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

Теплоенергетичний факультет

Кафедра автоматизації проектування енергетичних процесів і систем

«На правах рукопису»
УДК _____

«До захисту допущено»

Завідувач кафедри
_____ _О. В. Коваль___
(підпис) (ініціали, прізвище)
“___”_____2019 р.

Магістерська дисертація

зі спеціальності (спеціальзації) 122 – комп’ютерні науки
Освітньо-професійна програма Комп’ютерний моніторинг та геометричне моделювання процесів та систем

на тему Побудова системи протидії атакам по стороннім каналам на захищенний бездротовий зв'язок пристроїв введення інформації.

Виконав: студент 6-го курсу, групи ТМ-81мп

Кропенко Дмитро Олегович _____
(прізвище, ім’я, по батькові) (підпис)

Керівник к.т.н., доцент Ходаковський О.В. _____
(посада, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”

Факультет теплоенергетичний

Кафедра автоматизації проектування енергетичних процесів і систем

Рівень вищої освіти другий (магістерський) за освітньо-професійною програмою

Спеціальність 122 – комп’ютерні науки та інформаційні технології

Освітньо-професійна програма Комп’ютерний моніторинг та геометричне моделювання процесів та систем

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ О.В. Коваль
(підпис)
”___”_____2019р.

ЗАВДАННЯ
на дипломну роботу студенту
Кропенку Дмитру Олеговичу
(прізвище, ім’я, по батькові)

1. Тема дисертації Побудова системи протидії атакам по стороннім каналам на захищенний бездротовий зв'язок пристроїв введення інформації
науковий керівник дисертації к.т.н., доцент Ходаковський О.В.
(прізвище, ім’я, по батькові науковий ступінь, вчене звання)

затверджені наказом по університету від «___»_____ 20__ р. No_____

2. Строк подання студентом роботи _____
3. Об’єкт дослідження методи протидії атакам по стороннім каналам на захищенний бездротовий зв'язок пристроїв введення інформації
4. Вихідні дані система протидії атакам по стороннім каналам на захищенний бездротовий зв'язок пристроїв введення інформації
5. Перелік завдань, які потрібно розробити
   1. Аналіз існуючих методів атак по постороннім атакам на захищені пристрої введення інформації та методи їм протидії.
   2. Розробка методу протидії атакам по постороннім каналам.
   3. Реалізація програмно-апаратного комплексу протидії атакам.
   4. Розробка стартап-проекту.
6. Орієнтовний перелік графічного (ілюстративного) матеріалу

презентація на тему “ Побудова системи протидії атакам по стороннім каналам на захищенний бездротовий зв'язок пристроїв введення інформації”___

7. Орієнтовний перелік публікацій

Кропенко Д.О., Ходаковський О.В. Захист шифрованого бездротового зв’язку пристроїв введення інформації від атак по постороннім каналам // Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення"(випуск 43)

8. Дата видачі завдання ”__”_____2019 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітки
1.	Отримання завдання	30.11.2018	
2.	Збір інформації	12.12.2018	
3.	Аналіз вимог завдання, вибір методів і засобів розв’язання поставленої задачі	15.02.2019	
4.	Підготовка матеріалів магістерської роботи	05.03.2019	
5.	Проміжний контроль підготовки	06.09.2019	
6.	Підготовка публікацій	15.10.2019	
7.	Підготовка доповідей на конференціях за темою магістерської роботи	27.10.2019	
8.	Доповідь на конференції	14.11.2019	
9.	Написання основних розділів автореферату	23.10.2019	
10.	Звіт за перший рік роботи над магістерською дисертацією	20.11.2019	

Студент _____ _____
(підпис) (прізвище та ініціали,)

Науковий керівник дисертації _____ _____
(підпис) (прізвище та ініціали,)

РЕФЕРАТ

Структура та обсяг магістерської дисертації

Магістерська дисертація складається зі вступу, чотирьох розділів, висновку, переліку посилань з 17 найменувань, містить 22 рисунки, 26 таблиць. Повний обсяг магістерської дисертації складає 89 сторінок, з яких перелік посилань займає 2 сторінки, додатки займають 11 сторінок.

Актуальність теми. Оскільки бездротові технології стали для нас звичайним явищем, ми зачасто вважаємо їх безпечними і все більше людей використовують бездротові периферійні пристрої, оскільки останні вже майже зрівнялися за ціною з дротовими. Сьогодні не існує стандартів, що регулюють безпеку бездротових периферійних пристроїв, що функціонують на радіочастоті 2,4 ГГц. Із цієї причини питання захисту таких пристроїв від взлому залишається на виробниках. Більше того, захищенний бездротовий зв’язок надійними та перевіреними алгоритмами шифрування даних є вразливим до атак по стороннім каналам: завдяки останнім досягненням в математиці є можливим проаналізувати зв’язок та частково або повністю відновити зміст передаючої інформації пристроями введення.

Мета дослідження полягає в розробці методу та системи протидії атакам по стороннім каналам на захищенний зв’язок пристроїв введення інформації.

Для досягнення поставленої задачі були сформульовані наступні **завдання дослідження**, що визначили логіку дослідження та його структуру:

- дослідити існуючі захищені бездротові пристрої введення інформації (ЗБПВІ);
- дослідити існуючі вектори та технології атаки по постороннім каналам;
- дослідити можливості застосування атак по постороннім атакам проти ЗБПВІ;
- розробити алгоритм активного захисту ЗБПВІ;
- реалізувати пристрій активного захисту ЗБПВІ;
- провести аналіз роботи пристрою.

Об’єктом дослідження є захищений бездротовий зв’язок пристроїв введення інформації.

Предметом дослідження є система протидії атакам по стороннім каналам на захищенний бездротовий зв’язок пристроїв введеня інформації.

Методи дослідження. Розв’язання поставлених задач виконувались з використанням наступних методів:

- безпосередній аналіз зв’язку за допомогою SDR;
- метод k-середніх та відстань для вилучення інформації із захищенного бездротового зв’язку.

Наукова новизна одержаних результатів. Найбільш суттєвими науковими результатами магістерської дисертації є:

- описано спосіб для аналізу інформації, передаючої про захищеному бездротовому зв’язку пристроїв введення інформації;
- створено метод протидії атакам по стороннім каналам на захищенний бездротовий зв'язок пристроїв введення інформації.

Практичне значення одержаних результатів роботи полягає в розробці методу протидії атакам по стороннім каналам на захищенний бездротовий зв'язок пристроїв введення інформації.

Апробації результатів дисертації. Результати досліджень оприлюднені на Міжнародній науковій інтернет-конференції "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення"(випуск 43)”.

Публікації. Наукові положення дипломної роботи опубліковані у 1 роботі.

Кропенко Д.О., Ходаковський О.В. Захист шифрованого бездротового зв’язку пристроїв введення інформації від атак по постороннім каналам // Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення"(випуск 43)

Ключові слова. *ПАКЕТ ДАНИХ, КЛАСТЕРИЗАЦІЯ, ЧАСОВІ МОМЕНТИ, ЕЙЛЕРОВА ВІДСТАНЬ, ЗАХИЩЕНИЙ ЗВ’ЯЗОК.*

РЕФЕРАТ

Структура и объем магистерской диссертации

Магистерская диссертация состоит из введения, четырех глав, заключения, списка ссылок из 17 наименований, содержит 22 рисунка, 26 таблиц. Полный объем магистерской диссертации составляет 89 страниц, из которых перечень ссылок занимает 2 страницы, приложения занимают 11 страниц.

Актуальность темы. Поскольку беспроводные технологии стали для нас обыденным явлением, мы часто считаем их безопасными и все больше людей пользуются беспроводными периферийными устройствами, поскольку последние уже практически сравнялись по цене с проволочными. На сегодняшний день отсутствуют стандарты, регулирующие безопасность беспроводных периферийных устройств, функционирующих на радиочастоте 2,4 ГГц. По этой причине вопросы защиты таких устройств от взлома остается на производителях. Более того, защищенный беспроводной связи надежными и проверенными методами шифрования данных является уязвимым к атакам по сторонним каналам: благодаря последним достижениям в математике возможно проанализировать связь и частично или полностью восстановить содержание передающей информации устройствами ввода.

Цель исследования заключается в разработке метода и системы противодействия атакам по сторонним каналам на защищенный связь устройств ввода информации.

Для достижения поставленной задачи были сформулированы следующие **задачи исследования**, определили логику исследования и его структуру:

- исследовать существующие защищеные беспроводные устройства ввода информации (ЗБУВИ);
- исследовать существующие векторы и технологии атаки по посторонним каналам;

- исследовать возможности применения атак по посторонним атакам против ЗБУВИ;
- разработать алгоритм активной защиты ЗБУВИ;
- реализовать устройство активной защиты ЗБУВИ;
- провести анализ работы устройства.

Объектом исследования является защищенная беспроводная связь устройств ввода информации.

Предметом исследования является система противодействия атакам по сторонним каналам на защищенную беспроводную связь устройств ввода информации.

Методы исследования. Решение поставленных задач выполнялись с использованием следующих методов:

- непосредственный анализ связи с помощью SDR;
- метод k-средних и расстояние для извлечения информации из защищенной беспроводной связи.

Научная новизна полученных результатов. Наиболее существенными научными результатами магистерской диссертации является:

- описывается алгоритм анализа информации, передающей о защищенном беспроводной связи устройств ввода информации;
- создан метод противодействия атакам по сторонним каналам на защищенную беспроводную связь устройств ввода информации.

Практическое значение полученных результатов работы заключается в разработке метода противодействия атакам по сторонним каналам на защищенный беспроводной связи устройств ввода информации.

Апробации результатов диссертации. Результаты исследований опубликованы на Международной научной интернет-конференции "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення" (выпуск 43)

Публикации. Научные положения дипломной работы опубликованы в 1 работе.

Кропенко Д.О., Ходаковський О.В. Захист шифрованого бездротового зв’язку пристроїв введення інформації від атак по постороннім каналам // Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення"(випуск 43)

Ключевые слова. *ПАКЕТ ДАННЫХ, КЛАСТЕРИЗАЦИЯ, ВРЕМЕННОЙ МОМЕНТ, ЭЙЛЕРОВО РАССТОЯНИЕ, ЗАЩИЩЁННАЯ СВЯЗЬ.*

ABSTRACT

The structure and scope of the master's thesis

The master's thesis consists of an introduction, four chapters, a conclusion, a list of links of 17 items, contains 22 figures, 26 tables. The full volume of the master's thesis is 89 pages, of which a list of links takes 2 pages, additionals takes 11 pages.

Relevance of the topic. Since wireless technologies have become commonplace for us, we often consider them safe and more and more people use wireless peripherals, since the latter are almost equal in price to wire ones. To date, there are no standards governing the safety of wireless peripherals operating on the 2.4 GHz radio frequency. For this reason, issues of protecting such devices from hacking remain with manufacturers. Moreover, secure wireless communications with reliable and proven data encryption methods is vulnerable to attacks by third-party channels: thanks to the latest advances in mathematics, it is possible to analyze the connection and partially or completely restore the contents of the transmitting information by input devices.

The purpose of the study is to develop a method and system to counter attacks through third-party channels to a secure connection of information input devices.

To achieve this goal, the following **research objectives** were formulated, the research logic and its structure were determined:

- explore existing secure wireless information input devices (ZBUVI);
- explore existing vectors and attack technologies through extraneous channels;
- explore the possibility of using attacks against extraneous attacks against ZBUVI;
- develop an active protection algorithm for ZBUVI;
- implement an active protection device ZBUVI;
- analyze the operation of the device.

The object of research is a secure wireless communication devices input information.

The subject of this research is a system of counteracting attacks through third-party channels to secure wireless communication of input devices.

Research Methods. The solution of the tasks was carried out using the following methods:

- direct communication analysis using SDR;
- k-means method and distance to extract information from secure wireless.

The scientific novelty of the results. The most significant scientific results of the master's thesis are:

- an algorithm for analyzing information transmitting about secure wireless communication of input devices is described;
- a method has been created to counter attacks through third-party channels to secure wireless communications of input devices.

The practical significance of the obtained results consists in the development of a method of counteracting attacks through third-party channels on secure wireless communication devices for inputting information.

Testing the results of the dissertation. The research results were published at the International Scientific Internet Conference "Information suspension: technology, economy and technology aspects of becoming" (issue 43)

Publications. The scientific provisions of the thesis are published in 1 work.

Кропенко Д.О., Ходаковський О.В. Захист шифрованого бездротового зв’язку пристроїв введення інформації від атак по постороннім каналам // Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення"(випуск 43)

Keywords. *DATA PACKAGE, CLUSTERING, TIME MOMENT, EULER DISTANCE, PROTECTED COMMUNICATION.*

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

CSC — контрольна сума, що використовується для перевірки цілісності даних під час передачі та збереженні.

USB — Universal Serial Bus інтерфейс, що використовується для під’єднання периферійних пристроїв.

RPi — Raspberry Pi.

Аутентифікація — процедура перевірки достовірності даних.

Донгл — радіоприймач, що під’єднується до комп’ютера через USB.

ЗБПВІ — захищені бездротові пристрої введення інформації

ІЧ — інфрачервоний інтерфейс.

Периферійний пристрій — пристрій, що дозволяє вводити інфомацію у комп’ютер.

ПК — персональний комп’ютер.

ГВЧ — генератор випадкових чисел

ПОСТАНОВКА ЗАДАЧІ

Для даної дипломної роботи поставлені такі задачі:

1. Дослідити існуючі захищені бездротові пристрої введення інформації (ЗБПВІ)
2. Дослідити існуючі вектори та технології атаки по постороннім каналам
3. Дослідити можливості застосування атак по постороннім атакам проти ЗБПВІ
4. Розробити алгоритм активного захисту ЗБПВІ
5. Реалізувати пристрій активного захисту ЗБПВІ
6. Провести аналіз роботи пристрою
7. Оформити результати роботи у вигляді пояснювальної записки згідно ДСТУ 3008-95 від 29.12.1993 №8.3-5/1259

ВСТУП

У сьогоднішньому світі мобільних технологій бездротове з’єднання використовується усюди. Ми використовуємо його для того, щоб користуватися Інтернетом у дорозі, під’єднувати мобільні пристрої та аксесуари до свого ПК, слухати музику із телефону — цей перелік можна продовжувати. Така як бездротові технології стали для нас посякденним явищем, ми зачасто вважаємо їх достатньо безпечними та все більше використовуємо бездротовимі периферійні пристрої, оскільки останні майже вже зрівнялися із ціною дротових, однак мало хто замислюється, що саме такі пристрої не захищені від злому.

Сьогодні не існує стандартів, що регулюють безпеку бездротових периферійних пристроїв, що функціонують на радіочастоті 2,4 ГГц. Із цієї причини питання захисту таких пристроїв від взлому залишається на виробниках. Більше того, захищенний бездротовий зв’язок надійними та перевіреними алгоритмами шифрування даних є вразливим до атак по стороннім каналам: завдяки останнім досягненням в математиці є можливим проаналізувати зв’язок та частково або повністю відновити зміст передаючої інформації пристроями введення.

Більш того, навіть захищенний бездротовий зв’язок надійними та перевіреними алгоритмами шифрування даних є вразливим до атак по постороннім каналам: завдяки останнім досягненням в математиці є можливим проаналізувати зв’язок та частково або повністю відновити зміст передаючої інформації пристроями введення.

Метою даної магістерської дисертації є дослідження існуючих векторів атак по постороннім каналам, дослідження та реалізація методу протидії атакам, а також створення робочої моделі.

РОЗДІЛ 1. АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ АТАК ПО ПОСТОРОННІМ АТАКАМ НА ЗАХИЩЕНІ ПРИСТРОЇ ВВЕДЕННЯ ІНФОРМАЦІЇ ТА МЕТОДИ ЇМ ПРОТИДІЇ

1.1 Типи підключеннь бездротових периферійних пристроїв введення

Використовують такі типи бездротового зв’язку:

- радіочастотний;
- інфрачервоний (ІЧ);
- Bluetooth;
- Wi-Fi.

За наявності ІЧ-інтерфейсу передача даних виконується по оптичному каналу в інфрачервоному діапазоні. Головними перевагами ІЧ-технології є низька ціна, відносно великий радіус дії (до декількох десятків метрів) та низький рівень енергоспоживання. Із основних недоліків ІЧ-технології можна виділити необхідність забезпечення прямої видимості поміж оптичними сенсорами приймача та передавача, і також обмежені допуски на кут їх відхилення відносно один одного. Цю технологію рідко використовують у бездротових клавіатурах та мишках.

Технологія Wi-Fi відзначається дуже великим радіусом дії, а також стабільною роботою. Недоліком є саме те, що пристрій повинен бути постійно підключеним до локальної мережі і не буде працювати за її відсутності.

Bluetooth — технологія бездротового зв'язку, що створена в 1998 році групою компаній: Ericsson, IBM, Intel, Nokia, Toshiba.

Основне застосування Bluetooth — забезпечення економного (з точки зору споживаного струму) та дешевого радіозв'язку між різноманітними типами

комп’ютерних пристроїв, такі як мобільні телефони та аксесуари до них, портативні і настільні комп'ютери, принтери та інші пристрої.

До недоліків можна виднести те, що передача інформації через Bluetooth має набагато більшу затримку, ніж у радіопередавачів.

Радіо — різновид бездротового зв'язку, у якому в якості носія сигналу використовуються короткі радіохвилі, що вільно поширювані в просторі.

Передача відбувається таким чином: на передаваючій стороні формулюється сигнал із необхідними характеристиками (частота та амплітуда сигналу). Надалі сигнал модулює більш частотне коливання та випромінюється антеною у повітря. На приймаючій стороні сигнал демодулюється та фільтрується. Таким чином, відбувається виділення корисного сигналу. Отриманий сигнал може трохи відрізнятися від переданого передаючим пристроєм (спотворення внаслідок перешкод і наведень).

Переваги:

- надшвидший відгук на дії користувача в порівнянні із Bluetooth;
- використання режиму економного енергоспоживання;
- низька ціна на ринку. Ціна практично зрівнялася із провідними аналогами.

Недоліки:

- необхідність підключення донглу до компєютера через USB порт;
- відсутність стандарту, який регулює безпеку радіобездротових пристроїв введення, що працюють на частоті 2,4 ГГЦ;
- у деяких моделях не використовуються ані механізми аутентифікації, ані шифрування даних, що потенційно дозволяє видати свій пристрій за чужий.

Порівняння описаних технологій бездротового зв’язку наведено у таблиці 1.1. Слід зауважити, що дані у таблиці наведені відносно застосування у периферійних пристроях.

Надалі буде розглянуто периферійні пристрої, що мають радіочастотне з’єднання із ПК, так як саме цей тип пристроїв є найпоширенішим.

Таблиця 1.1 — Порівняння характеристик бездротового зв’язку

	ІЧ-інтерфейс	WiFi	Bluetooth	Радіочастотний
Ціна	Низька	Висока	Середня	Середня
Якість зв’язку	Низька	Висока	Висока	Висока
Швидкість передачі даних	Низька	Висока	Середня	Середня
Швидкість обробки даних	Висока	Середня	Середня	Висока
Захищеність зв’язку	Низька	Висока	Висока	Низька
Поширеність	Низька	Низька	Висока	Висока

NRF24 — це високоінтегрований радіомодуль із пониженим споживанням енергії (ULP) із швидкістю передачі даних 2Мбіт/с і працює в діапазоні радіо 2,4 ГГц. За допомогою цього модуля можна зв'язати декілька пристроїв для передачі даних по радіоканалу. Можливо об'єднати до семи приладів в єдину радіомережу на частоті 2,4 ГГц. Модуль NRF24 використовується майже у всіх сучасних периферійних пристроях. Модуль зображено на рис. 1.1.

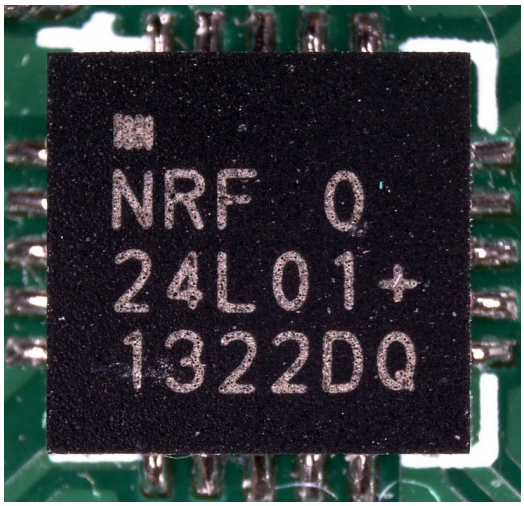


Рисунок 1.1 - Радіомодуль NRF24

За надійну та стабільну передачу та прийом даних відповідає імплементований протокол Enhanced ShockBurst — пристрою необхідно давати відповідь про прийом даних таким чином підтверджуючи зворотний зв'язок.

Звичайний пакет NRF24 надсилається по раідочастотам в наступному форматі: пакет починається із преамбули, яку радіомодуль використовує для ідентифікації вхідних пакетів. Надалі вказана адреса кінцевого вузла і може бути вказана від 2 до 6 байтів. Пізніше з'являється корисне навантаження із зафіксованим розміром, після чого йде додатковий CRC задля перевірки цілісності даних після прийому. CRC рахується по всьому пакету, за винятком CRC та преамбули. Радіоприймачу необхідно бути попередньо повідомленим про довжину корисного навантаження, так як звичайний пакет не містить інформації про довжину. Коли отриманий пакет відповідає адресу приймача радіо, а CRC проходить перевірку, модуль зберігає корисне навантаження у внутрішній пам’яті пристрою для наступного вивантаження мікроконтролером. Структуру типового пакету зображено на рис. 1.2.

Преамбула (1 байт)	Адреса (2-6 байт)	Корисне навантаженя (32 байт)	CRC (0-2 байт)

Рисунок 1.2 - Структура типового пакету

Модуль NRF24 має режим "Enhanced Shockburst", що має ряд переваг перед використання типових пакетів, а саме:

- довжина навантаження пакету може бути встановлена динамічно і є частиною структури пакету. Отримуючий вузол має можливість автоматично відсилати підтвердження відправнику для того, щоб указати на те, що пакет був отриманий правильно;
- відправник в автоматичному режимі повторить передачу кілька разів, поки підтвердження не буде оброблено у налаштованому таймауті; цей алгоритм називається "Автоматизована обробка транзакцій пакетів".

Структура пакету у режимі "Enhanced Shockburst" зображено на рис. 1.3.

Преамбула (1 байт)	Адреса (2-6 байт)	Розмір корисного навантаження (6 біт)	PID (2 біт)	NO_ACK (1 байт)	Корисне навантаження (0-32 байт)	CRC (1-2 байт)

Рисунок 1.3 - структура пакету режиму "Enhanced Shockburst"

Можна побачити, що було додано дев’ятибітне поле для керуванням пакетом, що зберігає розмір корисного завантаження (у байтах), ідентифікатор пакету (PID) для виявлення повторних передач та тригер, що призводить до припинення відправлення пакетів підтвердження на основі кожного пакету. Також CRC тепер є обов'язковим. Як і звичайний пакет, отриманий пакет повинен відповідати адресі приймача радіо, а CRC повинен бути дійсним, щоб зберегти навантаження у внутрішній пам'яті, в іншому випадку повідомлення буде скинуто.

1.2 Існуючі вектори атак по стороннім каналам

Існують такі типи атак по стороннім каналам:

- атака зондуванням;
- атака за часом;
- атака за помилками обчислення;
- атака за енергоспоживанням;
- атака за електромагнітним випромінюванням;
- акустична атака;
- візуальна атака.

Надалі будуть розглядатися тільки ті атаки, які можна застосувати проти пристроїв із захищеним бездротовим зв’язком.

1.2.1 Візуальна атака

До даного сценарію атак відноситься візуальне спостереження за пристроєм, за допомогою якого вводиться інформація. Даний метод зазвичай не потребує технічних навичок та може виконати кожен, хто має здатність спостерігати. За допомогою додаткових пристроїв можливо збільшити дистанцію для проведення атаки.

Найдешевший пристрій для спостереження є бінокль - оптичний прилад, що складається із двох паралельно розташованих з'єднаних разом зорових труб, для спостереження віддалених предметів двома очима: за рахунок цього спостерігач бачить стереоскопічне зображення, на відміну від зорової труби. У цих біноклях кожна зорова труба має об'єктив у вигляді позитивної лінзи і окуляр у вигляді від'ємної лінзи. Труба Галілея відразу дає пряме (неперевёрнутое) зображення, тому між об'єктивом і окуляром немає інших оптичних деталей. Перевагою біноклів Галілея є компактність - вони коротші і легше всіх інших типів біноклів. Недолік - різке погіршення якості зображення при збільшеннях більше чотирикратного.

Для більш дальнього спостереження використовується оптичний телескоп — телескоп (рис. 1.4), який збирає і фокусує електромагнітне випромінювання оптичного діапазону. Його основні завдання збільшити блиск і видимий кутовий розмір об'єкта, тобто, збільшити кількість світла, що приходить від небесного тіла) і дати можливість вивчити дрібні деталі спостережуваного об'єкта. Збільшене зображення досліджуваного об'єкта спостерігається оком або фотографується. Основні параметри, які визначають характеристики телескопа - діаметр, або апертура, і фокусна відстань об'єктива, а також фокусна відстань і поле зору окуляра. Оптичний телескоп є трубою, що має об'єктив і окуляр і встановлену на монтуванні, забезпеченою механізмами для наведення на об'єкт спостереження і стеження за ним. Задня фокальна площина об'єктива поєднана з передній фокальній площиною окуляра. У фокальній площині об'єктива замість окуляра може поміщатися матричний приймач випромінювання.

Рисунок 1.4 - Телескоп

1.2.2 Акустична атака

Так як при використанні пристроїв введення інформації виникає механічний звук, його можна проаналізувати та відновити введену інформацію. Наразі у вільному доступі доступне програмне забезпечення для проведення даної атаки - keytap2 - інструмент для відновлення тексту з аудіо. Він не потребує навчальних даних - натомість використовує статистичну інформацію про частоти букв і n-грамів в англійській мові. Інструмент ще в розробці, але вже можна успішно використовувати.

Для приймання звуку можна використовувати мікрофони направленої дії, що складаються з дифузора, а також підсилювача. Багато модифікацій використовуються спецслужбами. Сучасні пристрої виробляються з фільтрами і без них. Багато модифікації здатні похвалитися високою чутливістю. Якщо вірити фахівцям, то модель доцільніше купувати з двома літієвими батарейками. Мінімальна порогова частота в середньому становить 300 МГц. Чутливість на імпедансі не перевищує 3 мВ. У багатьох моделей застосовується два підсилювача. Провідність звукового сигналу в такому випадку зростає досить сильно. Дальність прослуховування такими мікрофонами складає 200 метрів.

Для більш дальнього прослуховування використовуються лазерні мікрофони (рис. 1.5). Вони дозволяють записувати мова або інші будь-які звуки при зондуванні будь-яких поверхонь, що відбивають. Зондуємий об'єкт - віконне скло яке працює як мембрана, яка коливається з певною звуковою частотою, і при цьому створює фонограму розмови. Лазерний мікрофон генерує випромінювання, яке відбивається від поверхні скла і модулюється акустичним сигналом. При відображенні сигнал приймається фотоприймачем де вже йде розшифровка даних. Якщо сказати простіше, то при генерації акустичного сигналу, звукова хвиля досягає межі розділу повітря-скло і створює вібрацію (відхилення від початкового положення поверхні скла). Ці відхилення створюють дифракцію світла. Якщо розміри падаючого оптичного пучка маленький в порівнянні з довжиною поверхневої хвилі, то в суперпозиції буде домінувати дифракційну пучок нульового порядку. При цьому пучок гойдається з частотою звуку в дзеркальному відображенні. Даний мікрофон дозволяє прослуховувати на відстані до 1000 метрів.

Рисунок 1.5 - Лазерний мікрофон

1.2.3 Атака по електромагнітному випроміненню

Як електричні пристрої, компоненти комп'ютера часто генерують електромагнітне випромінювання як частина їх операцій. Зловмисник, який може спостерігати ці випромінювання і може зрозуміти їх причинно-наслідковий зв'язок з

базовими обчисленнями та даними, в стані вивести дивовижну кількість інформації про це обчисленні і даних. латформі, призначеної для зберігання цієї інформації від противника. Пристрій для аналізу електровипромінення зображено на рис. 1.6. Атаки по електромагнітному випромінюванню можуть також бути розділені на дві основні категорії: Простий Аналіз Електромагнітного Випромінювання і Диференціальний Аналіз Електромагнітного Випромінювання.

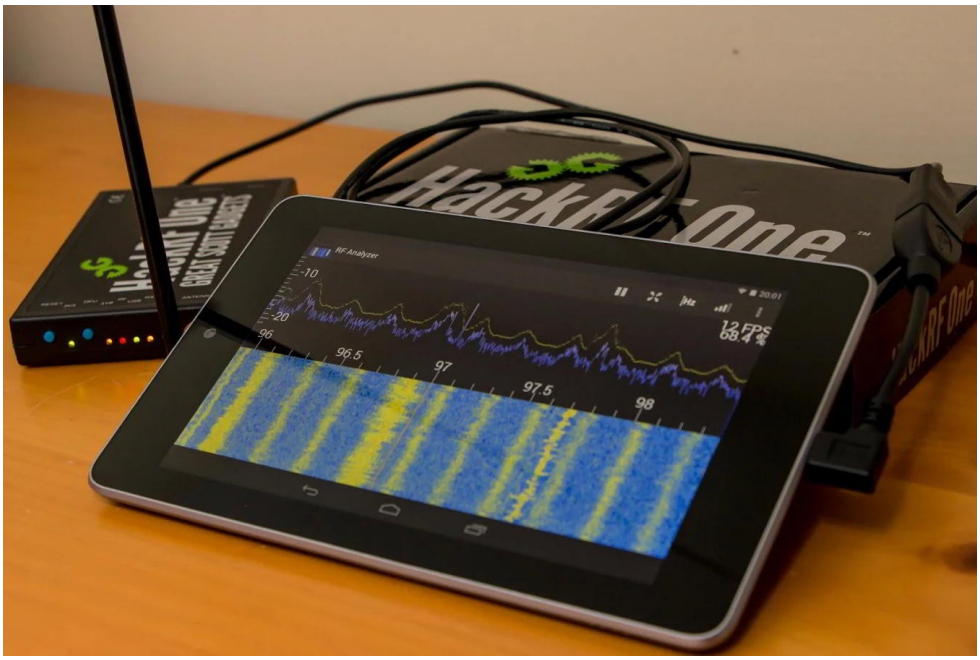


Рисунок 1.6 - Пристрій для аналізу електровипромінення

Потенціал використання електромагнітних випромінювань був відомий у військових колах протягом тривалого часу. Наприклад, недавно розсекречений документ TEMPEST, написаний Агентством Національної Безпеки, досліджує різні небажані випромінювання, включаючи електромагнітне випромінювання, лінії провідності і акустичні емісії. Несекретная література по методам атак і контрзаходів також обширна. Наприклад, Кун та інші обговорювали методи, засновані на програмному забезпеченні, для запуску і запобігання атак на основі виведення інформації на відео екрани від випускаються електромагнітних випромінювань. Результати експерименту на електромагнітних аналітичних атаках

на криптографічні пристрої, такі як смарт-карти і порівняння з атаками аналізу енергоспоживання були спочатку представлені Quisquater, а також Гандолфи.

Радіус даної атаки невеликий — до 50 метрів.

1.3 Аналіз існуючих методів та засобів захисту бездротового зв’язку

Деякі виробники передбачають перепрограмувальні донгли — це такі, у яких прошивку можна замінити. Logitech вже повідомила, що випустила модифіковану прошивку для бездротових пристроїв. На жаль, велика кількість донглів мають тільки для читання пам’ять, а отже їх вразливість виправити є неможливим, а це, в свою чергу, декілька мільйонів пристроїв, що регулярно використовуються людьми по всьому світі. Отже багато користувачів залишаються вразливими до зловмисників.

Lenovo надає консультативну підтримку та розробила оновлення прошивки. Але прошивку можна застосовувати тільки на момент виробництва. Тобто, не буде завантажених виправлень.

Компанія Dell заявила, що клієнти із пристроями, як клавіатури та миші KM714, можуть використати оновленням Logitech використовуючи технічну підтримку Dell.

Компанія Microsoft продає серію бездротових клавіатур, що допомагають захистити спілкування за допомогою покращеного стандарту шифрування (AES). Технологія шифрування AES зашифровує інформацію під час натискання клавіш до початку передачі її на комп’ютер або інший пристрій.

Покращений стандарт шифрування (AES) — розроблений Національним інститутом стандартів і технологій (National Institute of Standards and Technology – NIST) у 2001 році та прийнятий національним урядом США та інших країн із метою надійного захисту інформації та конфіденційних даних.

Клавіатури Microsoft, що використовують AES шифрування, застосовують генерування випадкових даних, тобто соління, і унікальні ідентифікатори для кожного переданого пакету даних, щоб запобігти складнішим атакам.

1.4 Висновки до першого розділу

В першому розділі були розглянуті типи бездротового з’єднання, типи атак по стороннім каналам, а також були розглянуті засоби для проведення атаки. Були розглянуті впроваджені методи захисту.

В розділі 2 поставимо за мету розробити метод атаки по постороннім каналам, а також алгоритм протидії даній атаці.

РОЗДІЛ 2. РОЗРОБКА МЕТОДУ ПРОТИДІЇ АТАКАМ ПО СТОРОННІМ КАНАЛАМ.

Для подальшої роботи необхідно проаналізувати типовий пристрій та його захищений бездротовий зв’язок.

2.1 Аналіз захищеного бездротового зв’язку типового пристрою введення інформації

Маємо пристрій введення інформації — клавіатуру Logitech K250, що використовує для з’єднання із комп’ютером донгл із радіоприймачем NRF24LU1. Клавіатуру зображено на рис. 2.1.

Для аналізу трафіку було використано RTL-SDR (рис. 2.2). RTL-SDR - це USB-донгл, який можна використовувати як комп'ютерне радіо сканер для прийому живих радіосигналів. Залежно від конкретної моделі, вона може приймати частоти від 500 кГц до 2.4 ГГц. Більшість програмного забезпечення для RTL-SDR також розробляється спільнотою та надається безкоштовно.

RTL-SDR походить від масово виготовлених телевізійних ключів DVB-T, заснованих на чіпсеті RTL2832U. Об'єднаними зусиллями Анті Палосаари, Еріка Фрі та Осмокома (зокрема, Стіва Маркграфа) було встановлено, що необроблені дані вводу / виводу на чіпсеті RTL2832U можна отримати безпосередньо, що дозволило перетворити ТВ-тюнер DVB-T у широкосмугове програмне забезпечення, визначене радіо за допомогою спеціального драйвера програмного забезпечення, розробленого Стівом Маркграфом. Якщо ви коли-небудь насолоджувалися проектом RTL-SDR, будь ласка, подумайте про пожертви Osmocom через Open Collective, оскільки саме вони розробили драйвери та реалізували RTL-SDR.

Рисунок 2.1 - Клавіатура Logitech K250

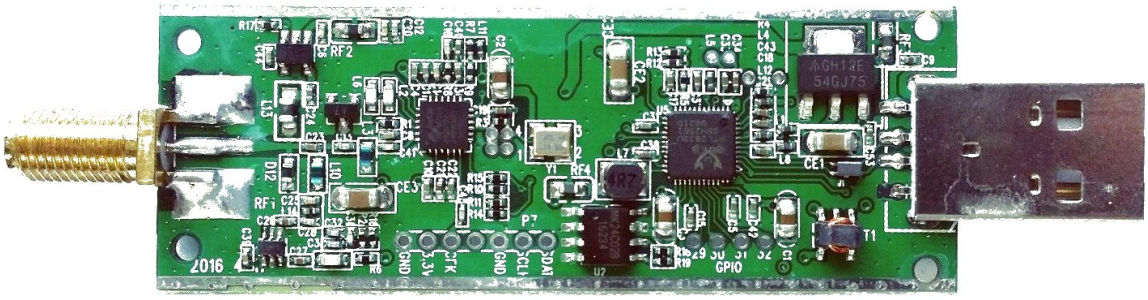


Рисунок 2.2 - Донгл RTL-SDR

За роки свого відкриття RTL-SDR став надзвичайно популярним і демократизував доступ до радіочастотного спектру. Тепер будь-хто, включаючи любителів бюджету, може отримати доступ до радіоспектру. Варто зазначити, що подібні можливості SDR коштували б сотні, а то й тисячі доларів лише кілька років

тому. RTL-SDR також іноді називають RTL2832U, DVB-T SDR, DVB-T dongle, RTL dongle, або "дешевим програмно визначеним радіо".

Радіо компоненти, такі як модулятори, демодулятори та тюнери, традиційно реалізуються в аналогових апаратних компонентах. Поява сучасних обчислювальних та аналогових цифрових перетворювачів дозволяє більшість цих традиційно апаратних компонентів реалізовувати за допомогою програмного забезпечення. Це дозволяє легко обробляти сигнал і, таким чином, виробляти дешеві широкосмугові радіо сканери.

Для аналізу сигналу було використано gqrx - програмно визначений радіоприймач, що працює на GNU Radio і інструментарії Qt GUI. Він може обробляти дані I/Q від різних типів пристроїв введення, включаючи Funcube Dongle Pro / Pro +, rtl-sdr, HackRF і універсальні програмні радіоперіферійні пристрої (USRP).

Виявлено, що для передачі натискання клавіші відправляються два пакети — під час натискання клавіші та під час відпускання клавіші. Результат аналізу роботи зв’язку зображено на рис. 2.3.

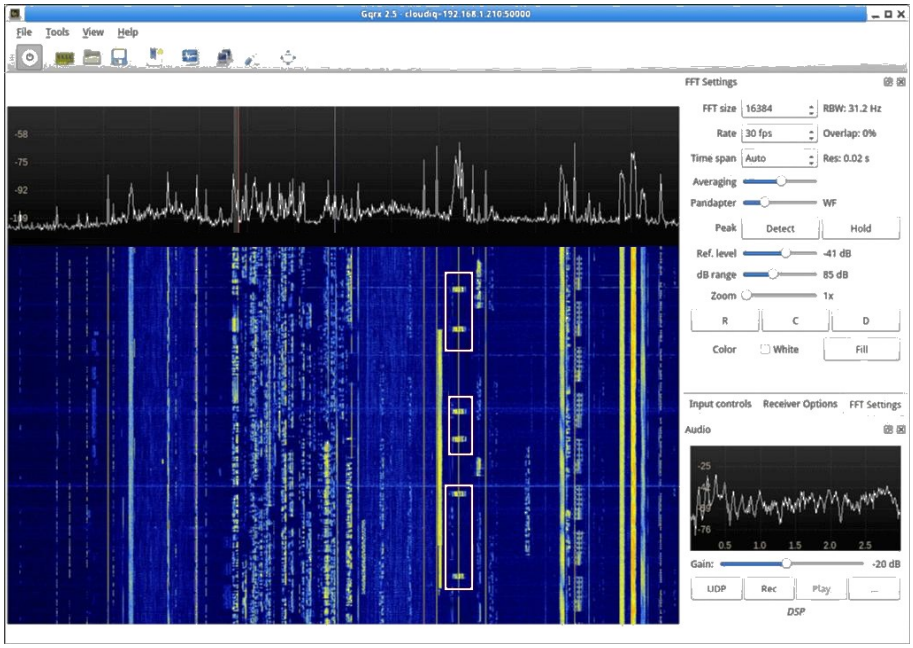


Рисунок 2.3 - Аналіз роботи зв'язку

2.2 Аналіз отриманих пакетів та вилучення інформації

Варто відмітити, що затримки між натисканнями зазвичай залежать від положення клавіші на клавіатурі, можна з певною ймовірністю відтворювати інформацію, що вводиться. Наприклад, більшість людей зазвичай набирають "s" після "a" значно швидше, ніж "g" після "s". Маючи точні моменти передачі пакетів можна дати оцінку — наскільки ці моменти відповідають тому чи іншому слову. Наприклад, при введені на клавіатурі “привіт дерево” маємо різні затримки між натисканнями. Затримки проілюстровано на рис. 2.4, де сині лінії — затримка у 150-200мс, рожеві лінії — затримка у 180-250мс, оранжеві лінії — затримка у 200-280мс, червоні лінії — затримка у 230-320мс, зелені лінії — затримка у 250-360мс, чорна цятка — затримка у 400-700мс.

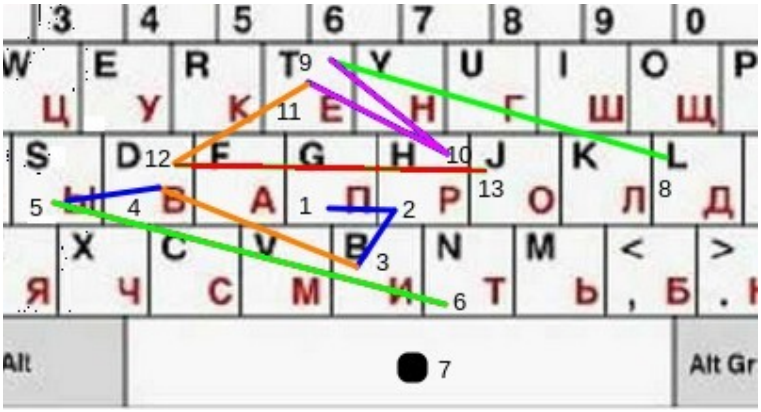


Рисунок 2.4 - Набір на клавіатурі

Для наступного аналізу необхідно мати перевірочний набір моментів та отриманий набір моментів.

Перевірочний набір моментів — набір моментів натискання та відтискання клавіш, про який відомо які саме клавіші були натиснутими. Даний набір можна отримати при звичайному наборі тексту або при чатінгу із жертвою.

Отриманий набір моментів — набір моментів натискання та відтискання клавіш, який був перехоплений при прослуховуванні трафіку жертви.

Для вилучення корисної інформації із отриманого трафіку жертви необхідно виконати наступне:

- фрагментувати отримані моменти;
- оцінка відстаней.

2.2.1 Фрагментація

Фрагментацію можна зробити вручну, автоматично, та змішано. До автоматичних можна віднести методи кластерного аналізу.

Кластеризація (або кластерний аналіз) - це задача розбиття множини об'єктів на групи, які називаються кластерами. Усередині кожної групи повинні виявитися «схожі» об'єкти, а об'єкти різних групи повинні бути якомога більш відмінні. Головна відмінність кластеризації від класифікації полягає в тому, що перелік груп чітко не заданий і визначається в процесі роботи алгоритму.

Застосування кластерного аналізу в загальному вигляді зводиться до наступних етапів:

1. Відбір вибірки об'єктів для кластеризації.
2. Визначення безлічі змінних, за якими будуть оцінюватися об'єкти у вибірці. При необхідності - нормалізація значень змінних.
3. Обчислення значень міри схожості між об'єктами.
4. Застосування методу кластерного аналізу для створення груп схожих об'єктів (кластерів).
5. Представлення результатів аналізу.

Після отримання та аналізу результатів можливе корегування обраної метрики і методу кластеризації до отримання оптимального результату.

Отже, як же визначати «схожість» об'єктів? Для початку потрібно скласти вектор характеристик для кожного об'єкта - як правило, це набір числових значень, наприклад, зростання-вага людини. Однак існують також алгоритми, що працюють з якісними (категорійними) характеристиками.

Після того, як ми визначили вектор характеристик, можна провести нормалізацію, щоб всі компоненти давали однаковий внесок при розрахунку

«відстані». У процесі нормалізації все значення приводяться до деякого діапазону, наприклад, [-1, -1] або [0, 1].

Нарешті, для кожної пари об'єктів вимірюється «відстань» між ними - ступінь схожості. Існує безліч метрик, ось лише основні з них:

Евклідова відстань - найбільш поширена функція відстані. Являє собою геометричним відстанню в багатовимірному просторі:

$$\rho(x, x') = \sqrt{\sum_{i}^{n} (x_i - x_i')^2}$$

Квадрат евклідова відстані - застосовується для додання більшої ваги більш віддаленим один від одного об'єктів. Ця відстань обчислюється таким чином:

$$\rho(x, x') = \sum_{i}^{n} (x_i - x_i')^2$$

Відстань міських кварталів (Манхеттенський відстань) - це відстань є середнім різниць по координатах. У більшості випадків ця міра відстані приводить до таких же результатів, як і для звичайного відстані Евкліда. Однак для цього заходу вплив окремих великих різниць (викидів) зменшується (тому що вони не зводяться в квадрат). Формула для розрахунку манхеттенського відстані:

$$\rho(x, x') = \sum_{i}^{n} | x_i - x_i' |$$

Відстань Чебишева - це відстань може виявитися корисним, коли потрібно визначити два об'єкти як «різні», якщо вони розрізняються за якоюсь однією координаті. Відстань Чебишева обчислюється за формулою:

$$\rho(x, x') = \max(| x_i - x_i' |)$$

Степенева відстань - застосовується в разі, коли необхідно збільшити або зменшити вагу, що відноситься до розмірності, для якої відповідні об'єкти сильно відрізняються. Статечне відстань обчислюється за такою формулою:

$$\rho(x, x') = \sqrt[r]{\sum_{i}^{n} (x_i - x_i')^p}$$

де r і p - параметри, що визначаються користувачем. Параметр p відповідальний за поступове зважування різниць за окремими координатами, параметр r

відповідальний за прогресивне зважування великих відстаней між об'єктами. Якщо обидва параметри - r і p - дорівнюють двом, то це відстань збігається з відстанню Евкліда.

Вибір метрики повністю лежить на дослідника, оскільки результати кластеризації можуть істотно відрізнятися при використанні різних заходів.

Можна виділити дві основні класифікації алгоритмів кластеризації:

- ієрархічні;
- плоскі;
- чіткі;
- нечіткі.

Ієрархічні алгоритми (також звані алгоритмами таксономії) будують не одне розбиття вибірки на непересічні кластери, а систему вкладених розбиття. Т.ч. на виході ми отримуємо дерево кластерів, коренем якого є вся вибірка, а листям - найбільш дрібні кластера.

Плоскі алгоритми будують одне розбиття об'єктів на кластери.

Чіткі (або непересічні) алгоритми кожному об'єкту вибірки ставлять у відповідність номер кластера, тобто кожен об'єкт належить тільки одному кластеру. Нечіткі (або пересічні) алгоритми кожному об'єкту ставлять у відповідність набір речових значень, що показують ступінь відносини об'єкта до кластерів. Тобто кожен об'єкт відноситься до кожного кластеру з певною ймовірністю.

У разі використання ієрархічних алгоритмів постає питання, як об'єднувати між собою кластера, як обчислювати «відстані» між ними. Існує кілька метрик.

Одиничний зв'язок (відстані найближчого сусіда) - у цьому методі відстань між двома кластерами визначається відстанню між двома найбільш близькими об'єктами (найближчими сусідами) в різних кластерах. Результуючі кластери мають тенденцію об'єднуватися в ланцюжки.

Повний зв'язок (відстань найбільш віддалених сусідів) -у цьому методі відстані між кластерами визначаються найбільшою відстанню між будь-якими двома об'єктами в різних кластерах (тобто найбільш віддаленими сусідами). Цей метод зазвичай

працює дуже добре, коли об'єкти походять з окремих груп. Якщо ж кластери мають подовжену форму або їх природний тип є «цепочечную», то цей метод непридатний.

Незважене попарне середнє -у цьому методі відстань між двома різноманітними кластерами обчислюється як середня відстань між усіма парами об'єктів в них. Метод ефективний, коли об'єкти формують різні групи, проте він працює однаково добре і в випадках протяжних («цепочечного» типу) кластерів.

Виважене попарне середнє - метод ідентичний методу невиваженого попарного середнього, за винятком того, що при обчисленнях розмір відповідних кластерів (тобто число об'єктів, що містяться в них) використовується в якості вагового коефіцієнта. Тому даний метод повинен бути використаний, коли передбачаються нерівні розміри кластерів.

Незважений центроїдного метод - у цьому методі відстань між двома кластерами визначається як відстань між їх центрами тяжкості.

Зважений центроїдного метод (медіана) - цей метод ідентичний попередньому, за винятком того, що при обчисленнях використовуються ваги для обліку різниці між розмірами кластерів. Тому, якщо є або підозрюються значні відмінності в розмірах кластерів, цей метод виявляється переважним до попереднього.

Серед алгоритмів ієрархічної кластеризації виділяються два основних типи: висхідні і низхідні алгоритми. Спадні алгоритми працюють за принципом «зверху-вниз»: на початку всі об'єкти поміщаються в один кластер, який потім розбивається на всі більш дрібні кластери. Більш поширені висхідні алгоритми, які на початку роботи поміщають кожен об'єкт в окремий кластер, а потім об'єднують кластери в усі більші, поки всі об'єкти вибірки не будуть міститися в одному кластері. Таким чином будується система вкладених розбиття. Результати таких алгоритмів зазвичай представляють у вигляді дерева - дендрограмми. Класичний приклад такого дерева - класифікація тварин і рослин.

Для обчислення відстаней між кластерами частіше все користуються двома відстанями: одиночній зв'язком або повним зв'язком.

До недоліку ієрархічних алгоритмів можна віднести систему повних розбиття, яка може бути зайвої в контексті розв'язуваної задачі.

Завдання кластеризації можна розглядати як побудова оптимального розбиття об'єктів на групи. При цьому оптимальність може бути визначена як вимога мінімізації середньоквадратичної помилки розбиття:

$$e^2(X,L) = \sum_{j=1}^{K} \sum_{i=1}^{n_j} \| x_i^{(j)} - c_j \|^2$$

де cj - «центр мас» кластера j (точка з середніми значеннями характеристик для даного кластера).

Алгоритми квадратичної помилки відносяться до типу плоских алгоритмів. Найпоширенішим алгоритмом цієї категорії є метод k-середніх. Цей алгоритм будує задане число кластерів, розташованих якнайдалі один від одного. Робота алгоритму ділиться на кілька етапів:

1. Випадково вибрати k точок, які є початковими «центрами мас» кластерів.
2. Віднести кожен об'єкт до кластеру з найближчим «центром мас».
3. Перерахувати «центримас» кластерів відповідно до їх поточним складом.
4. Якщо критерій зупинки алгоритму не задоволений, повернутися до п. 2.

Як критерій зупинки роботи алгоритму зазвичай вибирають мінімальну зміну середньоквадратичної помилки. Так само можливо зупиняти роботу алгоритму, якщо на кроці 2 не було об'єктів, що перемістилися з кластера в кластер.

До недоліків даного алгоритму можна віднести необхідність задавати кількість кластерів для розбиття.

Найбільш популярним алгоритмом нечіткої кластеризації є алгоритм c-середніх (c-means). Він являє собою модифікацію методу k-середніх. Кроки роботи алгоритму:

1. Вибрати початкове нечітке розбиття n об'єктів на k кластерів шляхом вибору матриці приналежності U розміру n x k.
2. Використовуючи матрицю U, знайти значення критерію нечіткої помилки:

$$E^2(X,U) = \sum_{i=1}^{N} \sum_{k=1}^{K} U_{ik} \| x_i^{(k)} - c_k \|^2$$

де ck - «центр мас» нечіткого кластера k:

$$c_k = \sum_{i=1}^{N} U_k x_i$$

3. Перегрупувати об'єкти з метою зменшення цього значення критерію нечіткої помилки.

4. Повертатися в п. 2 до тих пір, поки зміни матриці U не стануть незначними.

Цей алгоритм може не підійти, якщо заздалегідь невідомо число кластерів, або необхідно однозначно віднести кожен об'єкт до одного кластеру.

Суть алгоритмів, заснованих на теорії графів, полягає в тому, що вибірка об'єктів представляється у вигляді графа G = (V, E), вершинам якого відповідають об'єкти, а ребра мають вагу, рівний «відстані» між об'єктами. Перевагою графових алгоритмів кластеризації є наочність, відносна простота реалізації і можливість вносенія різних удосконалень, засновані на геометричних міркуваннях. Основними алгоритмами є алгоритм виділення зв'язкових компонент, алгоритм побудови мінімального покриває (остовного) дерева і алгоритм пошаровим кластеризації.

В алгоритмі виділення зв'язкових компонент задається вхідний параметр R і в графі видаляються всі ребра, для яких «відстані» більше R. Сполученими залишаються тільки найбільш близькі пари об'єктів. Сенс алгоритму полягає в тому, щоб підібрати таке значення R, що лежить в діапазон всіх «відстаней», при якому граф «розвалиться» на кілька зв'язкових компонент. Отримані компоненти і є кластери.

Для підбору параметра R зазвичай будується гістограма розподілів попарних відстаней. У завданнях з добре вираженою кластерної структурою даних на гістограмі буде два піки - один відповідає внутрікластерним відстаням, другий - межкластерним відстані. Параметр R підбирається із зони мінімуму між цими

піками. При цьому управляти кількістю кластерів за допомогою порога відстані досить важко.

Алгоритм мінімального покриваючого дерева спочатку будує на графі мінімальне покриває дерево, а потім послідовно видаляє ребра з найбільшою вагою. На рис. 2.5 зображено мінімальне покриває дерево, отримане для дев'яти об'єктів.

Шляхом видалення зв'язку з позначкою CD, з довжиною рівною 6 одиницям (ребро з максимальною відстанню), отримуємо два кластери: {A, B, C} і {D, E, F, G, H, I}. Другий кластер в подальшому може бути розділений ще на два кластери шляхом видалення ребра EF, яке має довжину, рівну 4,5 одиницям.

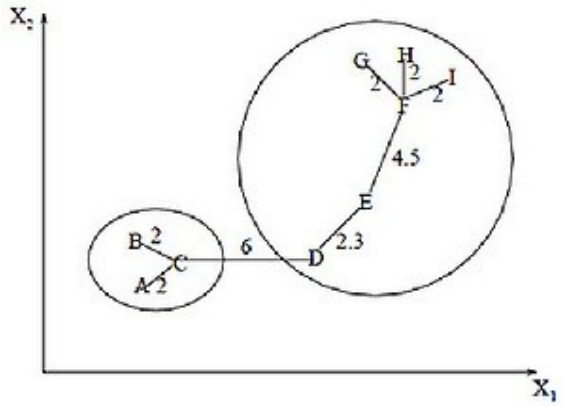


Рисунок 2.5 - Покриття дерева

Алгоритм пошарової кластеризації заснований на виділенні зв'язкових компонент графа на деякому рівні відстаней між об'єктами (вершинами). Рівень відстані задається порогом відстані c. Наприклад, якщо відстань між об'єктами, то.

Алгоритм пошарової кластеризації формує послідовність подграфов графа G, які відображають ієрархічні зв'язки між кластерами:

$$G^0 \subseteq G^1 \subseteq \ldots \subseteq G^m$$

де Gt = (V, Et) - граф на рівні ct,

,

ct - t-ий поріг відстані,

m - кількість рівнів ієрархії,

G0 = (V, o), o - порожня множина ребер графа, що отримується при t0 = 1,

Gm = G, тобто граф об'єктів без обмежень на відстань (довжину ребер графа), оскільки tm = 1.

За допомогою зміни порогів відстані {C0, ..., cm}, де 0 = C0 <c1 <... <cm = 1, можливо контролювати глибину ієрархії одержуваних кластерів. Таким чином, алгоритм пошарової кластеризації здатен створювати як плоске розбиття даних, так і ієрархічне.

2.2.2 Оцінка відстаней

Евклідова відстань - найбільш поширена функція відстані. Являє собою геометричним відстанню в багатовимірному просторі:

$$\rho(x, x') = \sqrt{\sum_{i}^{n} (x_i - x_i^{'})^2}$$

Квадрат евклідова відстань - застосовується для додання більшої ваги більш віддаленим один від одного об'єктів. Ця відстань обчислюється таким чином:

$$\rho(x, x') = \sum_{i}^{n} (x_i - x_i^{'})^2$$

Відстань міських кварталів (Манхеттенський відстань) - це відстань є середнім різниць по координатах. У більшості випадків ця міра відстані приводить до таких же результатів, як і для звичайного відстані Евкліда. Однак для цього заходу вплив окремих великих різниць (викидів) зменшується (тому що вони не зводяться в квадрат). Формула для розрахунку манхеттенського відстані:

$$\rho(x,x') = \sum_{i}^{n} | x_i - x_i^{'} |$$

Відстань Чебишева - це відстань може виявитися корисним, коли потрібно визначити два об'єкти як «різні», якщо вони розрізняються за якоюсь однією координаті. Відстань Чебишева обчислюється за формулою:

$$\rho(x, x') = \max(| x_i - x_i^{'} |)$$

Степенева відстань - застосовується в разі, коли необхідно збільшити або зменшити вагу, що відноситься до розмірності, для якої відповідні об'єкти сильно відрізняються. Статечне відстань обчислюється за такою формулою:

$$\rho(x, x') = \sqrt[r]{\sum_{i}^{n} (x_i - x_i')^p}$$

де r і p - параметри, що визначаються користувачем. Параметр p відповідальний за поступове зважування різниць за окремими координатами, параметр r відповідальний за прогресивне зважування великих відстаней між об'єктами. Якщо обидва параметри - r і p - дорівнюють двом, то це відстань збігається з відстанню Евкліда.

2.3 Висновки до другого розділу

У другому розділі був проаналізований алгоритм роботи клавіатури, описано метод атаки по стороннім каналам. Використовуючи отриману інформацію можемо створити алгоритм протидії атаким по стороннім атакам. У наступному розділі розробимо алгоритм та програмно-апаратного комплекс для протидії описаній атаці.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ ПРОТИДІЇ АТАКАМ

3.1 Елементна база

На ринку доступно декілька мікроконтроллерів, які можуть задовільнити потреби для виробництва цільового пристрою. Для вибору найкращого варіанту проведемо їх огляд.

3.1.1 Мікроконтроллери STM32

STM32 - це сімейство 32-бітних мікроконтролерних інтегральних схем від STMicroelectronics. Мікросхеми STM32 (рис. 3.1) згруповані у відповідні серії, засновані на одному і тому ж 32-бітному ядрі ARM-процесора, наприклад Cortex-M33F, Cortex-M7F, Cortex-M4F, Cortex-M3, Cortex-M0 + або Cortex-M0. Внутрішньо кожен мікроконтролер складається з ядра процесора, статичної пам'яті, флеш-пам'яті, інтерфейсу налагодження і різних периферійних пристроїв.

Рисунок 3.1 - Відлагоджувальна плата STM32

STM32 - це сімейство мікроконтролерних IC на основі 32-розрядних ядер RISC ARM Cortex-M33F, Cortex-M7F, Cortex-M4F, Cortex-M3, Cortex-M0 + і Cortex-M0. STMicroelectronics ліцензує IP-процесор ARM від ARM Holdings. Конструкції ядра ARM мають безліч параметрів опцій, і ST вибирає індивідуальну конфігурацію для використання в кожній конструкції. ST прикріплює свої власні периферійні пристрої до ядра перед перетворенням конструкції в кремнієву матрицю. Наступні таблиці підсумовують сімейства мікроконтролерів STM32.

Серія F3 STM32 - друга група мікроконтролерів STM32 на основі ядра ARM Cortex-M4F. F3 практично сумісний з типом pin-to-pin з серією STM32 F1. Відмінною особливістю цієї серії є наявність чотирьох швидких 12-розрядних АЦП з одночасною дискретизацией (мультиплексор на більш ніж 30 каналів) і чотирьох сумісних операційних підсилювачів з смугою пропускання 8 МГц з усіма відкритими висновками і додатково вбудованої PGA (Programmable Gain Array) мережу. Відкриті контактні площадки дозволяють використовувати цілий ряд схем перетворення аналогових сигналів, таких як смугові фільтри, фільтри згладжування, підсилювачі заряду, інтегратори / дифференциатора, диференціальні входи з високим коефіцієнтом посилення «КІП» та інші. Це усуває необхідність у зовнішніх операційних підсилювачах для багатьох додатків. Вбудований двоканальний ЦАП має довільну форму сигналу, а також можливість генерування апаратного сигналу (синус, трикутник, шум і т. Д.). Всі аналогові пристрої можуть бути повністю незалежними або частково внутрішньо підключеними, що означає, що в одній мікросхемі може бути майже все, що необхідно для вдосконаленої системи вимірювання і поєднання датчиків.

Чотири АЦП можуть бути відібрані одночасно, що дозволяє використовувати широкий спектр прецизійного аналогового контрольного обладнання. Для масиву мультиплексорів також можна використовувати апаратний планувальник, що забезпечує високу точність синхронізації при дискретизації більше 4 каналів незалежно від основного потоку процесора. Тригером вибірки і мультиплексування можна управляти з різних джерел, включаючи таймери і вбудовані компаратори, що дозволяє використовувати нерегулярні проміжки вибірки, де це необхідно.

Входи операційного підсилювача мають аналоговий мультиплексор 2-в-1, що дозволяє попередньо обробити вісім аналогових каналів з використанням операційного підсилювача; всі виходи операційного підсилювача можуть бути внутрішньо підключені до АЦП.

3.1.2 Мікроконтроллери AVR

AVR - це сімейство мікроконтролерів (рис. 3.2), розроблених Atmel з 1996 року, придбаних Microchip Technology в 2016 році. Це модифіковані 8-розрядні мікроконтролери RISC з архітектурою Гарварда. AVR був одним з перших сімейств мікроконтролерів, які використовували вбудовану флеш-пам'ять для зберігання програм, на відміну від одноразових програмованих ПЗУ, СППЗУ або ЕСППЗУ, використовуваних в той час іншими микроконтроллерами.

Ядро Atmel AVR об'єднує багатий набір команд з 32 робочими регістрами загального призначення. Всі 32 регістра безпосередньо підключені до арифметичного логічного блоку (АЛУ), що дозволяє отримати доступ до двох незалежних регістрів в одній інструкції, що виконується за один такт. Що виходять архітектура ефективніша щодо коду, забезпечуючи при цьому пропускну здатність до десяти разів швидше, ніж звичайні мікроконтролери CISC.

Рисунок 3.2 - Відлагоджувальна плата AVR

ATmega надає наступні функції: вбудована програмована флеш-пам'ять з можливістю читання під час запису, EEPROM, SRAM, 53 лінії введення-виведення загального призначення, 32 робочих регістра загального призначення, лічильник реального часу (RTC), чотири гнучких таймера / лічильники з режимами порівняння і PWM, 2 USART, двопровідний послідовний інтерфейс з байтовой орієнтацією, 8-канальний 10-розрядний АЦП з опціональним диференціальним вхідним каскадом з програмованим посиленням, програмований сторожовий таймер з внутрішнім генератором, послідовний порт SPI порт, IEEE std. Тестовий інтерфейс JTAG, що відповідає стандарту 1149.1, також використовується для доступу до вбудованої системи налагодження та програмування, а також шести програмно обираних режимів енергозбереження. У режимі очікування зупиняється центральний процесор, в той час як SRAM, таймер/лічильники, порт SPI і система переривань продовжують функціонувати. Режим Power-down зберігає вміст регістру, але зупиняє генератор, відключаючи всі інші функції мікросхеми до наступного переривання або апаратного скидання. У режимі енергозбереження асинхронний таймер продовжує працювати, дозволяючи користувачеві підтримувати базу таймера, поки інша частина пристрою знаходиться в сплячому режимі.

Режим шумозаглушення АЦП зупиняє ЦП і всі модулі введення / виводу, крім асинхронного таймера і АЦП, щоб мінімізувати шум перемикання при перетвореннях АЦП. У режимі очікування генератор Crystal / Resonator працює, поки інша частина пристрою знаходиться в сплячому режимі. Це дозволяє дуже швидкий запуск в поєднанні з низьким енергоспоживанням. У розширеному режимі очікування обидва основні генератори і асинхронний таймер продовжують працювати.

Atmel пропонує бібліотеку QTouch® для вбудовування ємнісних сенсорних кнопок, повзунків і коліщаток в мікроконтролери AVR. Запатентований отримання сигналу переносу заряду забезпечує надійне розпізнавання і включає в себе повністю викривлену звітність по сенсорних клавіш і включає технологію придушення суміжних клавіш ® (AKS TM) для однозначного виявлення ключових

подій. Простий у використанні набір інструментів QTouch Suite дозволяє досліджувати, розробляти і налагоджувати власні сенсорні додатки.

Цей телефон з використанням технології незалежної пам'яті Atmel. Onchip ISP Flash дозволяє перепрограмувати пам'ять програми в системі через послідовний інтерфейс SPI, за допомогою звичайного програматора незалежній пам'яті або за допомогою програми завантаження на кристалі, що працює на ядрі AVR. Завантажувальна програма може використовувати будь-який інтерфейс для завантаження програми

Програма в додатку Flash memory. Програмне забезпечення в розділі Boot Flash буде продовжувати працювати, поки оновлюється розділ Application Flash, забезпечуючи справжню операцію читання під час запису. Комбінуючи 8-бітний RISC-процесор з внутріпрограммной самопрограмміруемой флеш-пам'яттю на монолітному чипі, Atmel ATmega є потужний мікроконтролер, який забезпечує високу гнучкість і економічність.

Це рішення для багатьох вбудованих додатків управління. Пристрій ATmega підтримується повним набором інструментів розробки програм і систем, включаючи: компілятори C, макроассемблера, відлагоджувальники/симулятори програм, внутрішньоканальні емулятори та оціночні комплекти.

3.1.3 Мікроконтроллери PIC

PIC являє собою сімейство мікроконтролерів (рис. 3.3), виготовлених за технологією Microchip, отриманих з PIC1650, спочатку розробленого відділом мікроелектроніки General Instrument. Назва PIC спочатку відносилося до контролера периферійного інтерфейсу, і в даний час розширюється як програмований інтелектуальний комп'ютер. Перші частини сім'ї були доступні в 1976 році; до 2013 року компанія відвантажила понад дванадцять мільярдів окремих деталей, використовуваних в самих різних вбудованих системах.

Ранні моделі PIC мали постійний запам'ятовуючий пристрій (ПЗУ) або програмовану в польових умовах СППЗУ для зберігання програм, деякі з можливістю видалення пам'яті. Всі сучасні моделі використовують флеш-пам'ять для

зберігання програм, а нові моделі дозволяють PIC перепрограмувати себе. Програмна пам'ять і пам'ять даних розділені. Пам'ять даних має 8-бітну, 16-бітну і, в останніх моделях, 32-бітну ширину. Програмні інструкції різняться за кількістю бітів в залежності від сімейства PIC і можуть мати довжину 12, 14, 16 або 24 біта. Набір команд також залежить від моделі, при цьому більш потужні мікросхеми додають інструкції для функцій цифрової обробки сигналів.

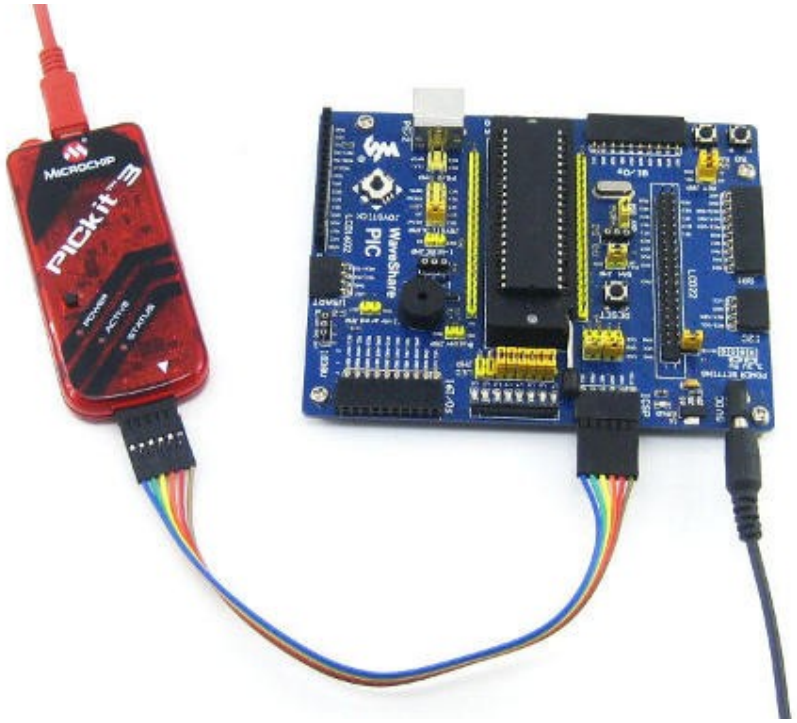


Рисунок 3.3 - Відлагоджувальна плата PIC16Cxxx

Апаратні можливості пристроїв PIC варіюються від 6-контактних SMD, 8-контактних мікросхем DIP до 144-контактних мікросхем SMD, з дискретними контактами введення-виведення, модулями АЦП і ЦАП і портами зв'язку, такими як UART, I2C, CAN і навіть USB. Варіанти з низьким енергоспоживанням і високою швидкістю існують для багатьох типів.

Виробник поставляє комп'ютерне програмне забезпечення для розробки, відоме як MPLAB X, асемблери і компілятори C/C ++, а також апаратне забезпечення програміста/відладчика для серій MPLAB і PICKit. Сторонні і деякі інструменти з відкритим вихідним кодом також доступні. Деякі деталі мають

можливість внутрішньосхемного програмування; доступні як недорогі програматори, так і високопродуктивні програматори

Пристрої PIC користуються популярністю як у промислових розробників, так і серед любителів завдяки їх низькій вартості, широкої доступності, великий базі користувачів, великому набору зауважень щодо застосування, доступності недорогих або безкоштовних інструментів розробки, послідовного програмування і можливості перепрограммируемой флеш-пам'яті.

3.1.4 Порівняння мікроконтроллерів

Для вибору мікроконтроллеру проведемо відбір за такими ознаками:

- архітектура;
- розрядність;
- розрядність АЦП;
- енергоспоживання;
- ціна;
- ціна пристроїв для розробки.

У таблиці 3.1 наведенно порівняння параметрів мікроконтроллерів.

Таблиця 3.1 - Порівняння мікроконтроллерів

Ознака	ATMega8	PIC16C100	STM32F103
архітектура	AVR	PIC	ARM
розрядність	8-розрядний	8-розрядний	32-розрядний
розрядність АЦП	10-розрядний	10-розрядний	12-розрядний
енергоспоживання	низьке	низьке	високе
ціна	12 грн.	10 грн.	50 грн.
ціна пристроїв розробки	25 грн.	300 грн.	60 грн.

Проаналізувавши таблицю, найкращим кандидатом для використання у подальшій розробці являється мікроконтроллер ATMega8. У майбутньому при розробці та масовому випуску пристроїв є можливість перейти на використання мікроконтроллеру PIC16C100.

3.2 Апаратний генератор випадкових чисел

Для генерації випадкових чисел мається можливість використовувати фізичні явища для іх утворення. Завдяки аналогово-цифровому перетворювачу можна створити апаратний генератор випадкових чисел.

3.2.1 Резисторний генератор

Тепловий шум, також званий шумом Джонсона, генерується всіма пасивними резистивними елементами електричних ланцюгів. Причина його появи - випадковий броунівський рух електронів в резистивному середовищі. Тепловий шум збільшується зі зростанням температури і опору і часто виявляється найсуттєвішою складовою шуму в прецизійних напівпровідникових перетворювачах даних.

Одним з успішних прикладів побудови ГВЧ на базі теплового шуму є генератор, розроблений компанією Intel в 1999 році і який використовується в чіпсетах Intel 800 серії.

ГВЧ Intel використовує послідовності випадкових чисел, що отримуються з двох тактових генераторів, частота роботи одного з яких перевищує частоту іншого в 100 разів. Тепловий шум з джерела (напівпровідникового резистора) посилюється і використовується для управління частотою коливань повільного генератора. Випадкові числа, отримані в результаті дрейфу (похибки ходу) двох генераторів, проходять подальшу апаратну обробку через «коректор Фон Неймана» для отримання збалансованого розподілу нулів і одиниць.

Серед недоліків даного генератора випадкових чисел можна виділити велике енергоспоживання (через кільцевого генератора, використовуваного для посилення теплового шуму) і відносно невелику для сучасних потреб швидкість генерації (приблизно 75 Кбіт/с після пост-обробки).

Один із представників, що використовує тепловий шум - Infinite Noise TRNG - апаратний генератор випадкових чисел з USB-ключем (рис. 3.4). Він використовує те, що називається “модульним множником ентропії” (раніше Infinite Noise Multiplier або FireBug). Крім того, що це просто, недорого і швидко, набагато легше отримати

правильні результати, ніж інші TRNG. Він природним чином захищає від впливу зовнішніх сигналів, таких як радіоперешкоди та перешкоди в джерелі живлення, що спрощує створення надійної конструкції без залучення фахівця з аналогової конструкції. Модульні умножители ентропії виробляють доказовий і легко вимірюваний рівень ентропії, заснований на тепловому шумі, приблизно рівний log2 (K) на вихідний біт, де K - коефіцієнт посилення між 1 і 2, встановлений двома резисторами навколо операційного підсилювача. “Монітор працездатності” може відстежувати це і перевіряти, чи знаходиться ентропія на виході в очікуваному діапазоні, який для описаного нижче нескінченного шуму TRNG знаходиться в межах 2% від log2 (1,82).

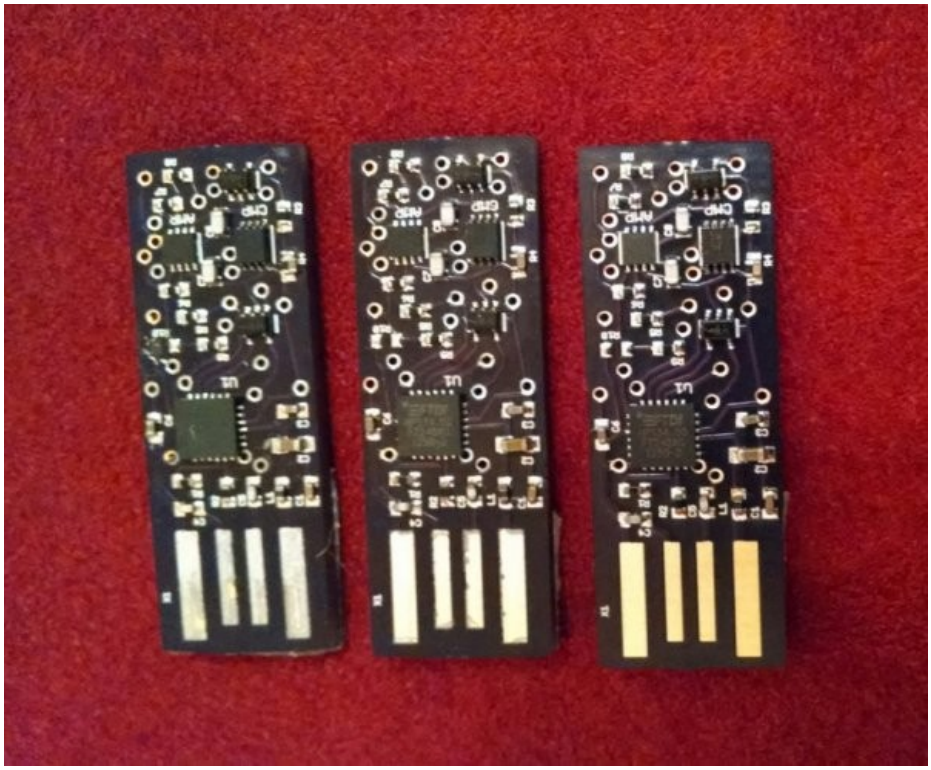


Рисунок 3.4 - Infinite Noise TRNG

Модульні ентропійних множники підходять як для реалізації на рівні плати, так і для реалізації ASIC. Швидкість обмежена швидкістю каскаду посилення і компаратора і може працювати зі швидкістю понад 100 Мбіт/с в секунду з високопродуктивними компонентами. Недорогі рішення з чотириканальними операційними підсилювачами CMOS можуть працювати зі швидкістю 8 Мбіт/с.

Суміжні біти з модульного ентропійного множителя корельовані, тому перед використанням в криптографії необхідно відбілювання. Це повинно бути зроблено шляхом постійного повторного заповнення криптографічно безпечної хеш-функції, такої як SHA-512, Blake2b, Keccak-1600 (SHA3), або потокового шифру, такого як ChaCha. У цій реалізації використовується Keccak -1600 з криптографически безпечним повторним заповненням більше 400 біт ентропії за раз, що дозволяє подолати проблему малої і низької швидкості, існуючу в системі GNU/Linux /dev/random. Користувачі, яким потрібно багато мегабайт в секунду даних для використання в криптографії, можуть встановити вихідний множник на свій розсуд, що змушує Keccak генерувати вихідний множник * 256 біт на повторне заповнення за допомогою TRNG Infinite Noise TRNG.

Модульна архітектура ентропійного умножителя була винайдена Пітером Алланом в 1999 році, яку він назвав Firebug. Я заново винайшов його в 2013 році. У Пітера є своя власна версія, яка називається Redoubler. Це дійсно правильний спосіб генерувати випадкові біти, будь то на платі зі стандартними деталями або на спеціальному чіпі.

3.2.2 Квантовий генератор

Одним з найбільш надійних способів отримання випадкових чисел є ГСЧ, реєструючий квантовий ефект удару фотонів в дзеркало. На напівпрозоре дзеркало направляються фотони, які генеруються джерелом одиночних фотонів. Фотон може відбитися, а може пройти через напівпрозоре дзеркало з однаковими частками ймовірності. Вибір, який «робить» фотон, абсолютно випадковий. На виході системи стоять два лічильника фотонів, які реєструють минулі і відображені фотони і формують вихідні електричні сигнали. Подібні квантові генератори мають високу швидкість вихідного потоку - до 10-16 Мбіт/с, - при якій не спостерігається ніяких кореляцій і виконуються всі статистичні тести.

Більшість джерел світла випускають фотони в абсолютно випадкові моменти часі і кількість фотонів, випущених за одиницю часу буде відрізнятися величину, що є повністю випадковою. Цей факт ліг в основу ГСЧ, побудованого на базі

світлочутливої КМОП-матриці звичайної фотокамери групою вчених з Женевського університету на чолі з Бруно Сангінетті.

Кожен піксель матриці рахує кількість фотонів, що потрапили на його поверхню за певний проміжок часу. Ці фотони конвертуються в електрони, які потім множаться на множник, визначений світлочутливістю матриці (рівень ISO). Кількість електронів за один і той же період буде відрізнятися на абсолютно випадкове число.

На практиці процес генерації таких випадкових чисел виглядає досить просто: матриця фотокамери засвічується зеленим світлодіодом і робляться два знімки з однаковою тривалістю витримки. Потім знімки програмно обробляються для отримання випадкових чисел. За словами розробників, випадкові числа, отримані в результати дослідів з використанням світлочутливої матриці сучасного мобільного телефону, успішно пройшли статистичні тести. Більш того, за рахунок великих розмірів матриці і частоти отримання знімків, розроблений ними ГСЧ може генерувати випадок.

Тепер Sanguinetti і його колеги Ентоні Мартін, Уго Цбінден і Ніколас Гізін використовували восьмимегапіксельну камеру зі смартфона Nokia N9 для створення пристрою, який може видавати випадкові числа зі швидкістю 1,25 Гбіт / с. Система використовує той факт, що камера настільки чутлива, що її можна використовувати для підрахунку кількості фотонів, які падають на кожен з окремих пікселів. Світло надходить від звичайного світлодіода, в якому електрони і дірки об'єднуються для створення фотонів. Це квантово-механічний процес, і тому число фотонів, отриманих за фіксований період часу, не є фіксованим, а є випадковим.

Камера і світлодіод відрегульовані так, що кожен піксель виявляє близько 400 фотонів за короткий час експозиції. Числа фотонів всіх пікселів камери об'єднуються в алгоритмі «екстрактора», який виводить послідовність випадкових чисел. У швейцарському експерименті камера використовувалася для створення потоку випадкових чисел зі швидкістю 1,25 Гбіт/с (рис. 3.5).

Проблемою будь-якого генератора випадкових чисел полягає в тому, що на числа можна було передбачувано вплинути не квантовими ефектами в системі. Це

може привести, наприклад, до зміщення вимірювань, що може привести до певних числах в порівнянні з іншими. Якщо потенційний подслушіватель знає все про генератор, він може в принципі передбачити класичну складову його виходу. Це полегшить злом системи.

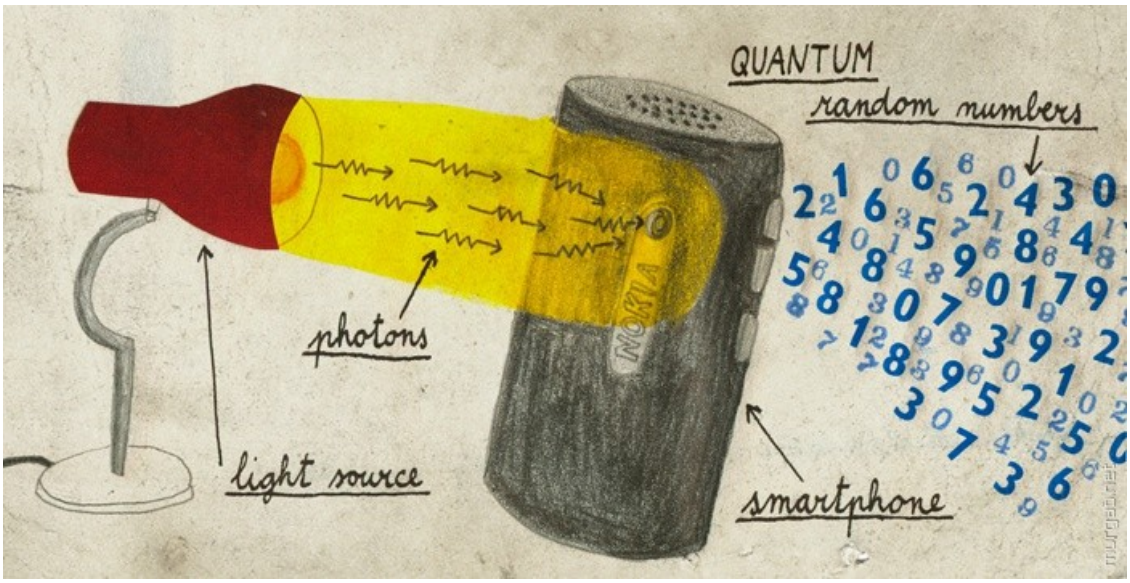


Рисунок 3.5 - Квантова геренація випадкових чисел

Однак, коли враховуються такі відхилення, команда вважає, що користувач повинен буде генерувати приголомшливі 10118 випадкових чисел, перш ніж він помітить відхилення від абсолютно випадковою послідовності.

Сангвінетті розповів, що всі компоненти QRNG його команди можуть бути інтегровані в мікросхему, яка буде коштувати кілька доларів і може бути легко інтегрована в портативні електронні пристрої, включаючи мобільні телефони. «Якщо є квантові технології, які скоро з'являться у всіх, ось і все», - каже він. Сангінетті також працює в технологічній компанії ID Quantique, яка була заснована в 2001 році Гізіном і виробляє обладнання для квантових і класичних систем шифрування. Він каже, що компанія розглядає можливість комерціалізації QRNG.

3.3 Розробка апаратної частини

Для розробки апаратної частини пристрою була використана Fritzing - це середа розробки з відкритим вихідним кодом по розробці програмного забезпечення САПР для любителів або хобі для проектування обладнання для електроніки, для підтримки дизайнерів і художників, готових перейти від експерименту з прототипом до створення більш постійної схеми. Він був розроблений в Потсдамському університеті прикладних наук.

Програмне забезпечення створено в дусі мови програмування Processing і мікроконтролера AVR і дозволяє дизайнеру, художнику, досліднику або любителю документувати свій прототип на основі AVR і створювати макет друкованої плати для виробництва. Пов'язаний веб-сайт допомагає користувачам ділитися і обговорювати проекти та досвід, а також скорочувати виробничі витрати. Fritzing можна розглядати як інструмент автоматизації електронного проектування для інженеров: вхідні метафора натхненна середовищем дизайнерів (макет на основі макета), а вихідні дані орієнтовані на доступні засоби виробництва.

Створене розведення елементів пристрою зображено на рис. 3.6.

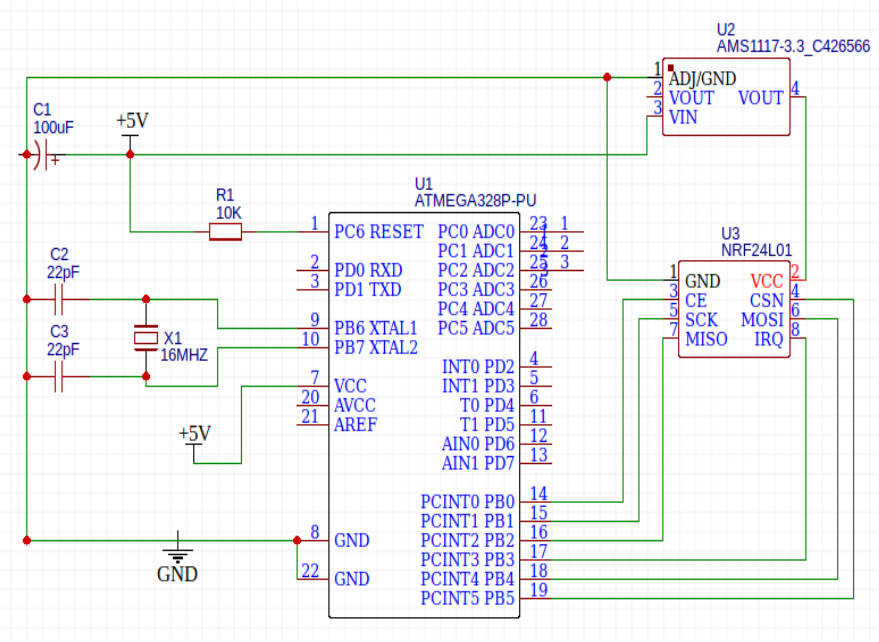


Рисунок 3.6 - Розведення елементів пристрою.

На базі створеного плану роведення елементів пристрою був створений пристрій. Розміщення елементів на платі та їх розведення зображено на рис. 3.7 та рис. 3.8.

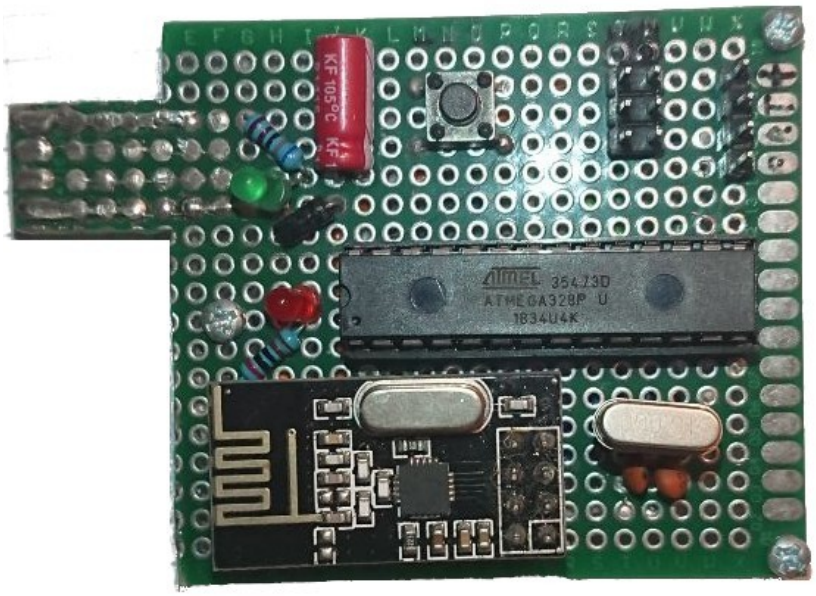


Рисунок 3.7 - Розміщення елементів на платі

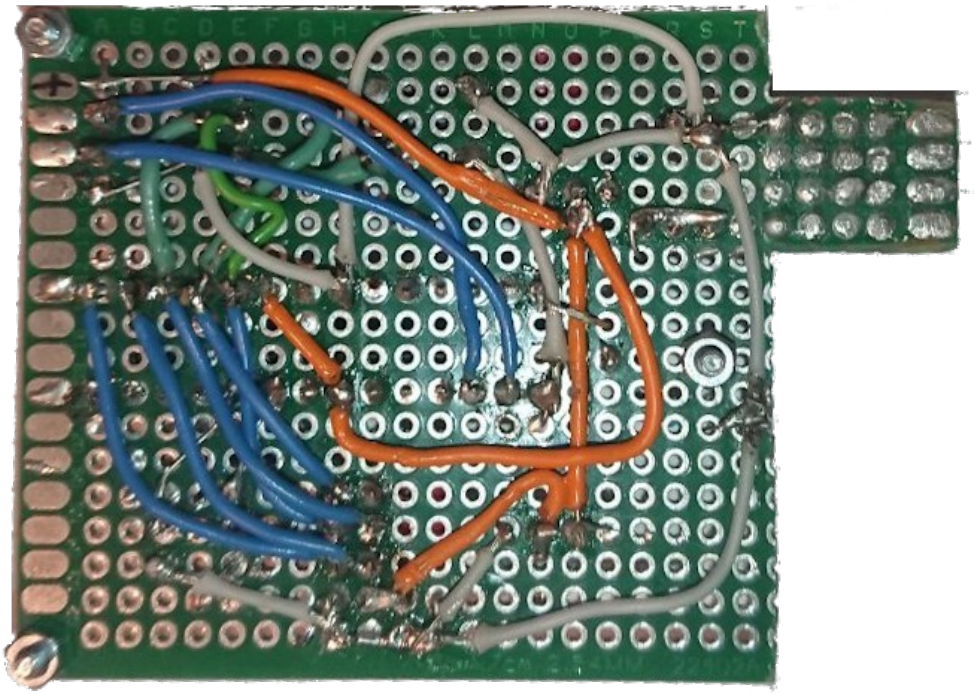


Рисунок 3.8 - Розведення елементів на платі.

Отриманий пристрій готовий та можна використовувати для розробки програмного забезпечення.

3.4 Розробка програмної частини

Отриманий пристрій підтримує декілька мов програмування, що мають між собою деякі відмінності та можуть вплинути на його роботу.

3.4.1 Мова програмування Arduino

Arduino - це програмне забезпечення з відкритим вихідним кодом, що використовується для розробки апаратного і програмного забезпечення, проектним і призначеним для користувача співтовариством, яке розробляє та виготовляє одноплатні мікроконтролери і набори мікроконтролерів для створення цифрових пристроїв. Його продукти ліцензуються відповідно до GNU Lesser General Public License (LGPL) або GNU General Public License (GPL), що дозволяє виготовлення плат Arduino і поширення програмного забезпечення будь-якою особою. Плати Arduino є в продажу в попередньо зібраному вигляді або у вигляді комплектів “зроби сам” (DIY)(рис. 3.9).

У платах Arduino використовуються різні мікропроцесори і контролери. Плати оснащені наборами цифрових і аналогових висновків введення / виведення (I/O), які можуть бути підключені до різних плат розширення, так званих щитів, або макетів (для створення прототипів) і іншими схемами. Плати оснащені інтерфейсами послідовної зв'язку, включаючи універсальну послідовну шину (USB) на деяких моделях, які також використовуються для завантаження програм з персональних комп'ютерів. Мікроконтролери можна програмувати з використанням мови програмування подібного до C і C++. На додаток до використання традиційних наборів інструментів компілятора проект Arduino надає інтегровану середу розробки (IDE), засновану на проекті мови обробки.

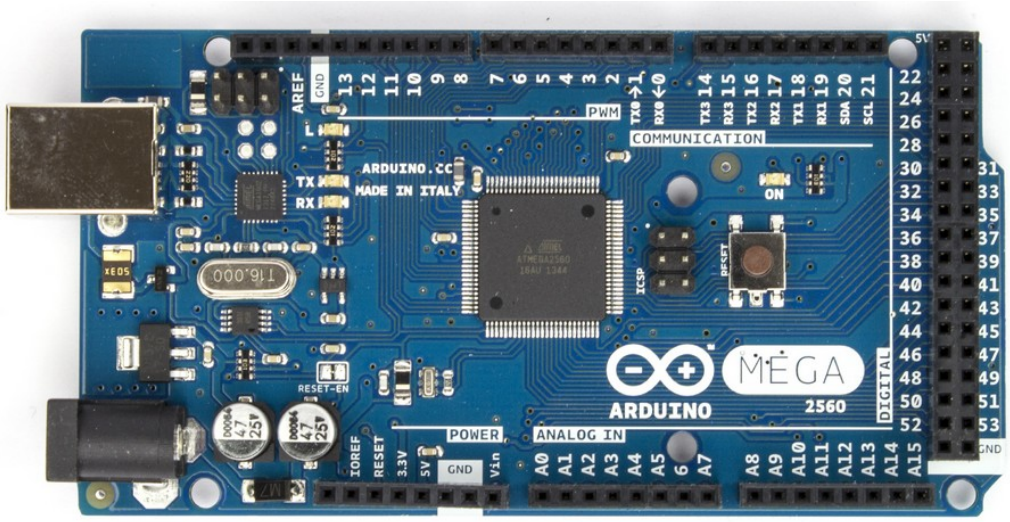


Рисунок 3.9 - Відлагоджувальна плата Arduino

Проект Arduino почався в 2005 році як програма для студентів Інституту проектування взаємодій Иврея, Иврея, Італія, з метою надати новачкам і професіоналам недорогий і простий спосіб створення пристроїв, які з'єднано їх середовищем з використанням датчиків і приводів. Типовими прикладами таких пристроїв, призначених для початківців любителів, є прості роботи, термостати і детектори руху.

3.4.2 Мова програмування C

C - це мова процедурного комп'ютерного програмування загального призначення, що підтримує структуроване програмування, область видимості лексичних змінних і рекурсію, в той час як система статичного типу запобігає ненавмисні операції. За своєю будовою C надає конструкції, які ефективно відображаються на типові машинні інструкції, і знайшов тривале застосування в додатках, раніше закодованих на мові асемблера. Такі програми включають операційні системи і різне прикладне програмне забезпечення для комп'ютерів, від суперкомп'ютерів до вбудованих систем.

Спочатку C був розроблений в Bell Labs Денніс Рітчі між 1972 і 1973 роками для створення утиліт, які працюють на Unix. Пізніше він був застосований для

повторної реалізації ядра операційної системи Unix. Протягом 1980-х C поступово завоював популярність. Він став одним з найбільш широко використовуваних мов програмування з компіляторами C від різних постачальників, доступних для більшості існуючих комп'ютерних архітектур і операційних систем. C стандартизований ANSI з 1989 року (див. ANSI C) і Міжнародною організацією зі стандартизації.

C є обов'язковою процедурною мовою. Він був розроблений для компіляції з використанням щодо простого компілятора, щоб забезпечити низькорівневий доступ до пам'яті і мовних конструкцій, які ефективно зіставляються з машинними інструкціями, і все з мінімальною підтримкою часу виконання. Незважаючи на свої низькорівневі можливості, мова був розроблений для підтримки кроссплатформенного програмування. Відповідна стандартам програма на C, написана з урахуванням переносимості, може бути скомпільована для широкого спектра комп'ютерних платформ і операційних систем з невеликими змінами в її вихідному коді. Мова доступний на різних платформах, від вбудованих мікроконтролерів до суперкомп'ютерів.

Враховуючи те, що C є кросплатформенним до AVR, PIC та ARM, що полегшить портування прошивки на нові мікроконтроллери, надалі для розробки буде використовуватися саме вона.

3.5 Аналіз роботи

Проаналізуємо роботу клавіатури без програмно-апаратного комплексу протидії атакам. Введемо слово “привіт” та проаналізуємо за допомогою RTL-SDR. Результат роботи зображено на рис. 3.10.

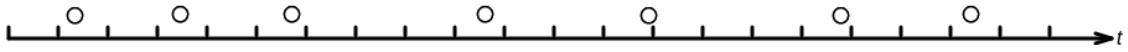


Рисунок 3.10 - Робота пристрою без захисту

Тепер ввімкнемо наш пристрій та знову введемо слово “привіт”, проаналізуємо за допомогою RTL-SDR. Результат зображено на рис. 3.11.

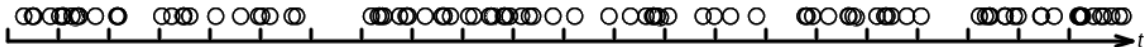


Рисунок 3.11 - Робота пристрою із захистом.

Виконання атаки за часом проти отриманих результатів є неможливим, а проблеми у роботі клавіатури не були помічені під час використання протягом години. Розроблений пристрій є працездатним, виконує поставлену ціль та не заважає штатній роботі клавіатури.

3.6 Висновки до третього розділу

У третьому розділі проведено аналіз наявних технологій та елементної бази, відібрано найкращі з них, на їх базі розроблено та зібрано програмно-апаратний комплекс протидії атакам по стороннім атакам на захищений бездротовий зв’язок пристроїв введення інформації, проведено тестування та аналіз його роботи.

РОЗДІЛ 4. РЕАЛІЗАЦІЯ СТАРТАП-ПРОЕКТУ

Wireless keyboard security (WKS) - це високоінтегрована мікросхема зі зниженим споживанням енергії (ULP) 2Мбіт/с для діапазону 2,4 ГГц. За допомогою модуля можна зв'язати кілька пристроїв для передачі даних по радіоканалу. Можна об'єднати до семи приладів в одну загальну радіомережу на частоті 2,4 ГГц.

Модуль має 4 робочих режими — виключення (Power Down), сплячий режим (Standby), прийом даних (RX mode), передача даних (TX Mode). У режимі прийому даних RX споживання струму вище, ніж в режимі передачі даних TX.

За стабільну і надійну передачу і прийом даних відповідає протокол Enhanced ShockBurst. Пристрій має давати відповідь про прийом даних, підтверджуючи таким чином зворотний зв'язок

В основу розробки ПЗ поставлено задачу удосконалення функціоналу вже існуючих на ринку конкурентів, шляхом того, що планується реалізувати підтримку функціональної можливості побудови вихідної інформації на основі редагування вхідної інформації опосередковано використовуючи графічний інтерфейс для взаємодії користувача з програмним кодом, що забезпечує інтуїтивно зрозумілий функціонал застосунку та знижує необхідність повного розуміння програмної реалізації.

Оскільки націлено забезпечити можливість використання графічного інтерфейсу для опосередкованої взаємодії користувача з програмним кодом, що характеризує винахідницький рівень винаходу, то з застосуванням додатку збільшиться швидкість реалізації спроектованої користувачем геометричної моделі та, відповідно, зменшиться «поріг входження» у користувача.

Даний проект планується реалізувати без реєстрації юридичної особи для зменшення оподаткування та спрощення фінансової звітності. Формою організації бізнесу буде фізична особа-підприємець.

4.1 Опис ідеї та технологічний аудит стартап-проекту

У якості найближчого аналогу ПЗ «NRF24L01» прийнято застосунок компанії NRF24L01.

До недоліків найближчого аналога відноситься максимальне залучення користувача застосунку до математичної складової і її програмної реалізації.

В основу винаходу поставлено задачу удосконалення застосунку компанії NRF24L01, шляхом того, що реалізовано підтримку функціональної можливості побудови вихідної інформації на основі редагування вхідної інформації опосередковано використовуючи графічний інтерфейс для взаємодії користувача з програмним кодом, що забезпечує інтуїтивно зрозумілий функціонал застосунку та знижує необхідність повного розуміння програмної реалізації.

4.2 Аналіз ринкових можливостей

Таблиця 4.1 - Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1.	Кількість головних гравців, од	5 головних гравців
2.	Загальний обсяг продаж, грн/ум.од	$185 млн
3.	Динаміка ринку (якісна оцінка)	зростає
4.	Наявність обмежень для входу (вказати характер обмежень)	затвердження ліцензійних умов провадження, створення маркетингової стратегії для проведення ефективної рекламної діяльності стосовно ПЗ
5.	Специфічні вимоги до стандартизації та сертифікації	відсутні
6.	Середня норма рентабельності в галузі (або по ринку), %	+19,8%

На основі розглянутих характеристик для показників стану ринку IT (в контексті ідеї стартап-проекту), можна зробити висновок, що ринок є привабливим для входження за попереднім оцінюванням.

Таблиця 4.2 - Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1.	Недосвідчені учасники команди	Призначення недосвідчених працівників (студентів) для виконання роботи проекту ставить під загрозу дату його завершення, оскільки їм може знадобитися більше часу, щоб ознайомитися з бізнес-моделлю, технологіями.	Щоб мінімізувати цей ризик, необхідно закласти достатньо часу на введення нових працівників у курс справи.
2.	Планування та послідовність виконання задач	Навіть якщо ці завдання виконують різні люди, їх одночасне виконання у великій кількості створює ризик для проекту, особливо наприкінці його реалізації.	Перевірити, чи не заплановано забагато завдань на один і той самий час. При плануванні задач проекту спочатку необхідно скласти список завдань і згрупувати їх, щоб оцінити весь обсяг проекту та кінцеві результати. Потім можна починати зв’язувати завдання, щоб отримати ідеальний розклад.
3.	Потужна клієнтська база конкурентів	Конкуренти, які мають впевнений досвід продукта на ринку здобули сильну базу клієнтів-споживачів.	Розвиток вражаючої маркетингової кампанії, створення стратегії піар-менеджменту, закладання регламенту рекламної кампанії, акційних пропозиції.

Таблиця 4.3 - Фактори можливостей

№ п/п	Фактор	Зміст	Можлива реакція компанії
1.	Аналіз досвіду конкурентів	Формування стратегії реалізації проекту без навчання на своїх помилках, а при навчанні на помилках конкурентів – невдалі рекламні, маркетингові ходи конкурентів.	Планування і реалізація проекту з максимальним виключенням ймовірності виникнення помилок вже досвідчених конкурентів на ринку споживачів.
2.	Націлення продукту на основні функціональності, які відстутні у конкурентів	Реалізація нових можливостей для споживачів, впровадження покращень суміжного з конкурентами проекту функціональностями.	Чітке планування задач, розподілення задач між розробниками з залученням прорахованих ризиків, мотивація команди ідеєю кінцевого продуту.
3.	Підвищення рентабельності проекту	За рахунок правильного планування всіх етапів проекту, чіткого формулювання бізнес-моделі є можливість залучення до команди проекту студентів в якості розробників.	Зниження кількості інвестицій для розробки і впровадження кінцевого продукту.

Таблиця 4.4 - Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підриємства (можливі дії компанії, щоб бути конкурентоспроможною)
1. Олігополістична конкуренція	Галузь в основному є конкурентною, проте існує декілька явних лідерів	Важко вийти на міжнародний рівень
2. Глобальний рівень конкурентної боротьби	Конкуренти з різних країн світу	Розвиток на українській IT арені та вихід на ринок

Продовження таблиці 4.4

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підриємства (можливі дії компанії, щоб бути конкурентоспроможною)
3. Внутрішньогалузева конкуренція	Конкуренція спостерігається в пропозиціях на покупку програмного забезпечення (вигідні пропозиції), якості функціональностей.	Розробка вузьконаправленого програмного забезпечення
4. Конкуренція за видами товарів: - товарно-видова	Конкуренція між програмними забезпеченнями одного виду	Випуск кращих і якісніших версій програмного забезпечення, взаємодія з пропозиціями і побажаннями споживача.
5. За характером конкурентних переваг – неціновa конкуренція	Функціональні можливості програмного забезпечення	Розширити функціональні можливості
6. За інтенсивністю – марочна конкуренція	Для споживачів має значення «бренд»	Створення добре відомої марки

Ступеневий аналіз конкуренції на ринку показав, що не дивлячись конкуренцію лідерів, у запропонованого проекту є можливість розвитку на українській ІТ арені з виходом на ринок. Можливі дії компанії, щоб бути конкурентоспроможною, це створення добре відомої марки та розширення функціональних можливостей програмного забезпечення.

Аналіз конкуренції в галузі за М. Портером показав, що можлива робота на арені ІТ України так, як конкурентна боротьба неінтенсивна і прямі конкуренти більше спеціалізуються на інших функціональних можливостях, також проект повинен відповідати умовам споживачів, які в залежності від ситуації можуть змінюватись.

Таблиця 4.5 - Аналіз конкуренції в галузі за М. Портером

	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
Складові аналізу	1. STM32 2. attiny85 3. GOM	Наявність товарних знаків, доступ до ресурсів	Основним постачальником є інтернет-ресурси	Торгівельні знаки, система інформації	відсутні
Висновки	Конкурентна боротьба неінтенсивна так, як прямі конкуренти більше спеціалізуються на інших функціональних можливостях	Є можливості входу на ринок за рахунок гнучкості цін; конкуренція є серед існуючих компаній	Зазвичай постачальники не диктують умови співпраці	Умови клієнтів в залежності від ситуації постійно змінюються	-

Таблиця 4.6 - Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)
1.	Потреби споживачів	Потреби споживачів обумовлюють необхідність розробки проекту
2.	Результативність	Завжди досягається кінцевий результат
3.	Маркетинговий потенціал	Використання не за призначенням
4.	Ціна та собівартість продукції	Не завищена, конкурентна ціна
5.	Технічне обслуговування	Випуск нових версій продукту

В результаті обґрунтування факторів конкурентоспроможності стало видно, що фактор потреби споживачів таких, як забезпечення якісного і дешевого зв’язку, створення карт поверхні Землі, передбачення прогнозу погоди і виявлення дефектів на стадії виробництва.

Таблиця 4.7 - Порівняльний аналіз сильних та слабких сторін програмного забезпечення для моделювання ізотропних кривих

№ п/п	Фактор конкурентоспроможності	Бали 1-20	Рейтинг програм-конкурентів у порівнянні з програмним забезпеченням «Maple»						
			-3	-2	-1	0	+1	+2	+3
1.	Потреби споживачів	10				+			
2.	Результативність	15						+	
3.	Маркетинговий потенціал	12				0			
4.	Ціна та собівартість продукції	8			+				
5.	Технічне обслуговування	17						+	

Порівняльний аналіз сильних та слабких сторін показав, що результативність і технічне обслуговування, а також ціна та собівартість продукції є сильними факторами конкурентоспроможності у порівняні з найближчим конкурентом - програмним забезпеченням компанії NRF24L01.

Таблиця 4.8 - SWOT- аналіз стартап-проекту

Сильні сторони: Технічна підтримка;легкий спосіб отримання і використання продукту; якість продукту; продукт відповідає потребам споживачів; доступність.	Слабкі сторони: Низька репутація компанії на початку впровадження проекту в життя; присутність багів.
Можливості: Вихід на міжнародний ринок; результативність; розвиток нових функціональних можливостей.	Загрози: Зниження доходів потенційних клієнтів; блокування реклами на просторах інтеренету, соцільних мереж; блокування інтернет-ресурсу програмного забезпечення.

SWOT-аналіз стартап-проекту вказав на сильні сторони, якими є цілодобова підтримка, інструкція легкий спосіб отримання і використання продукту, відповідність потребам споживачів та доступність. А слабкими сторонами є низька репутація компанії на початку впровадження проекту в життя та присутність багів.

Таблиця 4.9 - Альтернативи ринкового впровадження стартап-проекту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1.	Проведення конференції-демо для закордонних користувачів	50%	3-6 міс.

На основі SWOT- аналізу проекту було розроблено альтернативи ринкової поведінки стартап-проекту на ринку та орієнтовний оптимальний час їх ринкової реалізації з огляду на потенційні проекти конкурентів, що можуть бути виведені на ринок. В якості альтернативи було обрано проведення конференції-демо для закордонних користувачів.

4.3 Розробка ринкової стратегії проекту

Таблиця 4.10 - Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту) за рік	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1.	Навчальні заклади	Готові	1500	Середня конкуренція	Середня
2.	Звичайні користувачі	Готові	6500		
3.	Компанії	Готові	7000		
Які цільові групи обрано: Обрано всі три цільові групи.					

У якості можливої цільової аудиторії є навчальні заклади, компанії, які закупають клавіатури для працівників та звичайні користувачі. Усі групи не виключають можливості сприйняти продукт. Інтенсивність конкуренції в сегменті мала в Україні та вхід у сегмент є легким, через високий попит на внутрішній IT арені.

Таблиця 4.11 - Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
1.	Проведення конференції для закордонних користувачів	Ексклюзивний розподіл	Відповідна ціна, довіра до бренду	Стратегія лідерства по витратах

Для обраної альтернативи розвитку проекту було обрано ексклюзивний розподіл, а стратегію лідерства по витратах, як базову стратегію розвитку. Тому що, така стратегія передбачає, що компанія за рахунок чинників може забезпечити більшу, ніж у конкурентів маржу між собівартістю товару і середньоринковою ціною.

Таблиця 4.12 - Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект “першопрохідцем” на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки
1.	Проект не є першопрохідцем	Компанія буде забирати існуючих споживачів у конкурентів і шукати нових	Основні характеристики товару будуть схожими (Роздільна здатність, спектральний канал)	Стратегія позиціонування

При визначенні базової стратегії конкурентної поведінки к даному проекту, який не є першопрохідцем, було обрано стратегію позиціонування. Компанія показує чим відрізняється продукт від конкурентів, чим корисний, які є переваги над конкурентами, таким чином відбувається позиціонування на особливостях, які важливі споживачу.

Таблиця 4.13 - Визначення стратегії позиціонування

№ п/п	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкуренто-спроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
1.	Ціна, якість	Знизити ціни на продукцію та створити якісний товар	Відповідна ціна, довіра до бренду	Безпечність, надійність, якість

При визначенні стратегії позиціонування були обрані вимоги до товару цільової аудиторії такі, як ціна та якість. Обрано базову стратегію розвитку – знизити ціни на продукцію та створити якісний товар; асоціації було обрано на базі вимог цільової аудиторії, які формують комплексну позицію проекту-безпечність, надійність, якість.

4.4 Розробка маркетингової програми

Таблиця 4.14 - Визначення переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує ПЗ	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1.	Технічна підтримка	Своєчасна технічна підтримка	Відповідна ціна, довіра до бренду
2.	Адаптований інтерфейс користувача	Асоціативне використання новими користувачами	Наявність «Справки»

Висновки: при визначенні ключових переваг концепції потенційного товару було обрано вигоду, яку пропонує товар – своєчасну технічну підтримку,

ключовими перевагами перед конкурентами є відповідна ціна та довіра до бренду, також ще одна вигода- це адаптований інтерфейс користувача, ключовими перевагами якого є наявність «Справки» по експлуатації продукту.

Таблиця 4.15 - Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові		
I. Товар за задумом	Забезпечити можливість безпечного використання бездротової клавіатури		
II. Товар у реальному виконанні	Властивості/ характеристики	М/Нм	Вр/Тх /Тл/Е/Ор
	1.Простий у використанні 2.Забезпечення безпечності вводу даних з клавіатури 3.Невеликий розмір 4.Можливість додавання нових модулів Мультиплатформенність	-	-
	Якість: стандарти, нормативи, параметри тестування		
	Пакування – коробка з диском		
	Марка: “Wireless keyboard security”		
III. Товар із підкріпленням	До продажу: потребує ознайомлення з роботою ПЗ Після продажу: підтримка клієнтів		
За рахунок чого потенційний товар буде захищено від копіювання: патенту та комерційної таємниці			

Висновки: За задумом проект забезпечує можливість безпечного використання бездротової клавіатури. До продажу клієнти мають ознайомитися з роботою проекту, а після продажу буде цілодобова технічна підтримка. За рахунок патенту та комерційної таємниці товар буде захищено від копіювання.

Таблиця 4.16 - Формування системи збуту

№ п/п	Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, постачальника	Глибина каналу збуту	Оптимальна система збуту
1.	Клієнти купують продукт безпосередньо у компанії-розробника	встановлення контактів зі споживачами і їх підтримка;	Канал нульового рівня	Через сайт виробника

Висновки: при зазначеній специфіці закупівельної поведінки цільових клієнтів, що клієнти купують продукт безпосередньо у компанії - розробника, було обрано оптимальну систему збуту - через сайт виробника так, як це найпростіший спосіб придбання ПЗ для цільових клієнтів.

Таблиця 4.21 - Концепція маркетингових комунікацій

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідолення	Концепція рекламного звернення
1.	Клієнти дізнаються про нові продукти з реклами в інтернеті, соціальних мереж, по рекомендаціям інших людей	Інтернет, соціальні мережі	Відповідна ціна, довіра до бренду	- Поширення знань про продукт - Інформація про випробування товару	- Перелік основних правдивих даних про продукт - Науково-професійний стиль

Проаналізувавши специфіку поведінки цільових клієнтів, було обрано концепцію рекламного звернення: перелік основних правдивих даних про продукт, науково-професійний стиль. Реклама буде поширюватись через інтернет та соціальні мережі. Завданням рекламного повідомлення є зацікавлення та поширення знань про продукт новим клієнтам, та поширення інформації про випробування товару.

4.5 Елементи фінансової підтримки стартапу та аналіз ризиків

Організаційна структура проекту представлена на рис. 4.1. Структура управління проекту побудована за принципом розподілу повноважень та функціональних обов'язків.

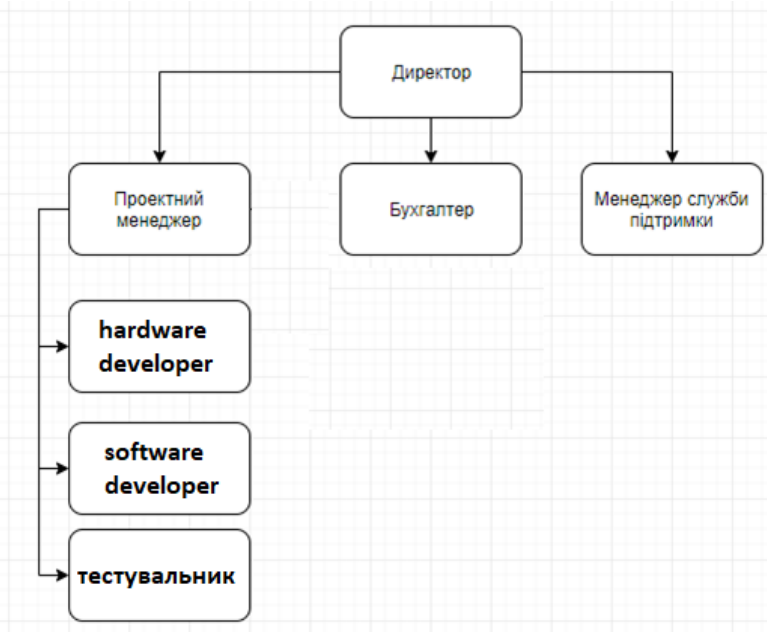


Рисунок 4.1. Організаційна структура проекту «WKS»

Команда розробників проекту включає в себе 1 тімліда, 2 розробника, 1 тестувальника. Хоча команда є невеликою, проте це не є показником неефективності, адже ключовою відмінністю даного проекту є скурпульозне планування всіх етапів розробки, тестування, експлуатації програмного забезпечення.

У складі технічної підтримки буде 1 людина, головними обов’язком якої буде повноцінна підтримка користувачів. Саме ці люди створюватимуть реакцію зворотного зв’язку на усі поради, питання, скарги тощо.

Команда проекту – молодь, це можливість студентів-програмістів 3го і вище курсів реалізувати свої здібності на реальному проекту. Головна особливість – кожний учасник команди має бути дисциплінований та цілеспрямований, надійний і зі стрімким бажанням розвиватися.

Механізм мотивації і стимулювання працівників передбачає нарахування премій та застосування заохочень щомісячно на зборах колективу.

Проведено розрахунки по видаткам та доходам проекту (табл. 5.2.) за перші три квартали релізу графічного редактора (орієнтовна дата релізу – лютий 2020 р.).

Таблиця 4.22 Кадровий склад та його характеристика

№	Посада	1 зміна (3 дні)	2 зміна (2 дні)	К-ть, всього чоловік	Посадовий оклад, грн.	Обов’язки	Примітки
А	Б	1	2	3	4	5	6
1.	Директор	1	1	1	9120	Контроль зовнішньої і внутрішньої діяльності, керівництво бізнес проектом, укладання угод з партнерами.	Власник
2.	Тімлід	1	1	1	10260	Планування, контроль розробки, налагодження процесів всередині команди	Керівник команди проекту
3.	Розробник	2	2	2	4560	Послідовна реалізація етапів розробки проекту	Учасник команди проекту

Продовження таблиці

№	Посада	1 зміна (3 дні)	2 зміна (2 дні)	К-ть, всього чоловік	Посадовий оклад, грн.	Обов’язки	Примітки
4.	Технічна підтримка	1	1	1	3420	Взаємодія з користувачами системи, учасник зворотньої реакції відносно пропозицій/ зауважень/ питань з боку користувачів	
5.	Бухгалтер	1	1	1	4180	Вирішення фінансових питань, ведення звітності стосовно фінансів проекту	
Всього, грн.:							36100 грн.

Таким чином, поточні щомісячні витрати в місяць з березня по липень 2020 р. складуть 44 251 грн. Перший місяць після релізу комплексу керування (лютий) – 84 024 грн. Власне, ці витрати і становлять необхідні кошти для релізу проекту та його місячного існування.

Для того, щоб виконати план доходів необхідно, щоб в середньому кількість проданих ліцензій на місяць становила 41 (вартість однієї ліцензії – 1 282 грн – 47.5$).

Динаміку витрат та доходів за перші два квартали релізу проекту наведено нижче (рис. 5.2). Перший місяць релізу проект буде перебувати на етапі розвитку. Витрати в лютому перевищать доходи на 30 922 грн. Але в наступних місяцях доходи проекту будуть вищі від витрат на 8 850 грн., що дасть можливість через 4 місяців (а саме у травні) перекрити всі витрати, які ми понесли для релізу «WKS».

Прогноз рентабельності проекту будується з розрахунку, що в перші місяці існування він буде знаходитися на етапі розвитку, але середньорічний рівень за доходами (перший рік) складе 80% ((чистий прибуток / загальні витрати за рік) * 100 %). Таким чином, ми прогнозуємо, що період окупності проекту – 4 місяці, і уже в кінці липня 2020 р. він принесе нам прибуток – 26 550 грн. Це позитивний результат.

Таким чином, ми можемо стверджувати, що підприємство не вийде за межі самоокупності, і в подальшому буде спостерігатися зростання продажів. Наші розрахунки показують, що податки не стануть перешкодою для подальшого розвитку цього підприємства (табл. 4.23).

Таблиця 4.23 - Грошовий потік

№	Показник	Перші 6 міс. діяльності
1.	Грошові кошти на початок, грн.	84024
2.	Обсяг продажу, грн.	318610
3.	Собівартість реалізованого продукту, грн.	225316
4.	Валовий прибуток, грн.	92153
5.	Адміністративні витрати, грн.	40153
6.	Реклама, грн.	0
7.	Фінансовий результат до оподаткування, грн.	53102
8.	Податок на прибуток (17%), грн.	9026,9
9.	Єдиний соціальний внесок, грн.	1089,8
10.	Чистий прибуток, грн.	39127

На початку функціонування проекту потрібно 84 024 грн. Фінансування бізнес-проекту «Пристрою активного захисту бездротової клавіатури - WKS» включає джерело інвестиційних ресурсів:

1. Власні кошти – 84 024 грн.

Ці кошти потрібні для запуску проекту і початку його роботи, а саме на забезпечення матеріально-технічної бази. Можливо, джерело фінансування будуть змінені за умови виграшу гранту або залучення інвесторів.

Ризик в управлінні можна охарактеризувати як можливість настання подій, які негативно вплинуть на досягнення поставлених цілей.

При розробці даного бізнес-плану проаналізована можливість виникнення кількох критичних ситуацій, які можуть негативно позначитися на роботі проекту - можливість невдачі або непередбачених витрат. Аналіз можливих ризиків здійснено за допомогою методу експертних оцінок (табл. 4.24).

Таблиця 4.24 - Оцінка ризику

Ризик	Експерти				Середня ймовірність	Вага	Бал
	1	2	3	4			
1. Ринковий ризик (зміна вимог споживачів продукції, посилення конкуренції)	25	10	15	8	14.5	1/5	2.9
2. Ринковий ризик (Неочікувані зміни на ринку бездротових клавіатур)	10	20	5	20	13.75	1/7	1.96
3. Операційний ризик, пов'язаний з відступом від цілей проекту	10	20	30	1	15.25	1/7	2.18
4. Ризик зміни валютних курсів	50	5	50	25	32.5	1/7	4.64
5. Ризик непрогнозованої інфляції	40	20	55	25	35	1/4	8.75
6. Ризик податкового тиску	0	0	35	20	13.75	1/7	1.96
Загальний ризик проекту							22.3

Оскільки загальний ризик проекту є менший за 50 – його можна вважати оптимальним.

Аналізуючи таблицю 4.24 можна виділити найбільш суттєві ризики та розробити заходи по їх запобіганню. В нашому випадку, найбільш важливим ризиком є «Ризик непрогнозованої інфляції», а це значить, що при масштабуванні системи цей аспект буде ключовим при плануванні складових проекту.

4.6 Висновки до четвертого розділу

Є достатньо обґрунтовані передумови, що дозволяють зробити припущення про те, що реалізоване апаратне забезпечення «WKS» для активного захисту бездротової клавіатури може бути успішно застосовано для різних цільових груп, в тому числі, для компаній, звичайних користувачів і навчальних закладів. В якості детальної аргументації надано розгорнутий аналіз запланованого проекту у вигляді маркетингового аналізу стартап-проекту, план організації стартап-проекту, фінансово-економічного аналізу та оцінки ризиків проекту, планування заходів з комерціалізації проекту.

ВИСНОВКИ

Під час роботи над магістерською дисертацією було розглянуто види підключення бездротових периферійних пристроїв, можливі атаки по стороннім каналам на захищенний бездротовий зв’язок цих пристроїв та існуючі методи захисту.

В ході роботи над магістерською дисертацією описано метод вилучення корисної інформації із захищенного трафіку, розроблено метод протидії описаній атаці, розроблено, виготовлено та протестовано пристрій активного захисту.

Пристрій активного захисту формує хибні пакети, розраховує затримку за розподілом Пуассона та відправляє в ефір. Такий метод захищає наявний зв’язок, а завдяки випадковій затримці емулює активну роботу пристрою введення інформації та не заважає його нормальній роботі.

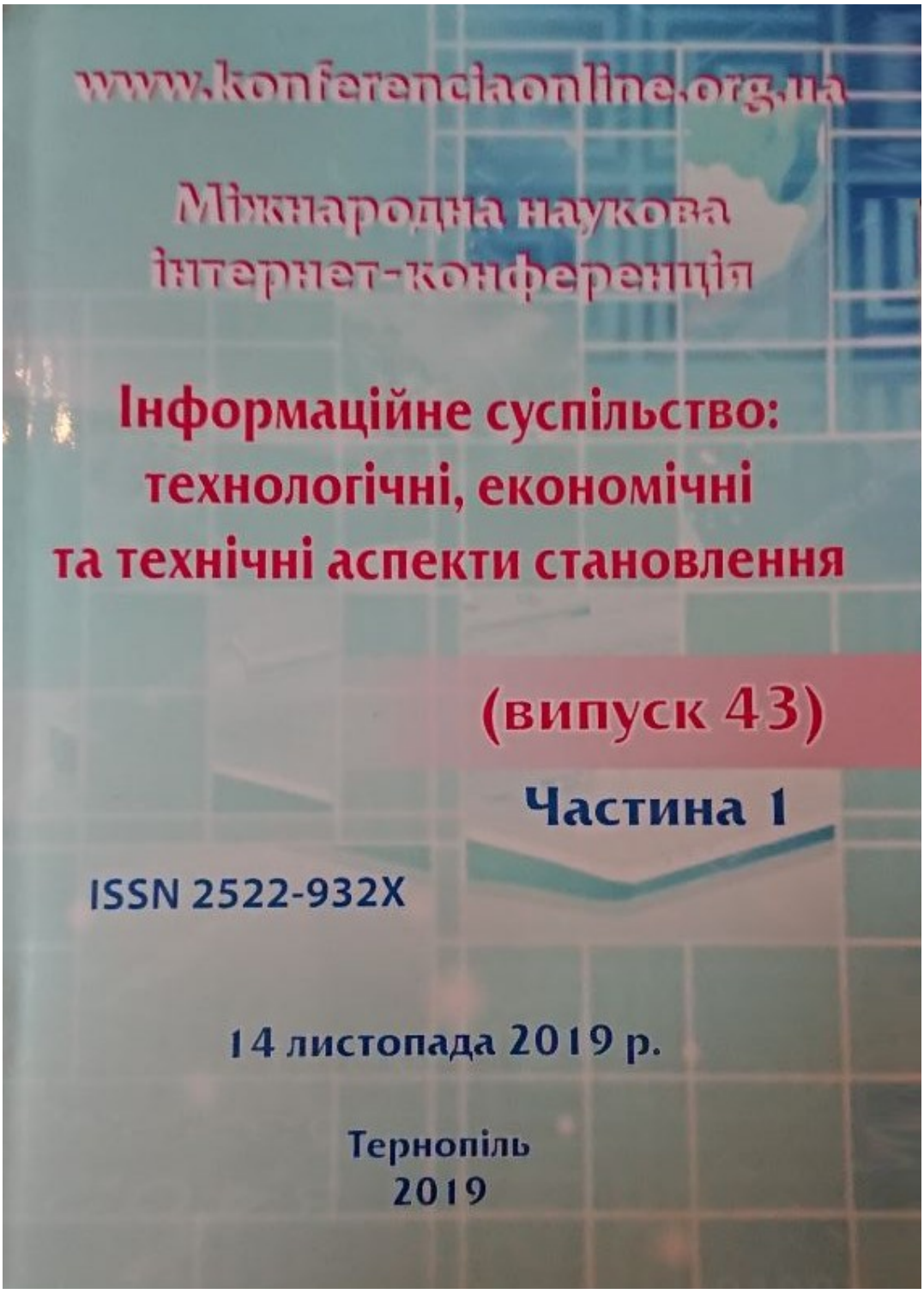
Розроблений метод протидії атакам може використовуватися в складі автономного пристрою активного захисту, а також може бути інтегрований у пристрої введення інформації на виробництві.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Об опасностях беспроводных клавиатур и мышей [Електронний ресурс] – Режим доступу: https://habr.com/company/pt/blog/325932/.
2. Уязвимость в протоколах беспроводных мышей [Електронний ресурс] – Режим доступу: https://tproger.ru/news/wireless-mice-are-hacked/.
3. Типы беспроводной связи: радиоканал или bluetooth? [Електронний ресурс] – Режим доступу: http://mobile-advices.blogspot.com/2012/10/types-wireless-connections-radiochannel.html.
4. Таненбаум Е., Уезеролл Д. Компьютерные сети. — Питер, 2012. — С. 960
5. Е. Мейволд. Безопасность сетей. — 2006. — С. 528
6. Нильс Фергюсон, Брюс Шнайер Практическая криптография — Москва: «Диалектика», 2004. — С. 420
7. С.Г. Баричев, В.В. Гончаров, Р.Е. Серов, Основы современной криптографии, 2-е издание, Москва, "Горячая линия - Телеком", 2002
8. А. А. Шимбирёв, Тетеревлева Ев.К., Тетеревлева Ек.К. — Курс лекций «Компьютерные сети» — МПТ РГТЭУ, 2013
9. INTEL-SA-00290 [Електронний ресурс] — Режим доступу: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html
10. Обзор видов атак по побочным каналам на криптографические устройства. Подлеснов А. В. Молодой учёный. 2015. № 1. с. 187-189
11. Реализация DDIO в чипах Intel допускает сетевую атаку по определению нажатий клавиш в сеансе SSH [Електронний ресурс] — Режим доступу: https://www.opennet.ru/opennews/art.shtml?num=51467
12. Taxicab geometry world [Електронний ресурс] — Режим доступу: http://www.ams.org/publicoutreach/feature-column/fcarc-taxi

13. Обзор алгоритмов кластерного анализа [Електронний ресурс] — Режим доступу: https://habr.com/ru/post/101338/
14. STM32 32-bit Arm Cortex MCUs [Електронний ресурс] — Режим доступу: https://www.st.com/en/microcontrollers-microprocessors/stm32-32-bit-arm-cortex-mcus.html
15. ATMega8 — 8-bit AVR [Електронний ресурс] — Режим доступу: https://www.microchip.com/wwwproducts/en/ATMEGA128
16. PIC Microcontroller [Електронний ресурс] — Режим доступу: https://pic-microcontroller.com
17. What is Arduino [Електронний ресурс] — Режим доступу: https://www.arduino.cc/en/Main/

ДОДАТОК А. АПРОБАЦІЯ



www.konferenciaonline.org.ua

Міжнародна наукова інтернет-конференція

"Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення" (випуск 43)

14 листопада 2019 р.

Частина 1

Тернопіль – 2019

Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 43)" / Збірник тез доповідей: випуск 43 (м. Тернопіль, 14 листопада 2019 р.). – Частина 1. – Тернопіль. – 2019. – 141 с.

УДК 001 (063)
ББК 72я431

ISSN 2522-932X

Збірник тез доповідей підготовлено за матеріалами Міжнародної наукової інтернет-конференції (випуск 43) від 14 листопада 2019 р.

Збірник матеріалів науково-практичної інтернет-конференції включаються до наукометричної бази даних "РІНЦ/RSCI".

Тексти матеріалів конференції подаються в авторській редакції. Відповідальність за точність, достовірність і зміст поданих матеріалів несуть автори.

Наша адреса: Оргкомітет МНІК "Конференція онлайн"
а/с 797, м. Тернопіль 46005
тел. моб. 068 366 0 525
e-mail: inetkonf@ukr.net

URL Інтернет-конференції: http://www.konferenciaonline.org.ua/

використовуючи різні облікові записи. OAuth2 - простий стандарт авторизації, заснований на базових принципах інтернету, що робить можливим застосування авторизації практично на будь-якій платформі.

Література:

1. Authenticate to OAuth2 services. URL:
https://developer.android.com/training/id-auth/authenticate
2. Understanding OAuth2. URL:
http://www.bubblecode.net/en/2016/01/22/understanding-oauth2/

Кропенко Д.О.[1], студент
Ходаковський О.В.[2], к.т.н., доцент
Національний технічний університет України "Київський Політехнічний Інститут ім. Ігоря Сікорського", м. Київ
[1]Кафедра автоматизації проектування енергетичних процесів і систем, студент
[2]Кафедра автоматизації проектування енергетичних процесів і систем, доцент

ЗАХИСТ ШИФРОВАНОГО БЕЗДРОТОВОГО ЗВ'ЯЗКУ ПРИСТРОЇВ ВВЕДЕННЯ ІНФОРМАЦІЇ ВІД АТАК ПО ПОСТОРОННІМ КАНАЛАМ

Оскільки бездротові технології стали для нас повсякденним явищем, ми часто вважаємо їх безпечними та все більше людей користуються бездротовими периферійними пристроями, оскільки останні вже практично зрівнялися за ціною з дротовими, однак мало хто замислюється, що такі пристрої не захищені від злому. Насьогодні відсутні стандарти, що регулюють безпеку бездротових периферійних пристроїв, з цієї причини питання захисту від злому залишається на виробниках [1].

Більш того, навіть захищений бездротовий зв'язок надійними та перевіреними алгоритмами шифрування даних є вразливим до атак по постороннім каналам: завдяки останнім досягненням в математиці є можливим проаналізувати зв'язок та частково або повністю відновити зміст передаючої інформації пристроями введення.

У доповіді буде описаний один із методів вилучення корисної інформації із трафіку захищеного бездротового зв'язку пристрою введення інформації та метод протидії подібним атакам.

Метою доповіді є демонстрація доступності виконання подібних атак та можливості їм протидії.

Подібний метод атаки згадується у вразливості CVE-2019-11184, де під час SSH сесії відправляються пакети у момент натискання клавіш на клавіатурі [2].

Даний метод атаки є атакою по часу — виконавши високоточний замір часу виконання різних подій та їх аналіз, можна розшифрувати захищені дані. Цей вид атаки є пасивним та неруйнівним [3].

Маємо пристрій введення інформації — клавіатуру Logitech K250, що використовує для з'єднання із комп'ютером донгл із радіоприймачем NRF24LU1. Для аналізу трафіку було використано RTL-SDR. Виявлено, що для передачі натискання клавіші відправляються два пакети — під час натискання клавіші та під час відпускання клавіші.

Варто відмітити, що затримки між натисканнями зазвичай залежать від положення клавіші на клавіатурі, можна з певною ймовірністю відтворювати інформацію, що вводиться. Наприклад, більшість людей зазвичай набирають "s" після "a" значно швидше, ніж "g" після "s". Маючи точні моменти передачі пакетів можна дати оцінку — наскільки ці моменти відповідають тому чи іншому слову [4].

Для подальшого аналізу необхідно отримати перевірочний набір моментів, кожен з яких відповідає певному слову. Отримати даний набір можна при звичайному введені тексту на комп'ютері, зафіксувавши моменти натискання та відпускання клавіш.

Для оцінки використаємо формулу Евклідової відстані (1)[5]:

$$d = \sqrt{\sum_{i=1}^{2n}(x_i - y_i)^2}, \quad (1)$$

де d — відстань між словами; x_i , y_i — моменти натискання для перевірочного та отриманого слів; n — кількість букв у слові.

За допомогою формули отримаємо чисельний показник — наскільки моменти натискання отриманого слова відповідає моментам натискання перевірочного слова. Виконуючи обчислення для усіх перевірочних слів можемо визначити отримане слово.

При великій кількості даних для пришвидшення обчислень можна використати простішу формулу, наприклад, Манхеттенську відстань (2)[5]:

$$d = \sum_{i=1}^{2n}|x_i - y_i| \quad (2)$$

Для протидії аналізу пропонується в ефір відправляти хибні пакети за допомогою пристрою. Даний пристрій можна створити на базі мікроконтроллера ATMEGA-328P та радіопередавача NRF24L01. Схему з'єднання апаратних елементів пристрою зображено на рисунку 1.

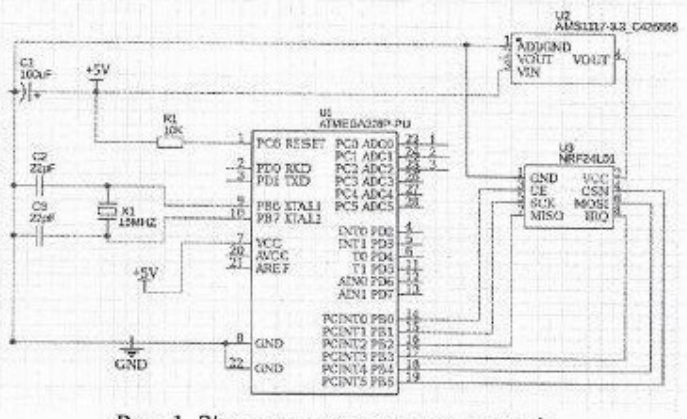


Рис. 1. З'єднання апаратних елементів

Передача хибних пакетів здійснюється із затримкою за розподілом Пуассона (3):

$$t = \frac{-\log\left(\frac{r}{r_{max}}\right)}{\lambda}, \qquad (3)$$

де λ — математичне очікування, r — невід'ємне випадкове число, r_{max} — максимальне значення випадкового числа.

Завдяки використанню випадкової затримки згенерований трафік не заважає роботі пристроїв введення інформації та ускладнює аналіз трафіку для вилучення передаючої інформації.

Висновки

Описано метод атаки на зашифрований зв'язок пристроїв введення інформації та аналіз трафіку. Запропоновано метод протидії подібним атакам, описано пристрій для захисту зв'язку.

Перспективами подальших досліджень у данному напрямку є дослідження можливості інтеграції описаного алгоритму захисту зв'язку при виробництві нових бездротових пристроїв введення інформації.

Література:

1. Об опасностях беспроводных клавиатур и мышей [Електронний ресурс] — Режим доступу: https://habr.com/company/pt/blog/325932/
2. INTEL-SA-00290 [Електронний ресурс] — Режим доступу: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00290.html
3. Обзор видов атак по побочным каналам на криптографические устройства. Подлеснов А. В. Молодой учёный. 2015. № 1. с. 187-189
4. Реализация DDIO в чипах Intel допускает сетевую атаку по определению нажатий клавиш в сеансе SSH [Електронний ресурс] — Режим доступу: https://www.opennet.ru/opennews/art.shtml?num=51467
5. Taxicab geometry world [Електронний ресурс] — Режим доступу: http://www.ams.org/publicoutreach/feature-column/fcarc-taxi

www.konferenciaonline.org.ua

WSSG

С Е Р Т И Ф І К А Т

цей Сертифікат підтверджує, що

Кропенко Д.О.

взяв(ла) участь у роботі Міжнародної наукової інтернет-конференції «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення» (Випуск 43)

Конференція проведена за сприянням та при активній участі Громадської організації «Наукова спільнота» та Wyższej Szkoły Społeczno-Gospodarcza w Przeworsku

м. Тернопіль
14 листопада 2019 року

ДОДАТОК Б. ЛІСТИНГ ПРОГРАМИ

Лістинг файлу Makefile

```
MCU=atmega328p
PROGRAMMER=usbasp
F_CPU=1600000
CC=avr-gcc
OBJCOPY=avr-objcopy
CFLAGS=-std=c99 -Wall -g -Os -mmcu=${MCU} -DF_CPU=${F_CPU} -I.
TARGET=target/main
SRCS=src/main.c src/nrf24l01.c

all:
	mkdir -p target
	${CC} ${CFLAGS} -o ${TARGET}.bin ${SRCS}
	${OBJCOPY} -j .text -j .data -O ihex ${TARGET}.bin ${TARGET}.hex

flash:
	avrdude -p ${MCU} -c ${PROGRAMMER} -U flash:w:${TARGET}.hex:i -F -P usb

clean:
	rm -fr target
```

Лістинг файлу main.c

```
#include <avr/io.h>
#include <avr/interrupt.h>
#include <math.h>
#include <stdbool.h>
#include <string.h>
#include <util/delay.h>
#include "nrf24l01.h"
#include "nrf24l01-mnemonics.h"

nRF24L01 *setup_rf(void);
void process_message(char *message);
void prepare_led_pin(void);
void  set_led_high(void);
void  set_led_low(void);
double poisson_keypress(void);
static char *rand_payload(char *str, size_t size);
void delay_ms(uint16_t n);
void delay_us(uint16_t n);
uint16_t hw_random();
double poisson_dist(uint16_t lambda, uint16_t input, uint16_t max_input);

volatile bool rf_interrupt = false;

int main(void) {
                        char * tmp_payload;
   uint8_t address[5] = { 0x6B, 0xB7, 0xE2, 0x9E, 0x31 }; //predefined keyboard
   prepare_led_pin();
   sei();
   nRF24L01 *rf = setup_rf();
   uint8_t addr[5];
   nRF24L01_read_register(rf, CONFIG, addr, 1);

                        tmp_payload = (char *) malloc(16);

                        set_led_high();

                        while(1){
```

```
                                nRF24L01Message msg;
                                rand_payload(tmp_payload, 16);
                                memcpy(msg.data, tmp_payload, 16);
                                msg.length = 17;
                                nRF24L01_transmit(rf, address, &msg);
                                set_led_high();
                                delay_us((int)(poisson_dist(1, hw_random() % 4096, 4096)*4096));
                                set_led_low();
                        }
    return 0;
}

nRF24L01 *setup_rf(void) {
    nRF24L01 *rf = nRF24L01_init();
    rf->ss.port = &PORTB;
    rf->ss.pin = PB2;
    rf->ce.port = &PORTB;
    rf->ce.pin = PB1;
    rf->sck.port = &PORTB;
    rf->sck.pin = PB5;
    rf->mosi.port = &PORTB;
    rf->mosi.pin = PB3;
    rf->miso.port = &PORTB;
    rf->miso.pin = PB4;
    // interrupt on falling edge of INT0 (PD2)
    EICRA |= _BV(ISC01);
    EIMSK |= _BV(INT0);
    nRF24L01_begin(rf);
    return rf;
}

void prepare_led_pin(void) {
    DDRC |= _BV(PC5);
    PORTC &= ~_BV(PC5);
}

void set_led_high(void) {
    PORTC |= _BV(PC5);
}

void set_led_low(void) {
    PORTC &= ~_BV(PC5);
}

// nRF24L01 interrupt
ISR(INT0_vect) {
    rf_interrupt = true;
}

uint16_t hw_random() {
  sei();
  ADMUX = 0b11111111;
  ADCSRA = 0b10001100;
  ADCSRA = ADCSRA | (1<< ADSC);
  ADCSRB = 0b10001100;
  ADCSRB = ADCSRB | (1<< ADSC);
            return ADCSRA|ADCSRB;
}

double poisson_dist(uint16_t lambda, uint16_t input, uint16_t max_input){
            return -(1./lambda)*(double)log((double)input/(double)max_input);
}

static char *rand_payload(char *str, size_t size)
{
    if (size) {
        --size;
        for (size_t n = 0; n < size; n++) {
            char key = hw_random() % 255;
```

```
            str[n] = key;
        }
    }
    return str;
}

void delay_ms(uint16_t n) {
  while(n--) {
    _delay_ms(1);
  }
}

void delay_us(uint16_t n) {
  while(n--) {
    _delay_us(1);
  }
}
```