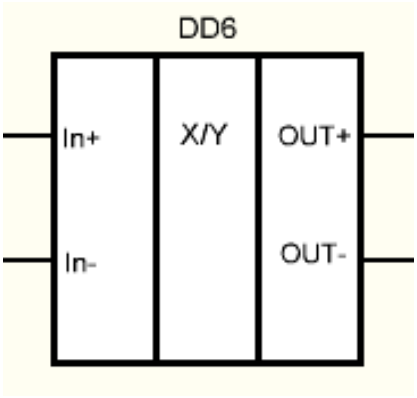

Рисунок 3.6 - Блок візуалізації дій робота

Схема електрична функціональна пристрою, що розробляється зображена в додатку Б.

4. РОЗРОБЛЕННЯ ПРИНЦИПОВОЇ ЕЛЕКТРИЧНОЇ СХЕМИ ПРИСТРОЮ

4.1 Вибір елементної бази

Для побудови пристрою стиснення даних необхідно вибрати серію мікросхем, на яких будуть реалізовані всі блоки пристрою.

Оптимальним для розроблюваного курсового проекту буде мікроконтролер Atmega8, перевагами якого є:

-низька вартість;

-високопродуктивний, що споживає мало енергії, 8-бітний мікроконтролер.

-32 восьмибітних регістри загального користування.

-Надійна незалежна пам'ять, побудована у вигляді декількох сегментів.

Мікроконтролер Atmega8 має 8-розрядний високопродуктивний AVR мікроконтролер з малим споживанням.

Мікросхема L293D використовується у якості драйвера двигунів, входи якої приєднані до виводів мікроконтролера так, як показано на схемі. На схемі входи драйвера двигунів L293D підключені до виводів порту С мікроконтролера Atmega8, але їх можна підключити до будь-якого з портів мікроконтролера. При цьому потрібно буде внести зміни в програмну частину, вказавши порт і безпосередньо його виводи у відповідних рядках програми. Схема зображена в додатку А.

4.2 Мікропроцесорний блок

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

Мікроконтролер ATMega8 має 28 виводів у корпусі PDIP, які зображені на рисунку 4.2.

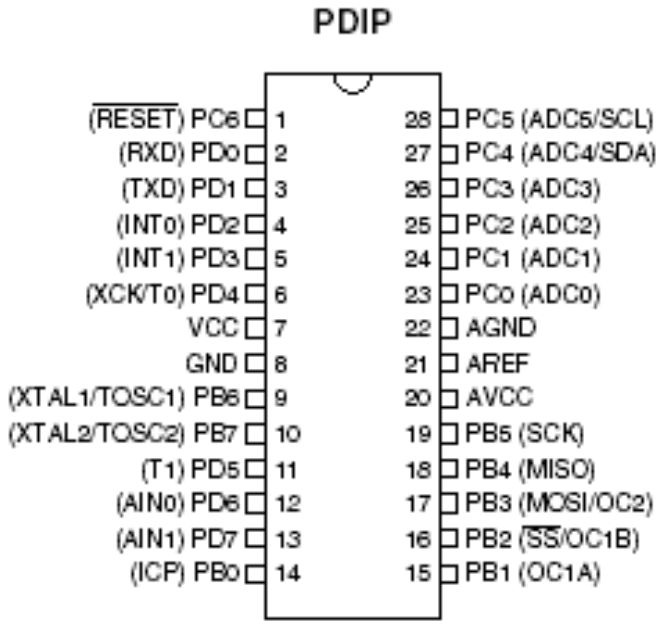

Рисунок 4.2- Призначення виводів мікроконтролера ATMega8у корпусі PDIP

Мікроконтролер ATMega8 має 32 виводи у корпусі TQFP, які зображені на рисунку 4.3.

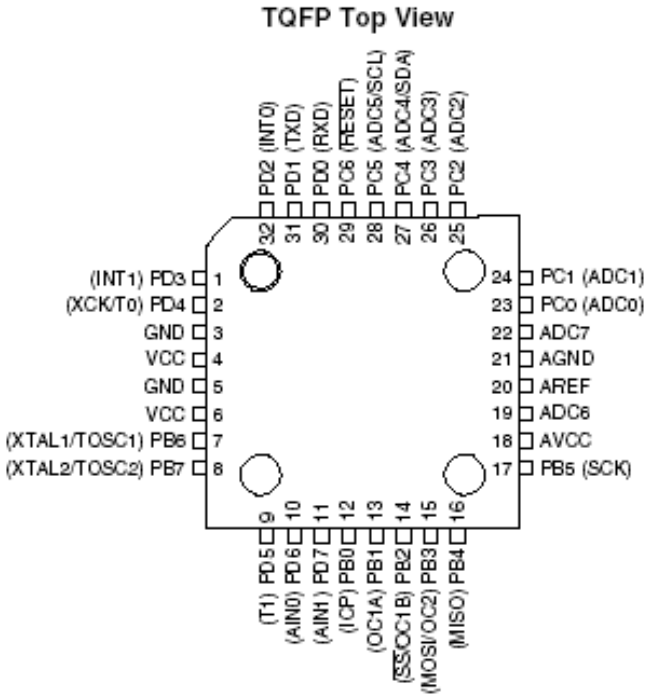

Рисунок 4.3- Призначення виводів мікроконтролера ATMega8 у корпусі TQFP

VCC,GND -напруга живлення та заземлення.

AVCC - напруга живлення аналого-цифрового перетворювача в даній схемі.

ПортВ – має 8-розрядний двонаправлений порт і вміщує в собі навантажувальні резистори.

Порт С -має 8-розрядний вихідний порт. Порт С використовується для шини адреси.

RESET- Вхід для скидання. Для скидання необхідно утримувати низький рівень на вході більш ніж 50 нс.

AGND -даний вивід повинен бути під’єднаний до окремого заземлення.

ПортD– має 8-розрядний двонаправлений порт, який має вбудовані навантажувальні резистори.

XTAL1, XTAL2 - Вхід та вихід інвертуючого підсилювача тактової частоти генератора.

AREF- вхід опорної напруги для аналого-цифрового перетворювача. На даний вивід подається напруга у межах між AGND и AVCC.

TOSC1, TOSC2 - Вхід та вихід інвертуючого підсилювача.

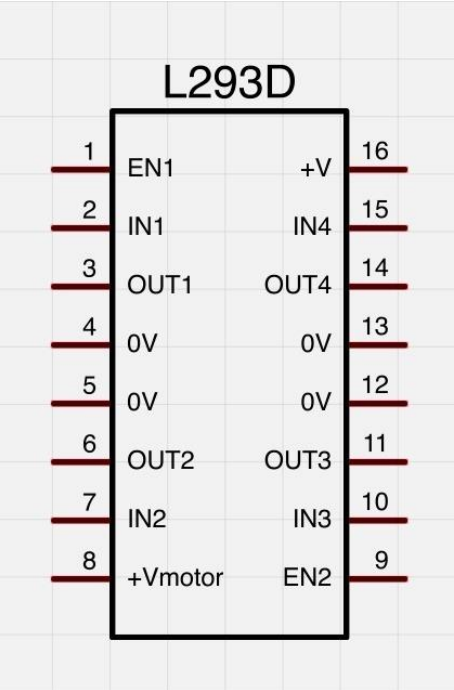

Рисунок 4.4 - Призначення виводів мікросхеми L293D

Мікросхема L293D.

Входи ENABLE1 і ENABLE2 відповідають за включення кожного з драйверів, що входять до складу мікросхеми.

Входи INPUT1 і INPUT2 управляють двигуном, підключеним до виходів OUTPUT1 і OUTPUT2.

Входи INPUT3 і INPUT4 управляютьдвигуном, підключеним до виходів OUTPUT3 і OUTPUT4.

Контакт Vs з'єднують з позитивним полюсом джерела електроживлення двигунів або просто з позитивним полюсом харчування, якщо харчування схеми і двигунів єдине. Простіше кажучи, цей контакт відповідає за харчування електродвигунів.

Контакт Vss з'єднують з позитивним полюсом джерела живлення. Цей контакт забезпечує харчування самої мікросхеми.

Чотири контакту GND з'єднують з "землею" (загальним проводом або негативним полюсом джерела живлення). Крім того, за допомогою цих контактів зазвичай забезпечують тепловід від мікросхеми, тому їх найкраще розпаювати на досить широку контактну площадку.

Модуль використовується для управління кроковими двигунами з напругою від 5 до 35 В. За допомогою однієї плати L298N можна управляти відразу двома двигунами. Найбільше навантаження, яку забезпечує мікросхема, досягає 2 А на кожен двигун. Якщо підключити двигуни паралельно, цезначення можна збільшити до 4 А.

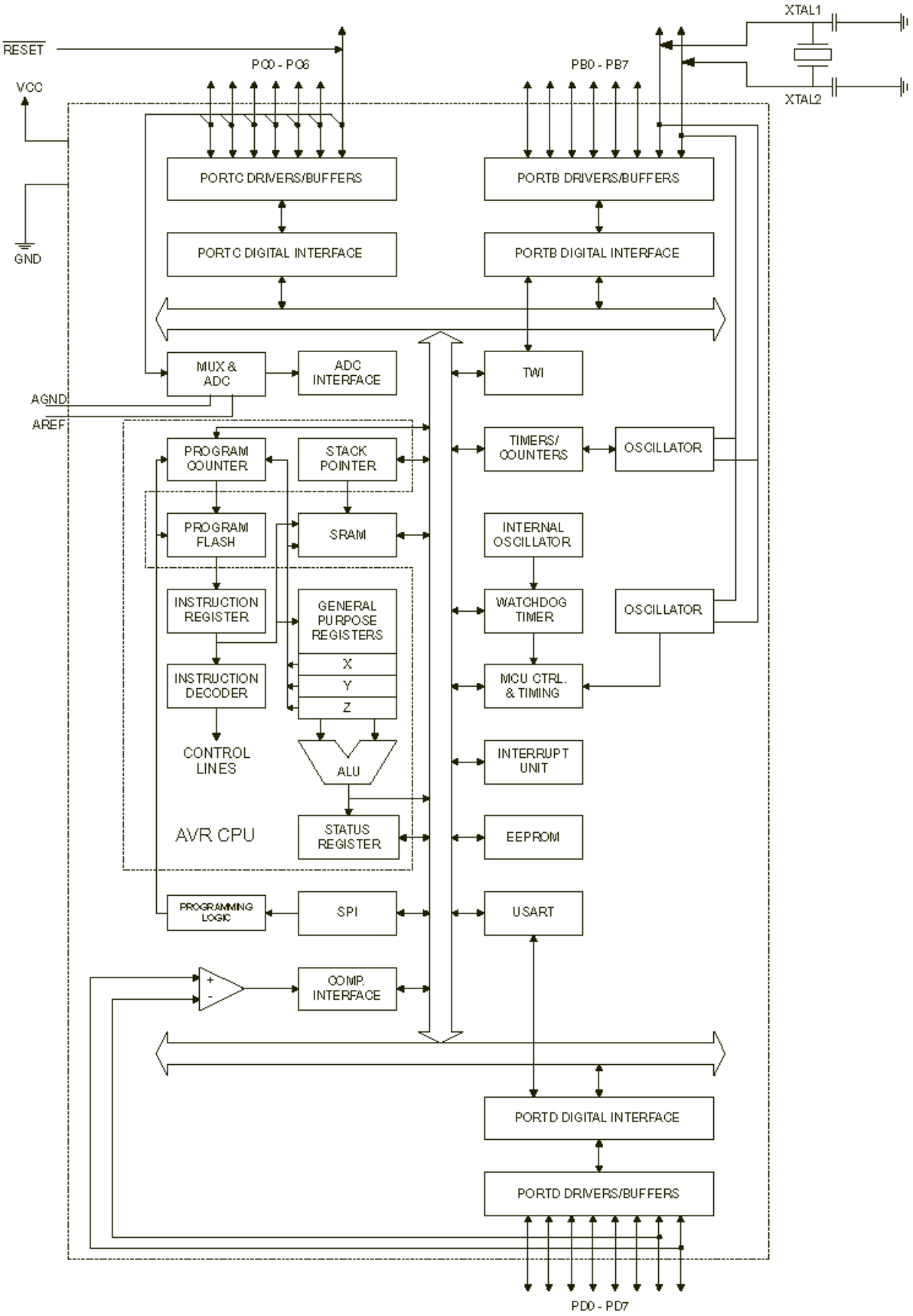

Рисунок4.4 - Функціональна схема мікроконтролера ATMega8

5.РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРИСТРОЮ

Для керування роботом, його треба запрограмувати. Для цього створюється спеціальна програма, яка потім завантажується в мікроконтролер.

Дана розробка містить у собі наступні компоненти:

AVR GCC –компілятор мов C и C++ для AVR;

avr-libc–стандартна C бібліотека для використання з GCC;

avr-as - ассемблер для мікроконтролерів AVR;

AVRDUDE - програматор (програма для загрузки та вигрузки коду мікроконтролерів);

avrdude-gui– графічний інтерфейс користувача для AVRDUDE;

MFile– автоматичний генератор Make-файлів for AVR GCC;

GNU Binutils - утиліти для AVR (

GNU Debugger (GDB) - дебагер (відладчик) с інтерфейсом командного рядка;

Insight - дебагер (відладчик) с графічним інтерфейсом користувача;

AVaRICE (JTAG ICE interface) - програма для інтерфейсів Atmel JTAG ICE;

SimulAVR - симулятор GDB з підтримкою симулятора від AVR;

Нижче приведена програма для обертання двигунами вперед та назад

```
#include <avr/io.h>
void delay(unsigned short ms
{
  unsigned short i, j, k;
        for (i=0; i<ms; i++)
            for (j=0; j<185; j++)
                k++;
}
int main(void)
{
   DDRC = 0xff;
     while (1) {
        PORT |= _BV(PC1);
        PORT &= ~_BV(PC2);
```

```
PORT |= _BV(PC3);
                PORT &= ~_BV(PC4);
        delay(1000);
                        PORT &= ~_BV(PC1);
                        PORT |= _BV(PC2);
                        PORT &= ~_BV(PC3);
                        PORT |= _BV(PC4);
        delay(1000);.
                    }
        }
        #include <avr/io.h>
        int main(void)
        {
        DDRC = 0xff;
          DDRD = 0x00;
          PORTD = 0xff;
             while (1) {
                      if (!(PIND & (1<<PIND1)))
                      {
                   PORT |= _BV(PC1);
                   PORT &= ~_BV(PC2);
                   PORT |= _BV(PC3);
                   PORT &= ~_BV(PC4);
                      }
              else
                      {
                   PORT &= ~_BV(PC1);
                   PORT |= _BV(PC2);
                   PORT &= ~_BV(PC3);
                   PORT |= _BV(PC4);
                      }
        }
        #include <avr/io.h>
        int main(void)
```

```
 {
DDRC = 0xff;
  DDRD = 0x00;
  PORT2 = 0xff;
      while (1) {
if (!(PIND & (1<<PIND1)))
 {
            PORT |= _BV(PC1);
            PORT &= ~_BV(PC2);
            PORT |= _BV(PC3);
            PORT &= ~_BV(PC4);
  }
  else
  {
                PORT &= ~_BV(PC1); //
                PORT |= _BV(PC2); //
                PORT &= ~_BV(PC3); //
                PORT |= _BV(PC4); //
  }
     }
}
#include <stdlib.h>
#include <soft_serout.h>
#include <sleep.h>
#include <analog.h>
#define m 2933
#define b 20
#define k 1
void main()
{
unsigned char dec[4],dec2[4];
unsigned int gp2=0,cm=0;
sleep(1000);
soft_out_init(2,9600);
```

```
while(1)
gp2 = analog(0);
cm = (m/(gp2+b)) - k;
utoa(gp2,dec,10);
utoa(cm,dec2,10);
out_byte(2,0xFE);
out_byte(2,0x00);
out_byte(2,0xFE);
out_byte(2,0x80);
out_text(2,"RAW Data= ");
out_text(2,dec);
out_byte(2,0xFE);serout_byte(2,0xC0);
out_text(2,"Distance= ");
out_text(2,dec2);
out_byte(2,0xFE);serout_byte(2,0xCE);
serout_text(2,"CM");
sleep(500);
}
}
#include <stdlib.h>
#include <motor.h>
#include <sleep.h>
#include <sound.h>
#include <analog.h>
void main()
{
unsigned int sensor=0;
unsigned char i=0;
sleep(200); sound(4000,50);
while(1)
{
sensor=0;
for (i=0;i<5;i++)
{
sensor=(sensor+analog(0));
```

```
}
sensor=(sensor/5);
if (sensor>260)
{
backward(50);
sleep(800);
s_left(50);
sleep(600);
}
else
{
forward(50);
}
}
```

ВИСНОВКИ

У даному проекті було розроблено пристрій для захисту конфіденційної інформації. В наш час захист конфіденційної інформаці є актуальним і потребує в надійних методах захисту.

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 мікроконтролер Atmega8, перевагами якого є:

-низька вартість;

-високопродуктивний, що споживає мало енергії, 8-бітний мікроконтролер.

ЛІТЕРАТУРА

1. http://studfiles.net/preview/5993348
2. http://fotocom.at.ua/publ/ucheba/zakhist_konfidencijnikh_...ogo_dostupu/2-1-0-74
3. 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
4. Журнал «Захист інформації». Том 21, № 1 (2019)
5. Усатенко С. Т., Каченюк Т.К., Терехова М.В. Выполнение электрических схем по ЕСКД: Справочник – М.; Издательство стандартов, 1989.
6. Зубчук В.И. и др.: Справочник по цифровой схемотехнике.— К.: Техника, 1990.— 448 с.: ил.
7. Разработка и оформление конструкторской документации радиоэлектронной аппаратуры: Справочник Э. Т. Романычевой, - М.; Радио и связь, 1989.
8. http://robotrends.ru/pub/1812/roboty-ploho-zashisheny-ot-hakerov-i-eto-opasno-2018
9. 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»)
10. https://www.geeksforgeeks.org/what-is-information-security-2016.
11. http://allbest.ru/otherreferats/law/00165045_0.html
12. http://referat.co/ref/56100/read?p=8

ДОДАТОК А

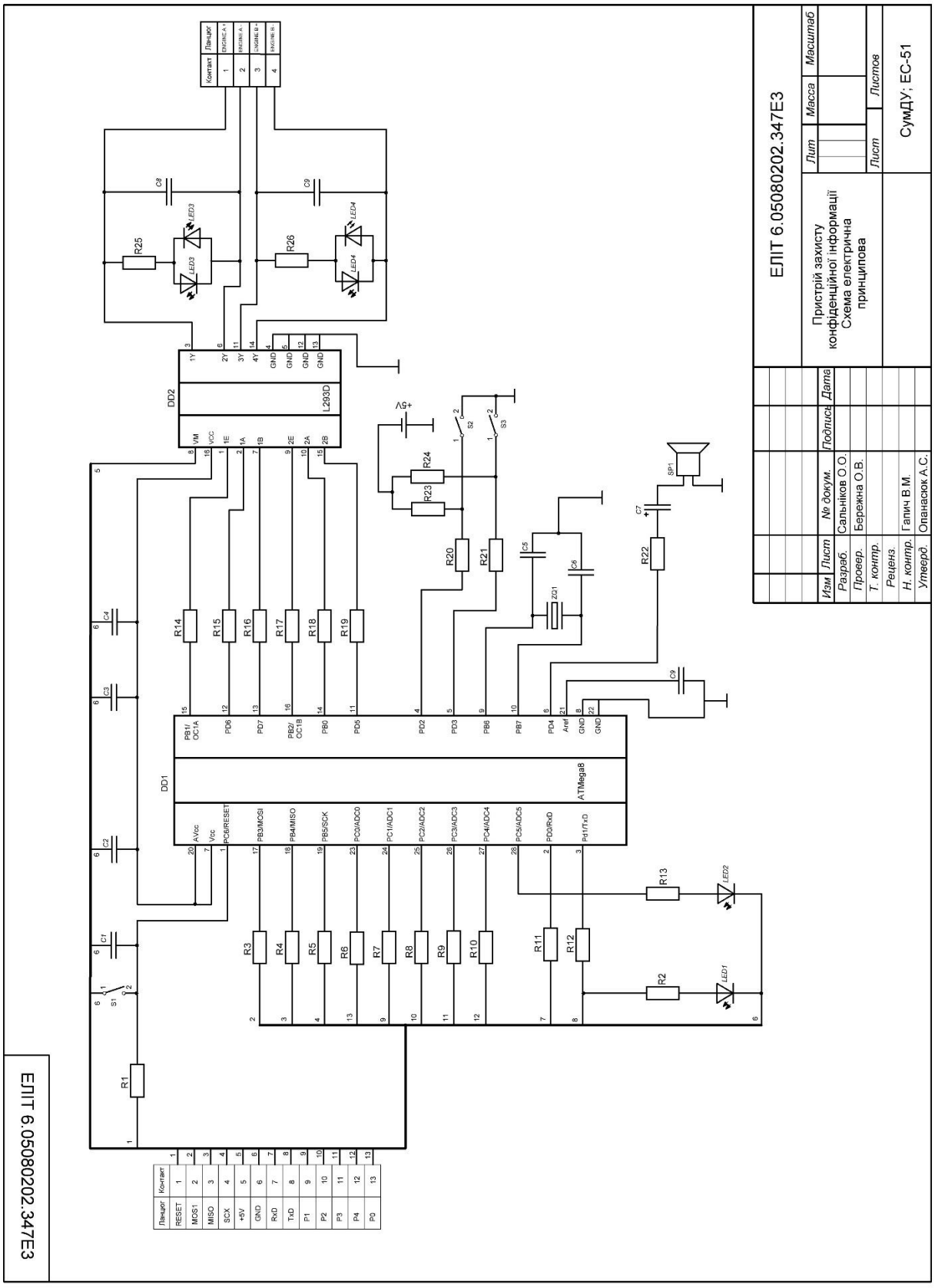

Рисунок 1 - Принципіальна схема пристрою

ДОДАТОК Б

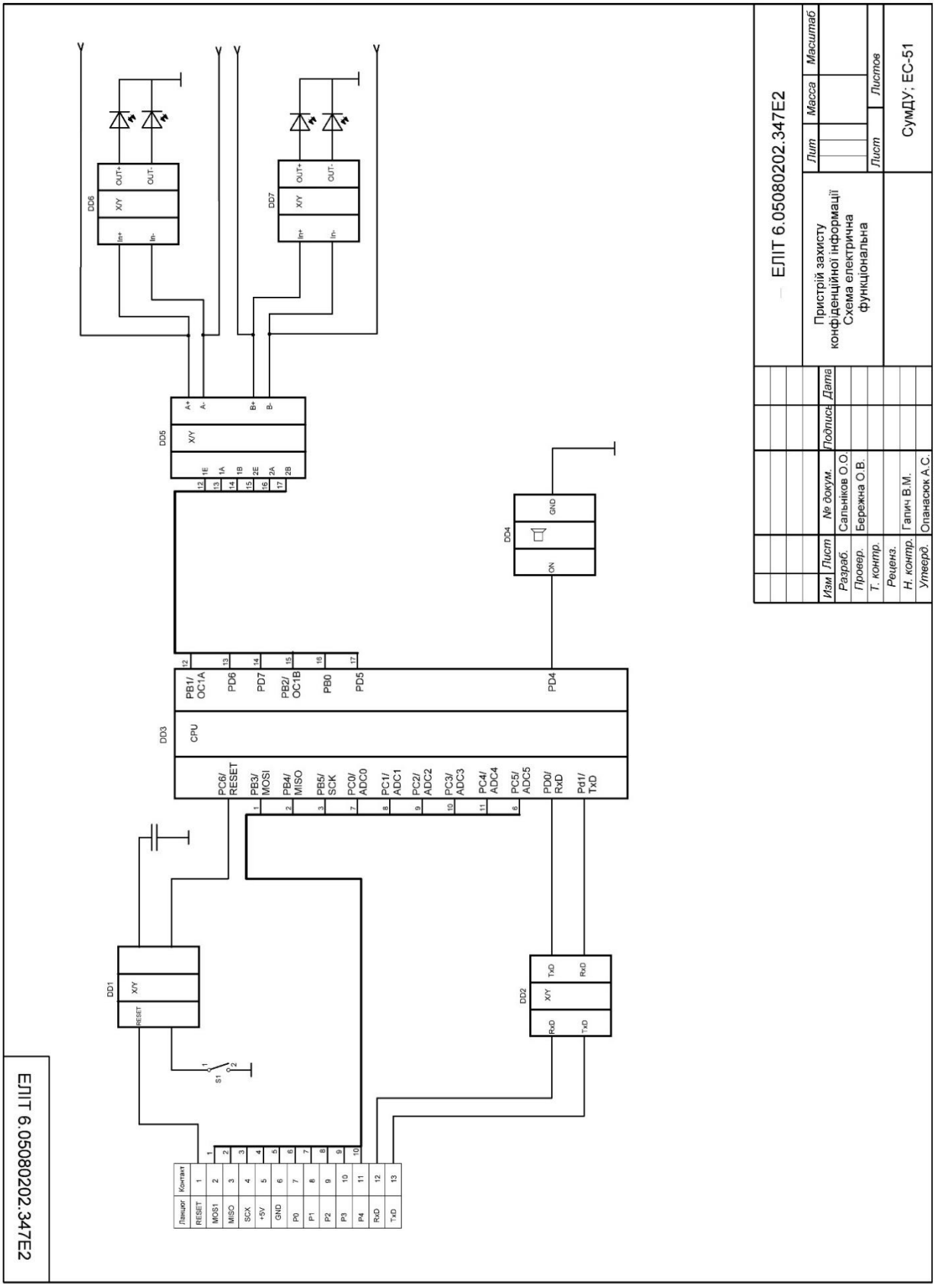

Рисунок 2 -Функціональна схема пристрою