

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

Радіотехнічний факультет

Кафедра радіоінженерії

До захисту допущено:

В.о. завідувача кафедри

_____ Сергій МАРТИНЮК

«___» _____ 20 р.

Дипломний проєкт

на здобуття ступеня бакалавра

за освітньою програмою ««Радіосистемна інженерія»

спеціальності 172 «Телекомунікації та радіотехніка»

**на тему: «Криптографічний аудіо-термінальний пристрій з бездротовим
інтерфейсом»**

Виконав (-ла):

студент (-ка) IV курсу, групи РС-81

Томчук І. В.

Керівник:

Старший викладач

Павлов О.І.

Рецензент:

Старший викладач

Омелянєнко М.Ю.

Засвідчую, що у цьому дипломному
проєкті немає запозичень з праць інших
авторів без відповідних посилань.

Студент (-ка) _____

Київ – 2022 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Радіотехнічний факультет
Кафедра радіоінженерії

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітня програма «Радіосистемна інженерія»

ЗАТВЕРДЖУЮ

В.о.завідувача кафедри

_____ Сергій МАРТИНЮК

«__» _____ 2022 р.

ЗАВДАННЯ
на дипломний проєкт студенту
Томчук Іван Вікторович

1. Тема проєкту «Криптографічний аудіо-термінальний пристрій з бездротовим інтерфейсом»

_____»,

керівник проєкту Старший викладач Павлов О.І.,

затверджені наказом по університету від «17_»__ червня 2022р. №_822-с_

2. Термін подання студентом проєкту 19 червня 2022 р. _____

3. Вихідні дані до проєкту пояснювальна записка, технічне завдання

4. Зміст роботи _Аналіз сучасних криптографічних рішень та їх застосування для створення захищеного каналу зв'язку. Розробка портативного пристрою для виконання функцій запису, відтворення за шифрованої передачі даних.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) схема електрична принципова, складальний кресленик, перелік елементів, специфікація, креслення друкована плата, схема структурна терміналу.

6. Консультанти розділів роботи*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 02 травня 2022 р. _____

Календарний план

№ з/п	Назва етапів виконання дипломного проєкту	Термін виконання етапів роботи	Примітка
	Огляд алгоритмів шифрування	02.05-13.05	
	Огляд аналогів	14.05 – 22.05	
	Вибір компонентів	23.05 – 03.06	
	Розробка плати	04.06 – 12.06	
	Розробка корпусу	13.06 – 19.06	

Студент

Іван ТОМЧУК

Керівник

Олег ПАВЛОВ

* Якщо визначені консультанти. Консультантом не може бути зазначено керівника дипломної роботи.

АНОТАЦІЯ

В дипломному проекті розроблено аудіо-термінальний пристрій з бездротовим інтерфейсом, впроваджено алгоритми криптографії для захисту даних, спроектовано плату за допомогою середовища Altium Designer. Створено схему електричну принципову, друковану плату, друкований вузол.

Призначення даної розробки – використання пристрою для передачі інформації людям, які зацікавлені у власній інформаційній безпеці. Оскільки на сьогоднішній день важко визначити, як пристрої обробляють та зберігають вашу інформацію.

При створенні проекту було розглянуто сучасні алгоритми забезпечення захисту даних, та вибір компонентів які є можливість знайти в найближчому магазині.

Ключові слова : алгоритми шифрування, бездротовий інтерфейс.

ANNOTATION

In the graduation project, an audio terminal device with a wireless interface was developed, cryptographic algorithms for data protection were implemented, and a board was designed in the Altium Designer environment. Created electrical principle diagram, printed circuit board, printed circuit board.

The purpose of this development is to use the device to transmit information to people interested in their own information security. Because today it is difficult to determine how devices process and store your information.

When creating the project, modern data protection agglomerations and the choice of components that can be found in the nearest store were taken into account.

Key words: encryption algorithms, wireless interface.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту

на тему: Криптографічний аудіо-термінальний пристрій з бездротовим інтерфейсом.

Київ — 2022року

ЗМІСТ

Перелік скорочень.....	2
Вступ.....	3
1 Шифрування	4
1.1 Сфери застосування	4
1.2 Обробка інформації	4
1.3 Методи шифрування.....	4
1.4 Алгоритми.....	5
1.4.1 AES	5
1.4.2 RSA.....	5
1.4.3 Blowfish.....	7
Висновки до першого розділу.....	8
2 Розробка плати	9
2.1 Огляд аналогів	9
2.1.1 Плата розробки ESP32-S3-Korvo-2 V3.0	9
2.1.2 Плата розробки ESP32-LyгаT V4.3	10
2.1.3 ССТ Криптофон [12].....	11
2.1.4 x-machine [13]	12
2.2 Схема структурна системи.....	13
2.3 Схема структурна терміналу.....	14
2.4 Вибір компонентів	15
2.4.1 Мікроконтроллер	15
2.4.2 Акумулятор.....	16

					РС81.466459.001 ПЗ						
ЗМ.	Лист	№ докум.	Підпис	Дата							
Розробив		Томчук І.В.			Криптографічний аудіо-термінальний пристрій			Літ.	Лист	Листів	
Перевірив		Павлов О.І.								1	
								РС-81 РТФ			
Н. Контр.		Павлов О.І.									
Затвердив		Павлов О.І.									

2.4.3 Модуль контролю заряду	16
2.4.4 Зовнішнє підключення	18
2.4.5 Стабілізатор живлення	18
2.4.6 Мікрофон	19
2.4.7 Фільтр шумів	20
2.4.8 Аудіопідсилювач.....	21
2.4.9 Підключення навушників.....	21
2.4.10 Підключення SD карти	21
2.5 Розрахунки для створення плати.....	23
Висновки до другого розділу	25
3 Корпус	26
Висновки до третього розділу	27
Перелік джерел посилань	28
Додаток А Технічне завдання.....	2
Додаток Б Відомість до ДП	
Додаток В Схема електрична принципова	
Додаток Г перелік елементів	
Додаток Д складальний кресленик	
Додаток Е складальний кресленик пристрій	
Додаток Є Друкована плата	
Додаток Ж структурна схема терміналу	
Додаток З структурна схема системи	

					РС81.466459.001 ПЗ				
ЗМ.	Лист	№ докум.	Підпис	Дата	Криптографічний аудіо-термінальний пристрій	Літ.	Лист	Листів	
Розробив	Томчук І.В.						1		
Перевірив	Павлов О.І.								
Н. Контр.	Павлов О.І.								
Затвердив	Павлов О.І.								
					РС-81 РТФ				

ПЕРЕЛІК СКОРОЧЕНЬ

ABS - акрилонітрил бутадієн стірол, пластик для 3д друку;

AES - Advanced Encryption Standard, симетричний алгоритм шифрування;

BT – Bluetooth, технологія безпроводної передачі даних;

I2C - послідовна шина даних для зв'язку інтегральних схем;

PSRAM – високо швидкісна псевдостатична пам'ять;

RSA - криптографічний алгоритм з відкритим ключем;

SPI - фактичний послідовний синхронний повнодуплексний стандарт передачі даних;

АЦП – аналогово цифровий перетворювач;

Жк дисплей – дисплей з використанням технології рідких кристалів;

ЦАП – цифро аналоговий перетворювач;

					PC81.466459.001 ПЗ	Лист
						2
Зм.	Лист	№ докум.	Підпис	Дата		

ВСТУП

Темою дипломного проекту є криптографічний аудіо-термінальний пристрій з бездротовим інтерфейсом. Актуальність вибраної теми виражається в тому, що на сьогодні більшість даних передається через інтернет у відкритому вигляді, або зберігається слабкими алгоритмами. Також виробники пристроїв та програмного забезпечення збирають дані у себе, для “покращення технічної підтримки”. Але вже доведено, що спецслужби мають повний доступ до даних.

Проаналізувавши сучасні алгоритми шифрування даних, було встановлено оптимальні варіанти, у яких на сьогодні неможливо обійти захист. Також для повноцінного захисту потрібно запускати алгоритм на пристроях власного проектування.

Аналоги на сьогодні існують, але їх замовлення може бути сприйняте державою як порушення законів. Оскільки більшість даних пристроїв мають мініатюрний розмір.

Тому на сьогодні тема проекту є актуальною як ніколи.

					<i>РС81.466459.001 ПЗ</i>	Лист
						3
Зм.	Лист	№ докум.	Підпис	Дата		

1 ШИФРУВАННЯ

1.1 Сфери застосування

Шифрування – перетворення інформації, яке дозволяє заховати інформацію для збереження її від посторонніх людей, але і показати для певного обмеженого кола осіб [1].

Основні цілі захисту інформації:

- Конфіденційність;
- Цілісність;
- Ідентифікація;

Конфіденційність – захист даних при передачі публічними та приватними каналами зв'язку.

Цілісність – забезпечення режиму, коли інформацію неможливо змінити.

Ідентифікація – підтвердження того, що саме відправник інформації є тим, ким він представився.

1.2 Обробка інформації

Обробка і захист інформації складаються з декількох етапів :

- Шифрування
- Розшифрування

На простому рівні, обидві операції – математичні функції, які виконують певну зміну даних. У таких функціях існує ключ – число або набір чисел, які задають унікальність обробки. Чим більший ключ – тим довше його підбирати для несанкціонованого доступу.

1.3 Методи шифрування

На сьогодні існує декілька методів :

- Симетричний;
- Асиметричний;

					РС81.466459.001 ПЗ	Лист
						4
Зм.	Лист	№ докум.	Підпис	Дата		

Симетричний – використання одного ключа для шифрування та розшифрування. В такому випадку чим більший ключ – тим кращий захист.

Асиметричний – використання відкритого та закритого ключа.

1.4 Алгоритми

1.4.1 AES

Симетричний алгоритм блочного шифрування. AES має фіксовану довжину у 128 біт, а розмір ключа може приймати значення 128, 192 або 256 біт. Через фіксований розмір блоку AES оперує із масивом 4×4 байт, що називається *станом* (версії алгоритму із більшим розміром блоку мають додаткові колонки). [2]

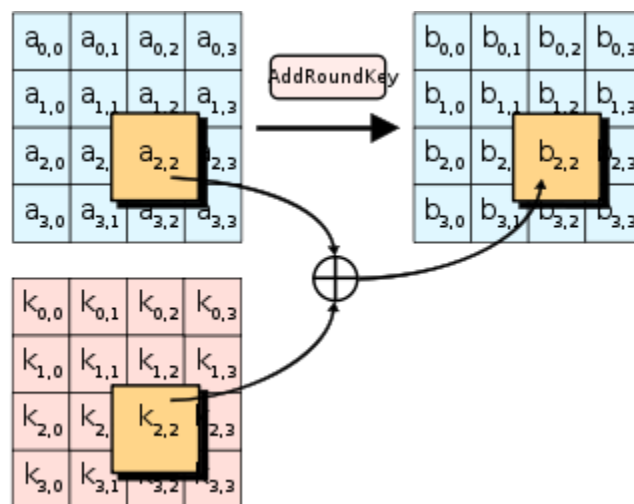


Рисунок 1.1 – Робота алгоритму AES

Недоліки : недостатня криптостійкість. На сьогодні існують алгоритми та машинні ресурси для підбору ключів [3].

1.4.2 RSA

RSA— криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел [4].

Даний алгоритм на сьогодні використовується як основа цифрового підпису, так і в криптовалютах. Оскільки має відкритий та закритий ключ доступу. З закритого ключа можливо згенерувати відкритий, але не навпаки.



Рисунок 1.2 – Як працює шифрування за RSA

Недоліки алгоритму – низька швидкість алгоритму. Якщо порівнювати швидкість виконання алгоритмів, виграють симетричні. Також даний алгоритм написано для потужних ПК, а не мікроконтролерів. Що робить з цього алгоритму ненадійного кандидата на реалізацію.

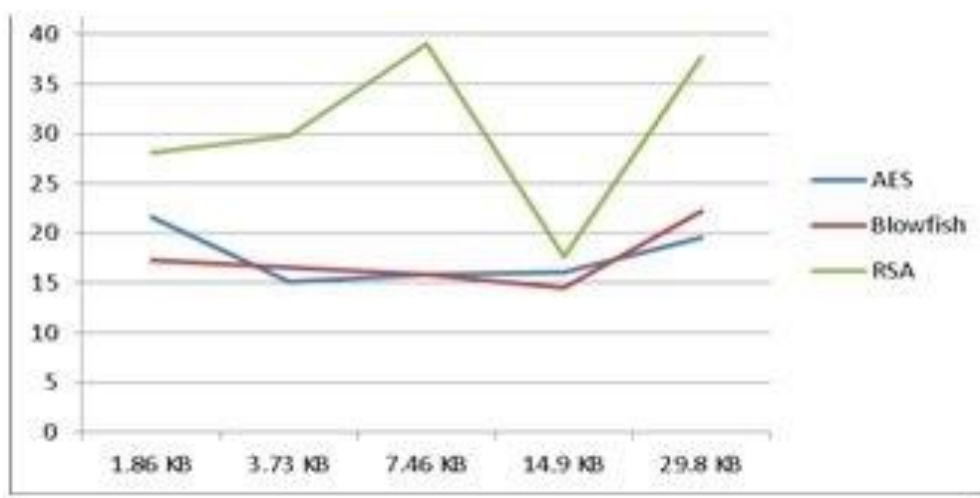


Рисунок 1.3 – Час обробки інформації залежно від алгоритму

Було проведено дослідження по затраченому часу на обробку алгоритму RSA [14]. Використано 8-бітний мікроконтролер PIC. Затрачений час для шифрування\дешифрування склав 2\120 секунд. Що робить мікроконтролери непридатними для обробки на льоту. Тому потрібно використовувати енергонезалежну пам'ять, для зберігання проміжних даних.

В 2010 групі вчених вдалось взламать ключ довжиною 748 біт. До доводить, що з сучасним розвитком техніки потрібне постійне оновлення алгоритмів [5].

На сьогодні величина ключа має складати не менше 2048 біт, оскільки менша довжина ключа піддається взлому [6].

1.4.3 Blowfish

Blowfish— криптографічний алгоритм, який реалізує блочне симетричне шифрування [7].

На сьогодні використовують для хешування паролів, створення SSH та інших протоколів мережевого та транспортного рівнів.

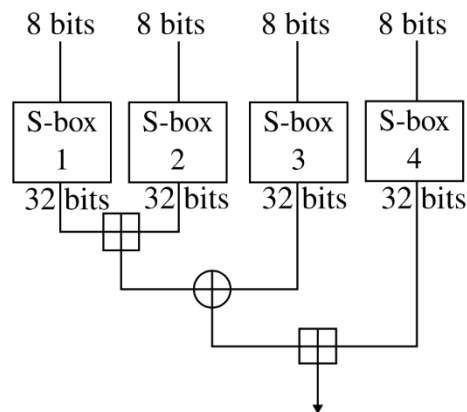


Рисунок 1.4 – Функція шифрування алгоритму.

Недолік – симетричність ключа. Потрібно буде постійно змінювати ключ для безпеки. Також було доведено, що при шифруванні файлу більше 4 ГБ, є можливість швидкого підбору ключа [8].

Написання алгоритмів шифрування самому є недоречною задачею, оскільки оцінкою ступеня захисту алгоритму ніхто займатись не буде. Тому для реалізації алгоритмів будемо використовувати відкриту бібліотеку алгоритмів OpenSSL [15].

Висновки до першого розділу

В цьому розділі було розглянуто види сучасних алгоритмів, де їх застосовують. Переглянуто популярні та стійкі варіанти, в залежності від поставлених задач. Визначено їх переваги а недоліки, При огляді було обрано гібридний алгоритм – застосування алгоритму AES для шифрування тексту повідомлення, а алгоритм RSA для передачі ключів AES.

					<i>РС81.466459.001 ПЗ</i>	Лист
						8
Зм.	Лист	№ докум.	Підпис	Дата		

2 РОЗРОБКА ПЛАТИ

2.1 Огляд аналогів

2.1.1 Плата розробки ESP32-S3-Korvo-2 V3.0



Рисунок 2.1 — Зовнішній вигляд

Характеристики:

- 16 MB Flash + 8 MB PSRAM;
- Основа ESP32-S3-WROOM-1;
- Підключення BT, WiFi;
- 2 мікрофони;
- Жк дисплей, камера;
- АЦП окремим чіпом, Аудіопідсилювач також;
- Вбудовані динаміки відсутні;

Аналіз:

Не має портативного джерела живлення. Присутній екран та камера. Велика кількість кнопок для створення керування. Також впаяний конвертер USB-to-UART для швидкої прошивки мікроконтроллера.

					PC81.466459.001 ПЗ	Лист
						9
Зм.	Лист	№ докум.	Підпис	Дата		

2.1.2 Плата розробки ESP32-LyraT V4.3



Рисунок 2.2 — Зовнішній вигляд RigExpert AA230

Характеристики:

- 4 MB Flash + 8 MB PSRAM
- Крок частоти 1кГц;
- Основа ESP32-WROVER-E;
- Підключення BT, WiFi;
- 1 мікрофон;
- Можливість підключення як зовнішніх динаміків, так і навушників;
- Аудіокодек окремим чіпом (ES8388);
- Зовнішнє джерело живлення;

Аналіз:

Простіший пристрій, який заточений під обробку лише аудіо потоку. Має як і інші плати для розробки певні лишні деталі, які можна прибрати при створенні пристрою.

					PC81.466459.001 ПЗ	Лист
						10
Зм.	Лист	№ докум.	Підпис	Дата		

2.1.3 ССТ Криптофон [12]



Рисунок 2.3 – Зовнішній вигляд пристрою фірми Saycom.

Має зовнішній вигляд звичайного телефона. Використовує для передачі сигналу мережу GSM. Алгоритм захисту даних – AES-256. Портативність забезпечується

Пристрій дозволяє використовувати публічні мережі зв'язку GSM для створення захищеного аудіо каналу. Можливість зберігання повідомлень відсутня, лише якщо запис увімкне оператор зв'язку.

Реалізація шифрування виконується крипто модулем на рівні заліза, що не дозволяє встановити програму, яка буде підміняти ключі. Але оскільки пристрій має GSM зв'язок, є можливість підключення через інтренет, що становить загрозу перехоплення даних.

Недоліки : використання на сьогодні слабкого ключа захисту даних. Неможливість перевірити чи насправді присутній захист.

					PC81.466459.001 ПЗ	Лист
						11
Зм.	Лист	№ докум.	Підпис	Дата		

2.1.4 x-machine [13]



Рисунок 2.4 – зовнішній вигляд безпроводного крипто-терміналу x-machine

Даний пристрій виконаний у ролі Bluetooth терміналу з модулем зв'язку gsm/umts. Містить мікроконтроллер для захисту інформації та акумулятор для портативності. Використовується алгоритм AES-256.

Використання пристрою можливе лише з пристроями компанії Apple. Оскільки в них закрита операційна система, можливість підхопити шкідливе ПЗ для прослуховування зводиться до мінімуму. Але як працює система всередині, теж ніхто не знає.

					РС81.466459.001 ПЗ	Лист
						12
Зм.	Лист	№ докум.	Підпис	Дата		

2.2 Схема структурна системи

Пристрій повинен знаходитись у користувачів, які хочуть передавати захищені повідомлення.

На сьогодні вже існують подібні рішення, але вони мають декілька недоліків.

Один з яких – ступінь недовіри до програмного забезпечення та заліза. При покупці телефона ми не можемо сказати, які дані збирає про нас користувач. Також у відкритих системах, таких як Android існує великий шанс взлому і встановлення ПЗ для прослуховування. Що неможливо перевірити без відповідних спеціалістів.

Тому було вирішено створити власний пристрій, який можна використовувати під задачі шифрування зв'язку.

Термінальний пристрій може бути оснащений Wifi та Bluetooth технологіями для зв'язку з мережею інтернет напряму та через посередників. Також можливе становлення модулів мобільного зв'язку для прямого виходу в мережу.

Використання веб серверу обумовлене тим, що виконувати передачу даних неможливо виконати між пристроями, якщо один з них не в мережі. Тому повідомлення буде зберігатись на сервері в очікуванні підключення користувача. Від цього можливо відмовитись, якщо встановити обмеження зв'язку, що не буде дозволяти записувати повідомлення без підтвердження отримувача.

Також існує можливість відправки повідомлення з серверу до отримувача шляхом відправки через месенджери. Такі повідомлення є можливість зберігати на телефоні у захищеному вигляді, а для прослуховування потрібно передати файл на термінал.

Схема структурна загальної системи наведена в додатку I.

					PC81.466459.001 ПЗ	Лист
						13
Зм.	Лист	№ докум.	Підпис	Дата		

2.3 Схема структурна терміналу

Для отримання даних потрібно їх отримати. В нашому випадку використовується мікрофон, оскільки пристрій створюється в першу чергу захисту аудіо зв'язку. Підключення мікрофону можливе декількома способами :

- Використання АЦП для зчитування значень;
- Використання протоколу I2C для передачі значення у цифровій формі;

Використовуємо метод АЦП, оскільки в сучасних мікроконтролерах він притусній повсюди.

Мікроконтроллер вибираємо 32 біти, оскільки на сьогодні вони вже є доступні для звичайних людей. Також існують варіації, де об'єднують зв'язок та мікроконтроллер.

Для зберігання ключів шифрування та проміжних даних використовуємо зовнішню енергонезалежну пам'ять. Оскільки мікроконтролер не буде встигати виконувати операції шифрування «на льоту».

Зв'язок можна обирати поміж варіантів :

- Мобільний зв'язок;
- Wifi;
- Bluetooth;

При виборі елементів було встановлено, що системи мобільного зв'язку кращі чим GSM коштують значних грошей. Тому обрано передачу даних через Wifi на телефон користувача.

Для виведення інформації потрібен аудіопідсилювач, так як мікроконтролер не має потужних виходів. Використовуємо аудіопідсилювач.

Сприйняття інформації доречніше проводити в навушниках, оскільки сторонні не будуть чути ваші повідомлення. Також використання навушників зменшує вимоги до підсилювача, оскільки можна вибирати малопотужний.

Схема структурна наведена у додатку I.

					<i>РС81.466459.001 ПЗ</i>	Лист
						14
Зм.	Лист	№ докум.	Підпис	Дата		

2.4 Вибір компонентів

2.4.1 Мікроконтролер

Для поставлених цілей нам необхідно обрати контролер який буде задовольняти ряд параметрів: компактність, наявність вбудованого WiFi або Bluetooth периферії, наявність вбудованого рішення для підключення SPI.

При порівнянні мікроконтролерів STM32 та ESP32, при однаковій ціні для виконання проекту підходить з вбудованим WiFi та Bluetooth.

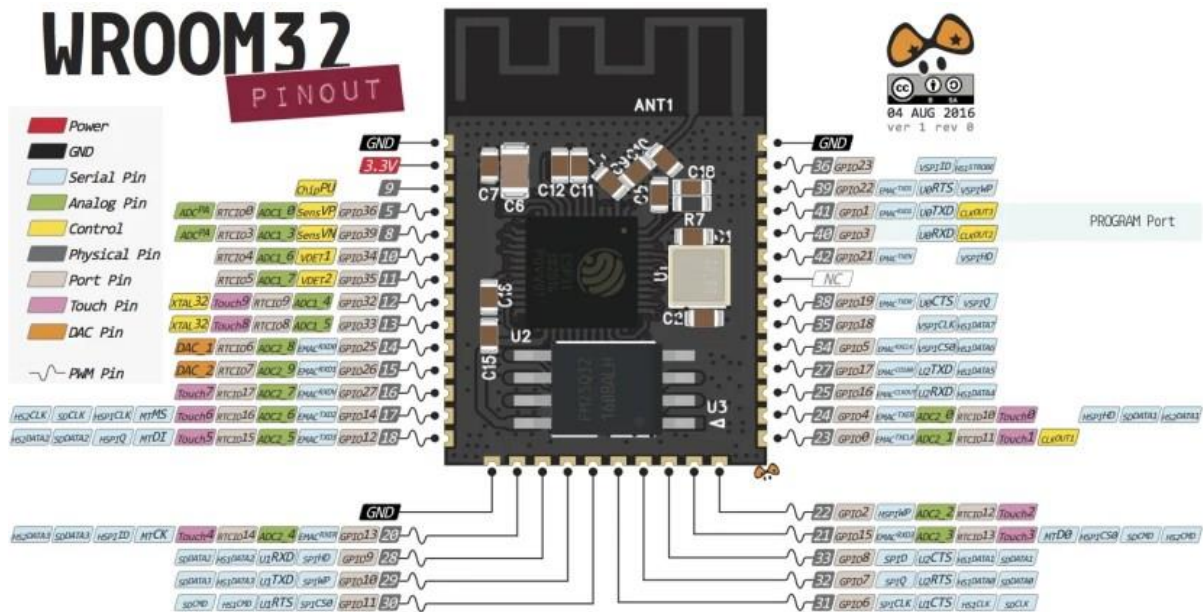


Рисунок 2.5 – Мікроконтролер ESP32-WROOM-32D

Модуль ESP32 має вбудований тактовий генератор та мікросмужкову антену, яка забезпечує бездротовий зв'язок за технологією WiFi та Bluetooth. Існують версії модулю з підключенням зовнішньої антени для збільшення радіусу зв'язку.

2.4.2 Акумулятор

Оскільки мікроконтроллер працює на живленні +3,3 В, є можливість обирати стандартні акумулятори. Але оскільки при різному рівні заряду ми отримуємо різну напругу, потрібно в конструкції передбачити використання стабілізатора. Коливання від +2,7 до +4,2 В.

Порівнюючи популярні варіанти на ринку, було оглянуто дві основних технології виготовлення. А саме :

- Li-ion;
- Li-pol;



Рисунок 2.6 – Типовий представний Li-ion технології

При детальному розгляді, встановлено що Li-ion мають більший запас енергії, що нам і потрібно. Також для даних акумуляторів існує безліч модулів контролю заряду.

При подальшій модернізації пристрою не виключається використання Li-pol акумуляторів для зменшення габаритів.

2.4.3 Модуль контролю заряду

При живленні пристрою від акумулятору, рано чи пізно заряд закінчиться. Тому його періодично потрібно заряджати. Щоб не носити з собою усюди зарядку для акумуляторів, було прийняте рішення її вмонтувати. Для зру-

					PC81.466459.001 ПЗ	Лист
						16
Зм.	Лист	№ докум.	Підпис	Дата		

чності використання будемо вважати, що зовнішнє живлення становить +5 В, оскільки сьогодні існує безліч блоків живлення такого типу.

Також модуль повинен сповіщати користувача, коли в пристрої повний заряд батареї та коли нульовий. Якщо переглядати datasheet акумулятора, буде знайдено залежність накопичування енергії від струму заряджання. Через це додаємо в характеристики модулю контролю заряду пункт про регулювання струму зарядки.

При огляді варіантів, які підпадали б під характеристики, було виявлено модулі, які розраховані виключно на 1 акумулятор та без регулювання струму зарядки. Мали мініатюрні розміри, що дозволяє ефективно використовувати площу плати. Але не мали індикації заряду, що робить їх не придатними до даної розробки.

Тому було обрано TP4056, що володіє усіма характеристиками, що потрібно :

- Регулювання струму;
- Можливість світлодіодної індикації процесу;
- корпус SOP-8;

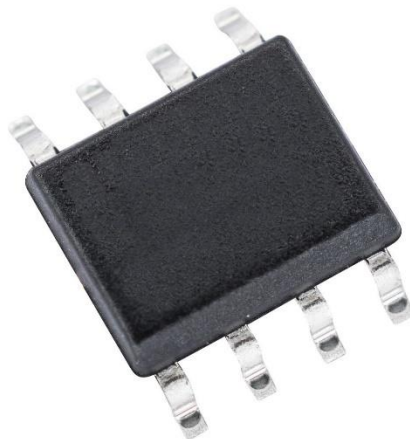


Рисунок 2.7 – Модуль TP4056

					<i>PC81.466459.001 ПЗ</i>	Лист
						17
Зм.	Лист	№ докум.	Підпис	Дата		

2.4.4 Зовнішнє підключення

Оскільки на сьогодні мобільні телефони є у кожного, найкращий варіант використати такий роз'єм, який є у кожного. Тому вибір складається з mini-usb та usb type-c. Робим вибір у користь останнього, тому що сьогодні у всі сучасні телефони його встановлюють.



Рисунок 2.8 – USB type-c роз'єм

2.4.5 Стабілізатор живлення

Оскільки мікроконтролер повинен мати живлення +3,3 В, акумулятор змінює напругу, потрібно використати стабілізатор. Мікроконтролер максимально бере 500мА.

Потрібен стабілізатор на +3,3 В та максимально 500мА.

Обираємо TPS73633, який вже налаштований на +3,3 В. Також стабілізатори TPS736 мають моделі, в яких напруга змінюється завдяки додаванню обв'язки.

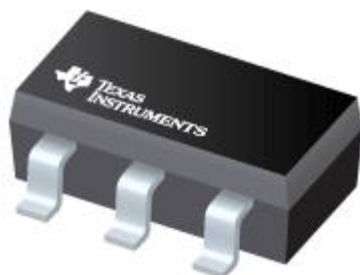


Рисунок 2.9 – Стабілізатор TPS73633

2.4.6 Мікрофон

Мікрофон KPCM15E-P

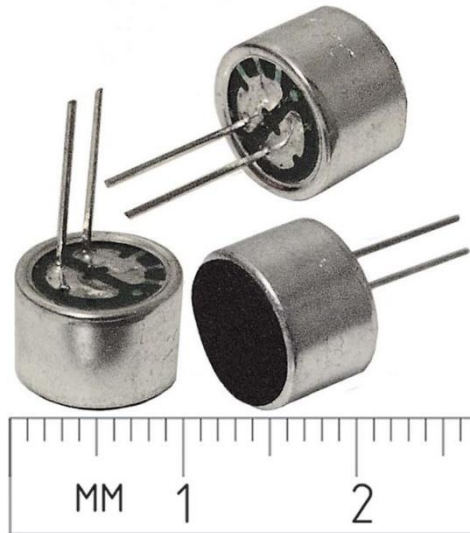


Рисунок 2.10 – Мікрофон KPCM15E

Має наступні характеристики :

- напруга живлення +3,3 В;
- струм споживання 0.5 мА;

Також для мікрофона потрібен підсилювач

Якщо розглянути готові модулі мікрофона для використання у проектах, знаходимо підсилювач MAX9814. За характеристиками нам підходить, тому його будемо використовувати.

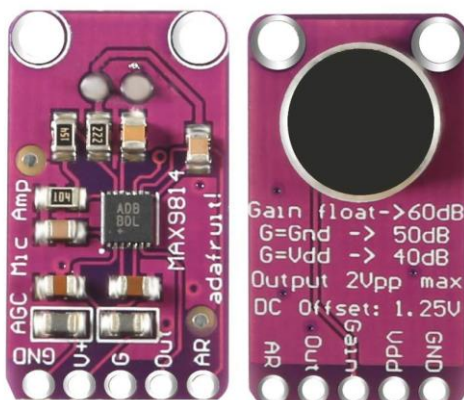


Рисунок 2.11 – Приклад готового модуля мікрофон + підсилювач

					PC81.466459.001 ПЗ	Лист
						19
Зм.	Лист	№ докум.	Підпис	Дата		

2.4.7 Фільтр шумів

Для зчитування даних з мікрофону використовуємо 8-бітний АЦП, який вбудований в мікроконтролер. При такому підключенні та перевірці даних, було виявлено сильні шуми на вході. Тому використовуємо фільтр. Обрано чіп MAX14626, який було використано в аналогічній конструкції.

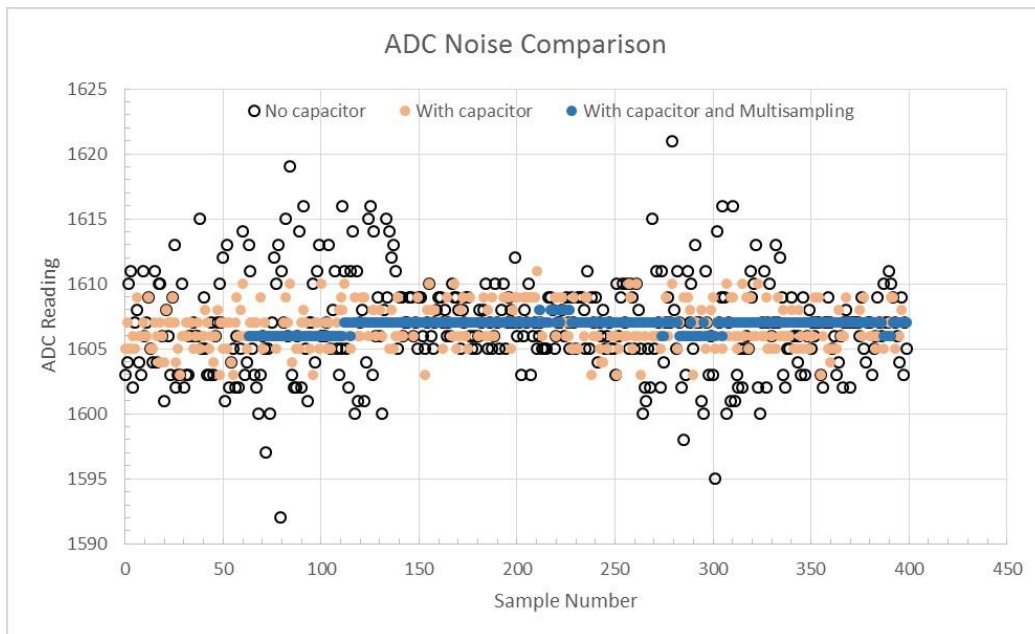


Рисунок 2.12 – Порівняння зчитування даних без фільтру, з фільтром та фільтр + алгоритм.

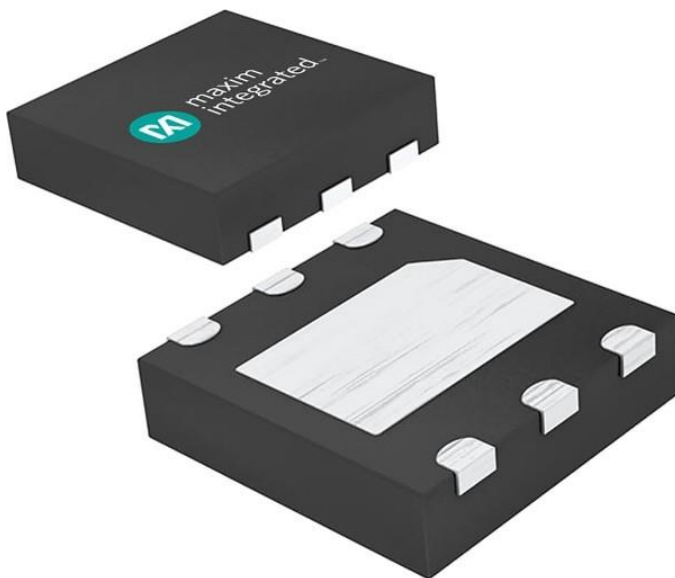


Рисунок 2.13 – Загальний вигляд модулю MAX14626

2.4.8 Аудіопідсилювач

Для видачі сигналу потрібен динамік або навушники. Для того, що б інформацію не було чути постороннім людям, обираємо навушники. Та й підсилювач тоді потрібен менш потужний.

Підсилювач потрібен малопотужний та малошумлячий, також потрібна низька напруга живлення.

При пошуку знаходимо LM4875, який заточений під роботу з навушниками.

2.4.9 Підключення навушників

Використовуємо роз'єм mini jack 3,5 мм на 3 контакти.

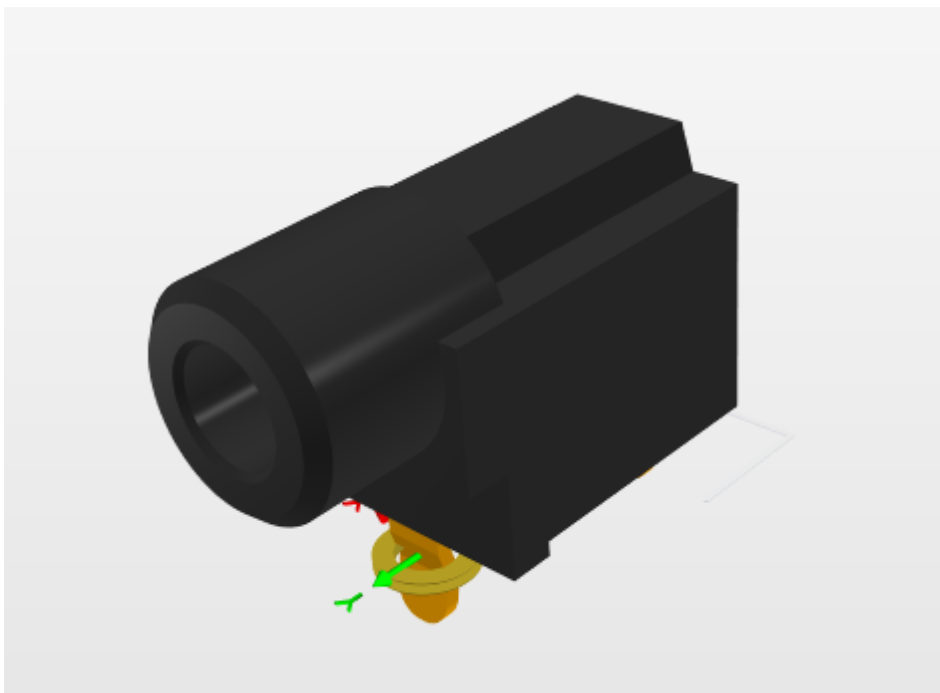


Рисунок 2.14 – Роз'єм mini jack 3,5 мм

2.4.10 Підключення SD карти

SD карта обмінюється даними за стандартом SPI. На мікроконтролері є порти для підключення такого стандарту без зайвих компонентів.

У карт пам'яті є таке поняття як клас швидкості. Тобто максимальна швидкість запису. На сьогодні 10 клас забезпечує 10Мб\с. Будемо використовувати 10 клас, оскільки такі карти не критично відрізняються в ціні.

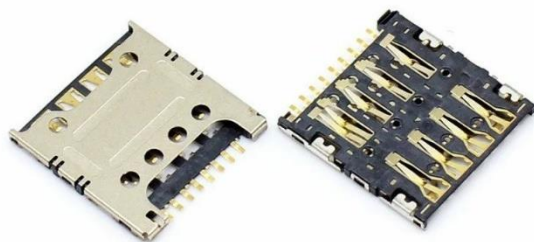


Рисунок 2.15 – Роз’єм для підключення sd карт.

Якщо переглянути аналоги пристрою, можемо побачити правильне підключення даного роз’єму.

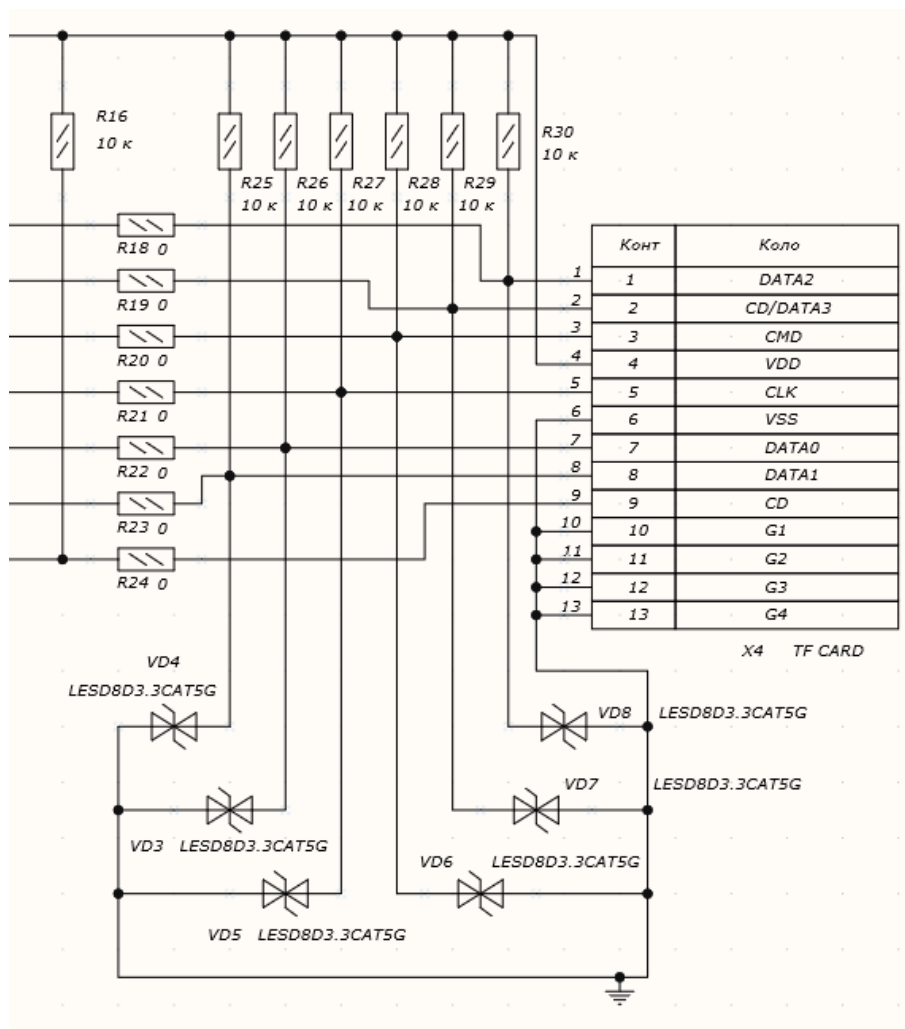


Рисунок 2.16 – Правильне підключення роз’єму

2.5 Розрахунки для створення плати

Вибір матеріалу та клас точності

Матеріал обрано FR4, оскільки для стандартних рішень його використовують найчастіше. Товщину матеріалу беремо, що б забезпечити мінімальну ширину доріжок. Обираємо 105 мкм. Плата повинна бути двохстороння, тому матеріал теж відповідний. Метод виготовлення плат – комбінований позитивний. Клас точності – 3, але при подальшому зменшенні габаритів потрібно буде обирати вже 4-й.

Ширина провідників

Таблиця 2.1 – Розрахунок ширини провідників під різні параметри

Назва провідника	Напруга, В	Струм, А	Ширина провідника	
			мінімальна, мм	максимальна, мм
Живлення акум.	3,3	1	0,476	0,55
Живлення зардки	5	1	0,476	0,55
Сигнальні	3,3	0,1	0,3	0,55

Площа плати

Мінімальна площа плати вираховується з площі елементів, з урахуванням коефіцієнту розміру.

Таблиця 2.2 – Площа елементів плати

Елемент	Площа	Корект. Площа
BM1	125,44	125,44
C1-C14	8,14	113,96
R1-R28	8,14	227,92
VD1-VD2	8,64	17,28
VD3-VD8	3,74	22,44
X1	1736,04	1736,04
X2	86,19	86,19
X3	184,652	184,652
DA1	28,14	56,28
DA2	16,073	32,146
DA3	17,64	35,28
DA4	28,14	56,28
DA5	22,5	45
DA6	516,554	1033,108
X4	1043	2086

З розрахунків випливає, що мінімальна площа плати складає 5858 мм². Також в площа потрібно включити площу під кріплення гвинтами з огляду на те, що відсутні жорсткі умови для розмірів плати, обираємо плату розміром 150x50 мм. Того кінцева площа складає 7500 мм².

Кріплення

Кріплення виконано в 4 точках на краях плати, гвинтами М2*5 DIN914.

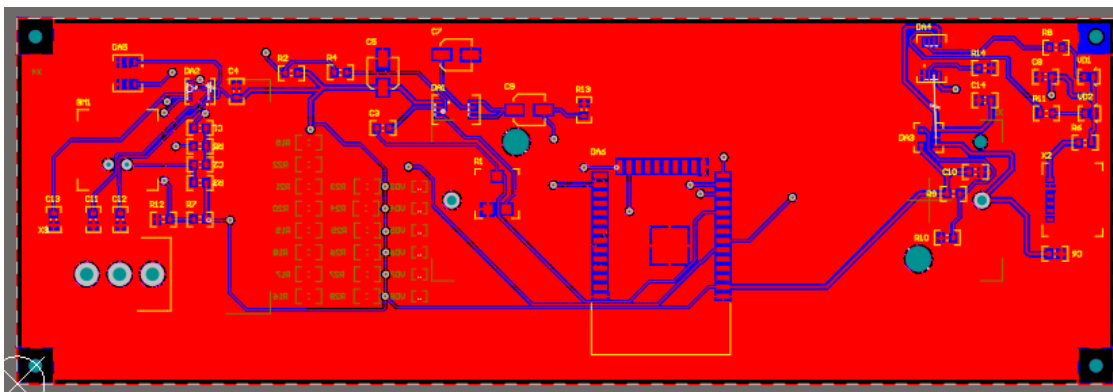


Рисунок 2.17 – Вигляд верхнього шару плати

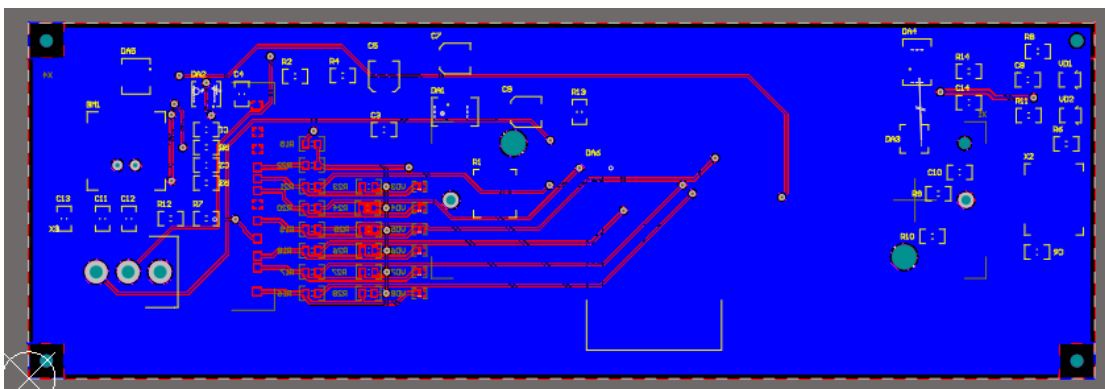


Рисунок 2.18 – Вигляд нижнього шару плати

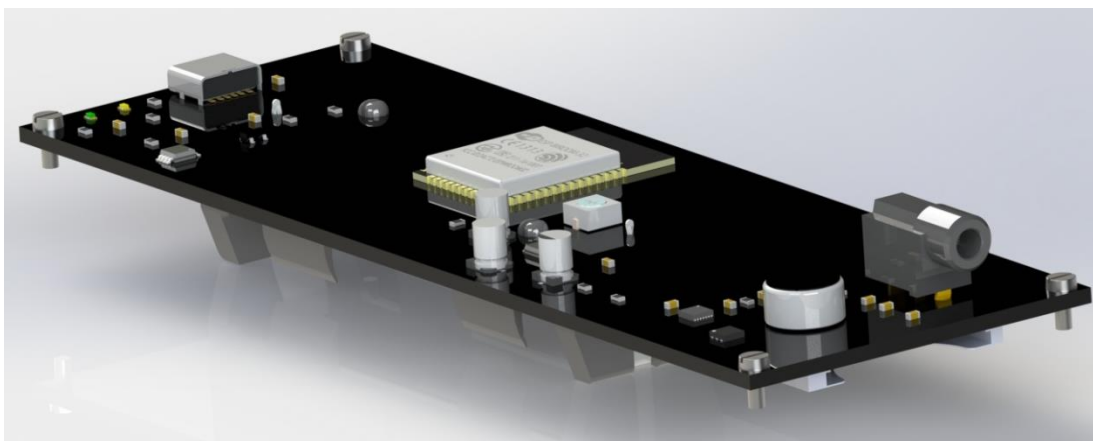


Рисунок 2.19 – Загальний вигляд плати

Висновки до другого розділу

Проведено огляд сучасних аналогів, їх технічних характеристик та сфери застосування. Розглянуто схеми електричні принципові, проведено аналіз та створено власну електричну схему для конкретних задач. Схема електрична принципова наведена в Додаток В.

Проведено вибір елементної бази для реалізації. Створено плату в середовищі Altium Designer. Було обраховано мінімальну ширину провідників, мінімальну площу плати та зроблено вибір матеріалу. Креслення друкованої плати знаходиться в додатку З. Складальний кресленик знаходиться в додатку Д.

					РС81.466459.001 ПЗ	Лист
						25
Зм.	Лист	№ докум.	Підпис	Дата		

3 КОРПУС

Корпус вирішено виготовляти з пластику методом 3Д друку. На сьогодні це популярна та недорога технологія. Пластик обрано ABS, так як має гарні механічні властивості та запас термостійкості. Товщина стінки складає 2 мм, що дозволяє вкласти в пристрій запас міцності.

Для аналізу корпусу вираховано вагу, яка складає 66 грам. При товщині друку 100 мікрон, яку зараз пропонують на ринку, ціна корпусу буде складати 924 грн.

Складальний кресленик наведено у додатку Є.

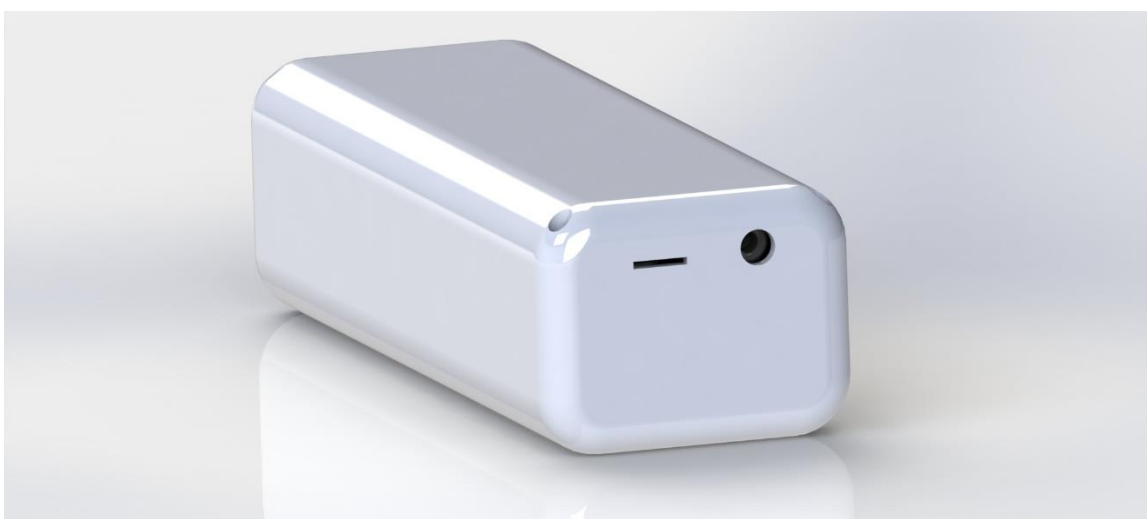


Рисунок 3.1 – зовнішній вигляд корпусу

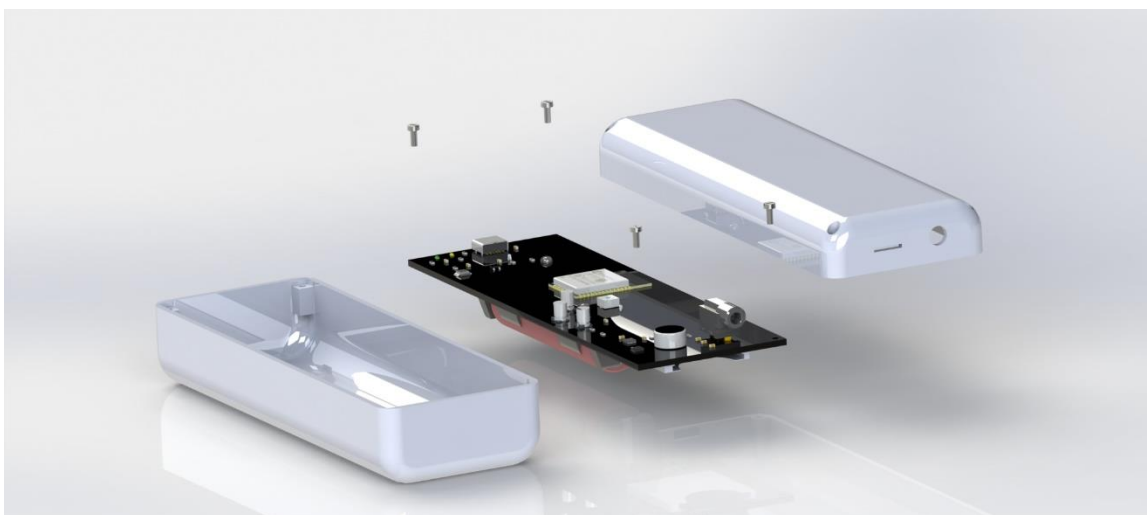


Рисунок 3.2 – вигляд корпусу у розібраному вигляді

					<i>PC81.466459.001 ПЗ</i>	Лист
						26
Зм.	Лист	№ докум.	Підпис	Дата		

Висновки до третього розділу

В ході створення друкованої плати було розроблено корпус для неї. Виготовлення корпусу покладається на технологію 3д друку. Матеріал корпусу складає пластик ABS, оскільки має стійкість до механічного та температурного впливу. При виготовленні корпусу є можливість економити, обравши друк товстішими шарами.

					PC81.466459.001 ПЗ	Лист
						27
Зм.	Лист	№ докум.	Підпис	Дата		

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Шифрування [електронний ресурс]. – Режим доступу: <https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5> – Назва з екрана.
2. Advanced Encryption Standard [електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard– Назва з екрана.
3. A Diagonal Fault Attack on the Advanced Encryption Standard [електронний ресурс]. – Режим доступу: <https://eprint.iacr.org/2009/581.pdf>– Назва з екрана.
4. RSA [електронний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/RSA>– Назва з екрана.
5. Attack of RSA728 [електронний ресурс]. – Режим доступу: <https://documents.epfl.ch/users/l/le/lenstra/public/papers/rsa768.txt>– Назва з екрана.
6. CA:MD5and1024 [електронний ресурс]. – Режим доступу: <https://wiki.mozilla.org/CA:MD5and1024>– Назва з екрана.
7. Blowfish [електронний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/Blowfish>– Назва з екрана.
8. GnuPG FAQ [електронний ресурс]. – Режим доступу: https://gnupg.org/faq/gnupg-faq.html#define_fish – Назва з екрана.
9. <driver/adc.h> [електронний ресурс]. – Режим доступу: <https://docs.espressif.com/projects/espressif/en/latest/esp32/api-reference/peripherals/adc.html> -Назва з екрана.
10. Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. New York, NY: John Wiley & Sons, 1995.
11. Encrypting data with the Blowfish algorithm [електронний ресурс]. – Режим доступу: <https://www.embedded.com/encrypting-data-with-the-blowfish-algorithm/>– Назва з екрана.

					<i>PC81.466459.001 ПЗ</i>	Лист
						28
Зм.	Лист	№ докум.	Підпис	Дата		

- 12.ССТ Криптофон [електронний ресурс]. – Режим доступу:
https://saycom.biz/content/saycom_cct_ru.pdf- Назва з екрана.
- 13.X-Mashine [електронний ресурс]. – Режим доступу:
https://saycom.biz/x-machine_ru.html - Назва з екрана.
- 14.Implementation of the RSA algorithm in a 8-bit microcontroller[електронний ресурс]. – Режим доступу:
<https://sites.google.com/site/ortegaalfredo/pic18rsa> - Назва з екрана.
15. [електронний ресурс]. – Режим доступу: <https://www.openssl.org/>-
Назва з екрана.

					РС81.466459.001 ПЗ	Лист
						29
Зм.	Лист	№ докум.	Підпис	Дата		

ДОДАТОК А

1 НАЗВА І ПІДСТАВА ДЛЯ ВИКОНАННЯ

Назва дипломного проекту “ Криптографічний аудіо-термінальний пристрій з бездротовим інтерфейсом ”.

Підставою для виконання є завдання, видане кафедрою радіоелектроніки від “02” травня 2022 р.

2 ВИКОНАВЕЦЬ

Виконавець – студент групи РС-81 Томчук Іван Вікторович

3 МЕТА ВИКОНАННЯ ДП І ПРИЗНАЧЕННЯ КОНСТРУКЦІЇ

Метою дипломного проекту є розробка криптографічного аудіо-термінального пристрою з бездротовим інтерфейсом та розроблення необхідної конструкторської документації.

Портативний пристрій повинен проводити запис, відтворення та шифрування аудіоданих.

Пристрій повинен працювати від акумулятора.

4 ТЕХНІЧНІ ВИМОГИ

Криптографічний аудіо-термінальний пристрій з бездротовим інтерфейсом повинен володіти наступними характеристиками:

- безпроводна передача даних;
- можливість ;
- живлення від акумулятору;
- портативні розміри пристрою;
- запис даних на внутрішній носій;
- можливість підзарядки акумулятору без розбирання пристрою;
- можливість сучасних алгоритмів шифрування

Головні технічні характеристики приведені в таблицях 1-5.

Таблиця 1 - Вимоги до радіозв'язку.

№	Параметр або характеристика	Одиниця вимірювання	Норма	Джерело
1	Тип зв'язку		Wifi, BT	
2	Швидкість передачі даних	Кб/с	100	

Таблиця 2 - Вимоги до конструкції.

№	Параметр або характеристика	Одиниця вимірювання	Норма	Джерело
1	Маса, не більше	кг	0,5	
2	Габаритні розміри, не більше	мм	30,5×62,4×160	

Таблиця 3 - Вимоги до надійності.

№	Параметр або характеристика	Одиниця вимірювання	Норма	Джерело
1	Середнє напрацювання на відмову T_B , не менше	год	5000	16

Таблиця 5 - Вимоги до джерела живлення.

№	Параметр або характеристика	Одиниця вимірювання	Норма	Джерело
1	Напруга живлення	В	3,0...5,2	
2	Струм споживання	мА	300	
3	Тривалість роботи	год	5	

Пристрій повинен забезпечувати безвідмовну роботу на протязі 24 годин з імовірністю не менше 0,99. Пристрій повинен зберігати працездатність при наступних параметрах навколишнього середовища:

- температура повітря 5...40°C;
- вологість до 90%;
- атмосферний тиск 84...106,7 кПа.
-

5 ВИМОГИ ДО РОЗРОБЛЮВАЛЬНОЇ ДОКУМЕНТАЦІЇ

Оформлення документації згідно ДСТУ 3008:2015.

Склад конструкторської документації :

1. Текстова документація (пояснювальна записка, перелік елементів).
2. Графічна документація (схема електрична принципова, схема електрична структурна, друкована плата, складальний кресленик).

5.1 Орієнтовний зміст дипломного проекту

Завдання на дипломний проект;

Зміст

Вступ

1. шифрування
2. розробка плати
3. огляд аналогів
4. Проектування корпусу
5. Перелік джерел посилань;

Додаток А Технічне завдання

Додаток Б відомість до дП

Додаток В Схема електрична принципова

Додаток Г перелік елементів

Додаток Д складальний кресленик

Додаток Е складальний креслений пристрій

Додаток Є Друкована плата

Додаток Ж Структурна схема терміналу

Додаток З структурна схема системи

6 СТАДІЇ І ЕТАПИ ДИПЛОМНОГО ПРОЕКТУВАННЯ

№ з/п	Назва етапів виконання дипломного проєкту	Термін виконання етапів роботи	Форма звітності
1	Огляд алгоритмів шифрування	02.05-13.05	
2	Огляд аналогів	14.05 – 22.05	
3	Вибір компонентів	23.05 – 03.06	
4	Розробка плати	04.06 – 12.06	
5	Розробка корпусу	13.06 – 19.06	

7 ПОРЯДОК ПРИЙМАННЯ ДИПЛОМНОГО ПРОЕКТУ

1. Представлення проміжних результатів дипломного проекту керівнику в зазначені терміни;
2. Представлення завершеного дипломного проекту керівнику;
3. Перевірка дипломного проекту на наявність плагіату;
4. Представлення кафедрі завершеного дипломного проекту за 10 днів до дати захисту;
5. Захист дипломного проекту перед екзаменаційною комісією.

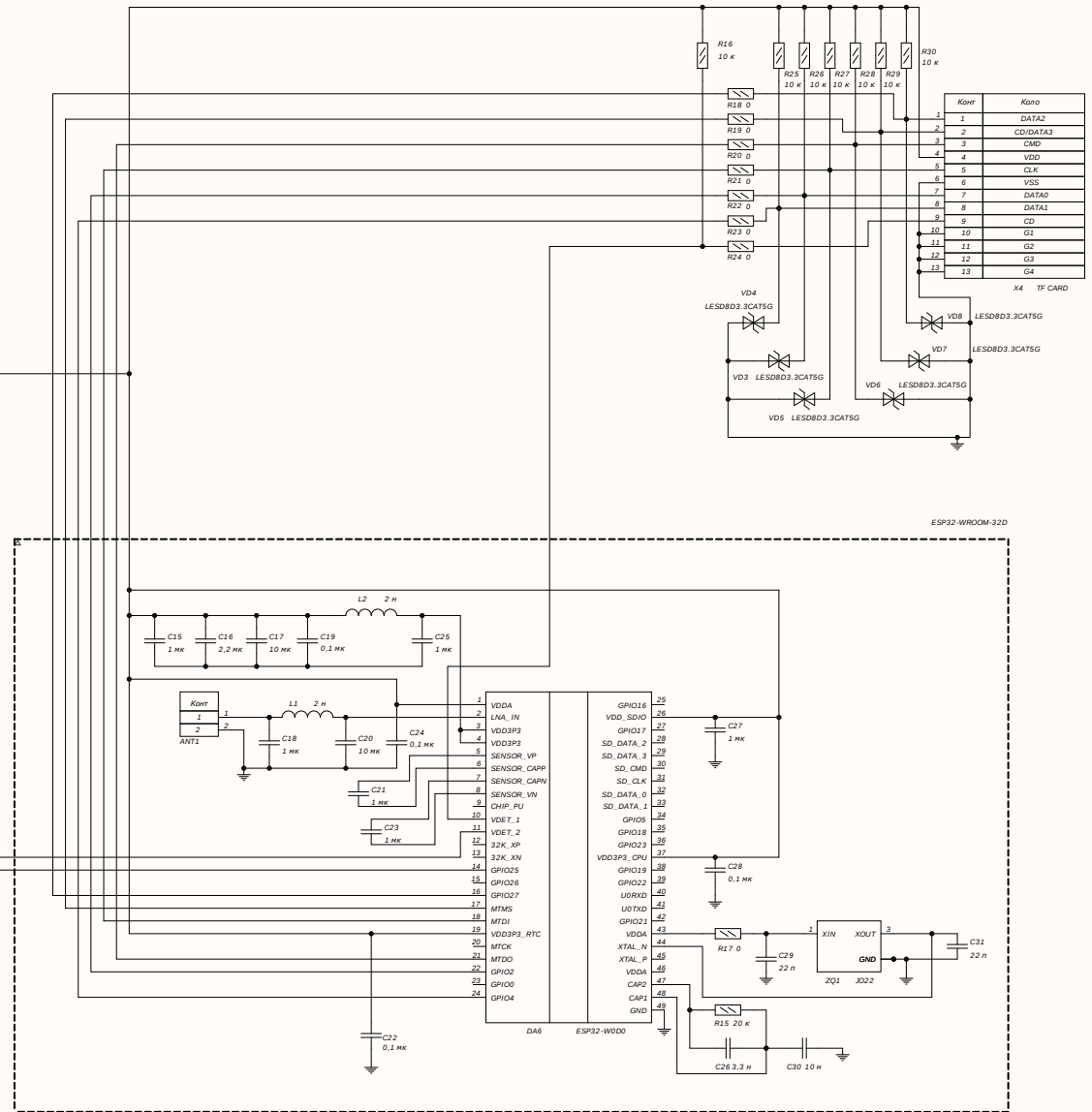
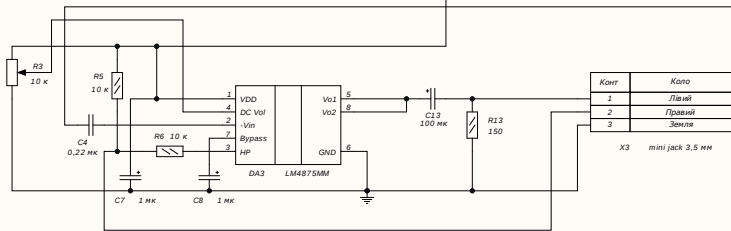
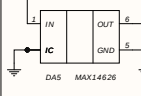
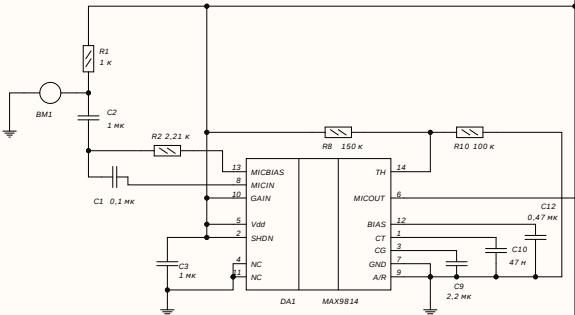
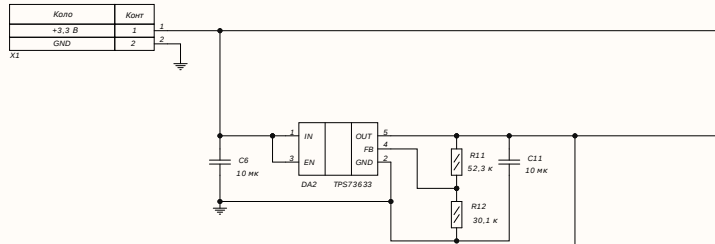
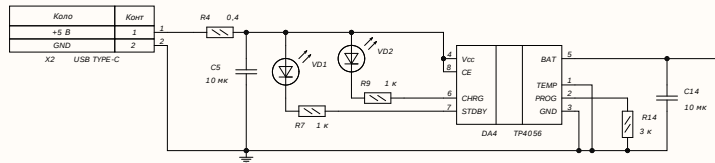
Виконавець

Томчук І.В. _____

Керівник

Старший викладач, Павлов О.І.

[illegible]



						PC81.466459.001 E3			
Эп. лист	№ докум.	Платим.	Дата	Криптографичний аудио-терміяльний пристрій схема електрична принципова			Л/т.	Маса	Масштаб
Розроб.	Томчук І.В.								
Рисув.	Павлов О.І.								
Т. контр.									
Н. контр.							Лист 1	Листів 1	
Зав.	Павлов О.І.						РС-81 РГО		

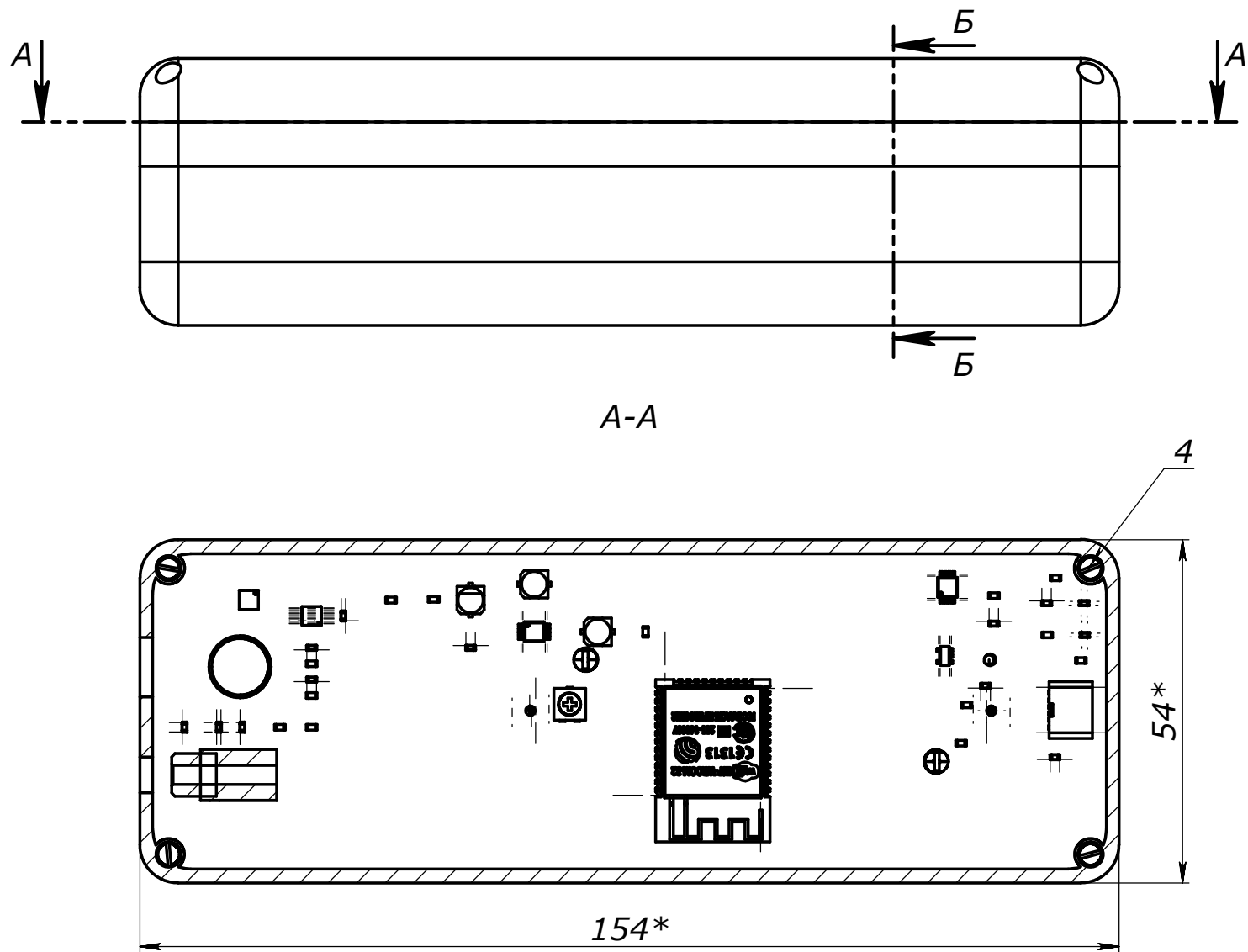
[illegible]

[illegible]

					PC81.466459.001 СК				
					Криптографічний аудіо-термінальний пристрій складальний кресленик	Лім.	Маса	Масштаб	
Зм.	Арк.	№ докум.	Підпис	Дата				1:1	
Розроб.	Томчук І.В.								
Перевір.									
Т. контр.						Аркуш	1	Аркушів	1
						PC-81 РТФ			
Н. контр.									
Затв.	Павлов О.І.								

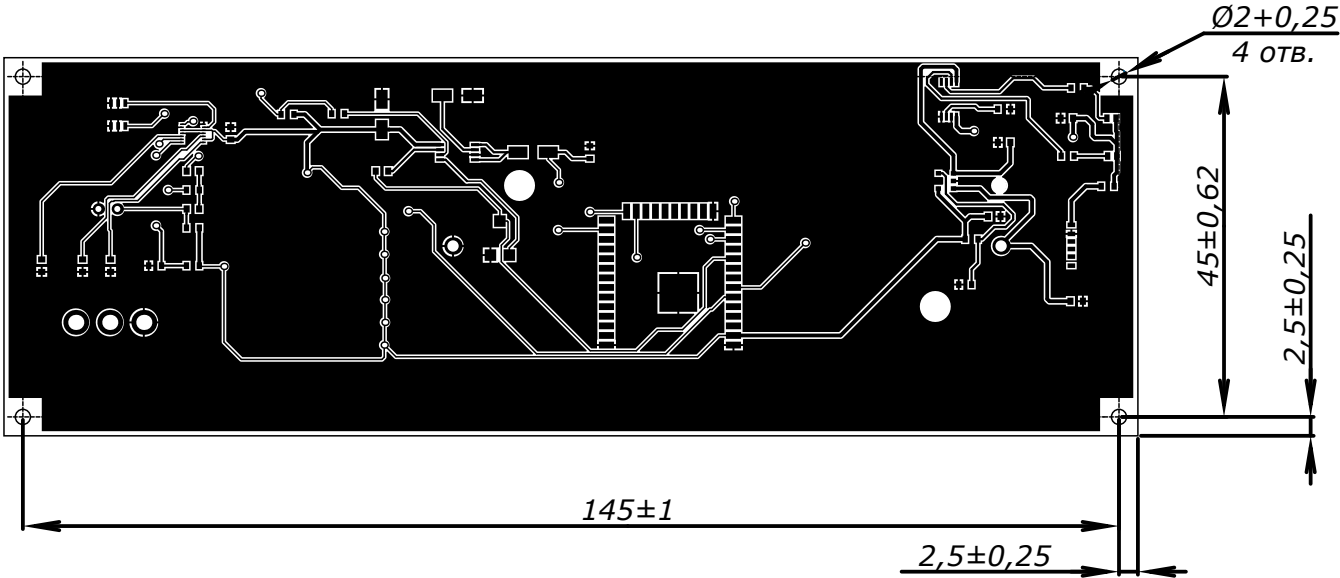
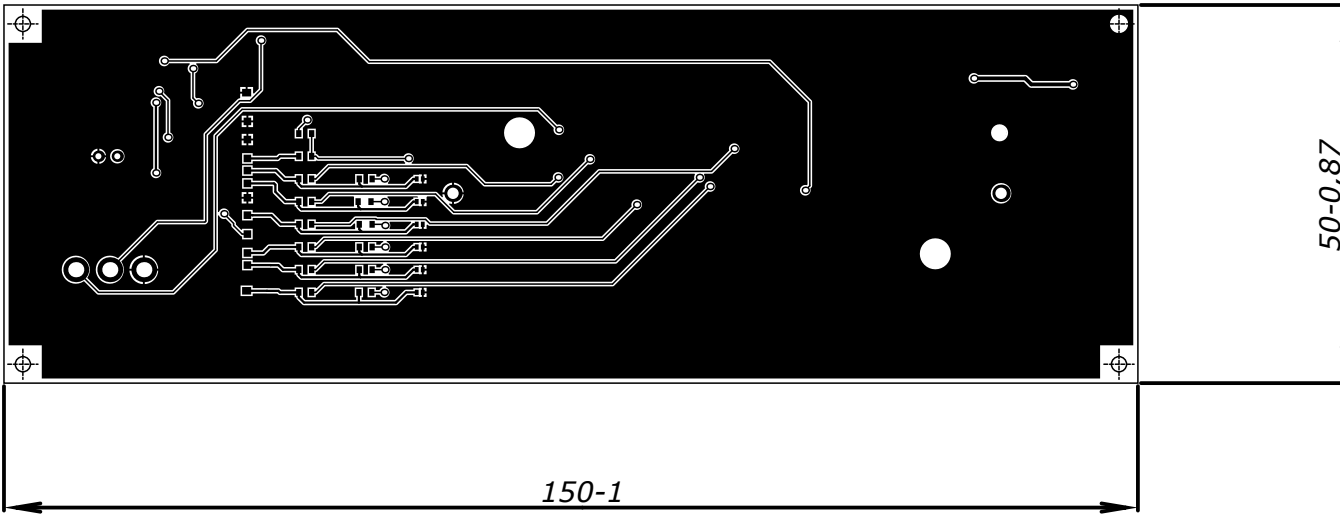
Інв. № подл.		Підп. та дата	Взам. інв. №	Інв. № дубл.	Підп. та дата	Справ. №	Перш. використ.
--------------	--	---------------	--------------	--------------	---------------	----------	-----------------

PC81.466459.001 СК



1. *Розміри для довідок
2. Монтаж проводиться згідно схеми електричної принципової PC81.466459.001 ЕЗ
3. Інші технічні вимоги по ОСТ4.ГО.070.0

					PC81.466459.001 СК										
					Криптографічний аудіо-термінальний пристрій складальний кресленик	Літ.			Маса			Масштаб			
Зм.	Лист	№ докум.	Підп.	Дата											
Розроб.	Томчук І.В.														
Перев.															
Т. контр.															
						Лист 1			Листів 1						
Н. контр.					:	PC-81 РТФ									
Затв.	Павлов О.І.														

Перв. застосування	Довідк. №	Підп. и дата	Зам. інв. №	Інв. № ориг.	Інв. № ориг.	Підп. и дата	Інв. № ориг.
PC81.466459.001					Ra10 ✓ (✓)		
					1. *Розміри для довідок 2. Плату виготовлено комбінованим позитивним методом 3. Клас точності 3 за ГОСТ 23751-86 4. Координати отворів Diplom.txt Топологія верхнього шару металізації в файлі TL.cam Топологія верхнього шару захистної маски в файлі TS.cam Топологія верхнього шару шовкографії в файлі TO.cam Топологія верхнього шару паяльної пасти в файлі TP.cam Топологія нижнього шару паяльної пасти в файлі BP.cam Топологія нижнього шару шовкографії в файлі BO.cam Топологія нижнього шару захистної маски в файлі BS.cam Топологія нижнього шару металізації в файлі BL.cam 5. Інші технічні вимоги по ОСТ4.ГО.010.070.014		
					PC81.466459.001		
					Криптографічний аудіо-термінальний пристрій		
					друкована плата		
					FR-4 105/105 1,5		
					PC-81		
					Копіював		
					Формат А3		

Інв. № ориг.	Підп. і дата	Зам. інв. №	Інв. № ориг.	Підп. і дата	Інв. № ориг.	Підп. і дата	Перв. застосування	PC81.466459.001 E1																																																																			
									<table><tr><td colspan="5">PC81.466459.001 E1</td><td colspan="3">Криптографічний аудіо-термінальний пристрій</td><td>Лім.</td><td>Маса</td><td>Масштаб</td></tr><tr><td>Зм.</td><td>Арк.</td><td>№ докум.</td><td>Підпис</td><td>Дата</td><td colspan="3" rowspan="3">схема структурна</td><td></td><td></td><td></td><td rowspan="2">1:1</td></tr><tr><td>Розроб.</td><td>Томчук І.В.</td><td></td><td></td><td></td></tr><tr><td>Перевір.</td><td></td><td></td><td></td><td></td></tr><tr><td>Т. контр.</td><td></td><td></td><td></td><td></td><td colspan="3" rowspan="3"></td><td colspan="3">Аркуш 1</td><td colspan="2">Аркушів 1</td></tr><tr><td>Н. контр.</td><td></td><td></td><td></td><td></td></tr><tr><td>Затв.</td><td>Павлов О.І.</td><td></td><td></td><td></td></tr></table>											PC81.466459.001 E1					Криптографічний аудіо-термінальний пристрій			Лім.	Маса	Масштаб	Зм.	Арк.	№ докум.	Підпис	Дата	схема структурна						1:1	Розроб.	Томчук І.В.				Перевір.					Т. контр.								Аркуш 1			Аркушів 1		Н. контр.					Затв.	Павлов О.І.			
PC81.466459.001 E1					Криптографічний аудіо-термінальний пристрій			Лім.	Маса	Масштаб																																																																	
Зм.	Арк.	№ докум.	Підпис	Дата	схема структурна						1:1																																																																
Розроб.	Томчук І.В.																																																																										
Перевір.																																																																											
Т. контр.								Аркуш 1			Аркушів 1																																																																
Н. контр.																																																																											
Затв.	Павлов О.І.																																																																										
									Копіював																																																																		
									Формат А3																																																																		

Інв. № ориг.	Підп. и дата	Зам. інв. №	Інв. № ориг.	Підп. и дата	Інв. № ориг.	Підп. и дата	Довідк. №	Перв. застосування	PC81.466459.002 E1																																																																					
Вед сервер та хмара криптографічний термінал криптографічний термінал криптографічний термінал Мережа мобільного зв'язку Мобільний телефон Wifi роутер Мережа інтернет Мобільний телефон Месенжер, Telegram, Viber Мобільний застосунок Криптографічний термінал																																																																														
<table><tr><td></td><td></td><td></td><td></td><td></td><td colspan="5">PC81.466459.002 E1</td></tr><tr><td>Зм.</td><td>Арк.</td><td>№ докум.</td><td>Підпис</td><td>Дата</td><td colspan="3" rowspan="4">Криптографічний аудіо термінальний пристрій схема структурна</td><td>Літ.</td><td>Маса</td><td>Масштаб</td></tr><tr><td>Розроб.</td><td></td><td>Томчук І.В.</td><td></td><td></td><td></td><td></td><td></td><td>1:1</td></tr><tr><td>Перевір.</td><td></td><td></td><td></td><td></td><td colspan="3">Аркуш 1</td><td>Аркушів 1</td></tr><tr><td>Т. контр.</td><td></td><td></td><td></td><td></td><td colspan="3"></td></tr><tr><td>Н. контр.</td><td></td><td></td><td></td><td></td><td colspan="3"></td><td colspan="3"></td></tr><tr><td>Затв.</td><td></td><td>Павлов О.І.</td><td></td><td></td><td colspan="3"></td><td colspan="3"></td></tr></table>															PC81.466459.002 E1					Зм.	Арк.	№ докум.	Підпис	Дата	Криптографічний аудіо термінальний пристрій схема структурна			Літ.	Маса	Масштаб	Розроб.		Томчук І.В.						1:1	Перевір.					Аркуш 1			Аркушів 1	Т. контр.								Н. контр.											Затв.		Павлов О.І.								
					PC81.466459.002 E1																																																																									
Зм.	Арк.	№ докум.	Підпис	Дата	Криптографічний аудіо термінальний пристрій схема структурна			Літ.	Маса	Масштаб																																																																				
Розроб.		Томчук І.В.									1:1																																																																			
Перевір.								Аркуш 1			Аркушів 1																																																																			
Т. контр.																																																																														
Н. контр.																																																																														
Затв.		Павлов О.І.																																																																												
Копіював																																																																														
Формат А3																																																																														