НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Навчально-науковий інститут прикладного системного аналізу
Кафедра системного проектування

До захисту допущено:

Завідувач кафедри

_____ Вадим МУХІН

«___»_____2023 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою

“Інтелектуальні сервіс-орієнтовані розподілені обчислювання”

зі спеціальності 122 "Комп'ютерні науки"

на тему: «Аналіз ризиків та переваг застосування носимих розумних речей та мереж в питаннях безпеки та виробничих ризиків»

Виконав:
студент IV курсу, групи ДА-92
Архипов Роман Володимирович

Керівник:
доцент, к.т.н
Кирюша Богдан Анатолійович

Консультант з нормконтролю:
доцент, к.т.н.,
Кирюша Богдан Анатолійович

Рецензент:

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент (-ка) _____

Київ – 2023

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Навчально-науковий інститут прикладного системного аналізу

Кафедра системного проектування

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 122 "Комп'ютерні науки"

Освітньо-професійна програма – "Інтелектуальні сервіс-орієнтовані розподілені обчислювання"

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Вадим МУХІН

«___»_____2023 р.

ЗАВДАННЯ

на дипломну роботу студенту

Архипову Роману Володимировичу

1. Тема роботи «**Аналіз ризиків та переваг застосування носимих розумних речей та мереж в питаннях безпеки та виробничих ризиків**», керівник роботи Кирюша Богдан Анатолійович, затверджені наказом по університету від «30» травня 2023 р. №2065-с

2. Термін подання студентом роботи 13 червня 2023 р.

3. Вихідні дані до роботи: Перелік носимих пристроїв, які можуть бути застосовані людиною під час перебування на робочому місці.

4. Зміст роботи: Робота присвячена аналізу ризиків та переваг використання носимих розумних пристроїв та мереж у сфері безпеки та виробничих ризиків, виявленню потенційних небезпек, які можуть виникнути при застосуванні цих технологій, а також визначенню можливостей та вигод, які вони можуть принести.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): Презентація до захисту роботи

6. Консультанти розділів роботи*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний	Рощина Н. В.		

7. Дата видачі завдання 15.04.2023

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Прибуття студента на практику, оформлення і отримання перепусток	Перший тиждень	
2	Проведення інструктажу з техніки безпеки	Перший тиждень	
3	Проведення екскурсій по підприємству	Перший тиждень	
4	Аналіз переліку носимих пристроїв, які можуть бути застосовані людиною під час перебування на робочому місці	Другий тиждень	
5	Аналіз платформ, на яких базуються ці пристрої	Третій тиждень	
6	Аналіз переліку вразливостей, які найчастіше мають місце для таких платформ	Четвертий тиждень	
7	Дослідження програмних та технічних засобів, придатних для подолання відомих вразливостей досліджених платформ.	П’ятий тиждень	

Студент Архипов Р. В.

Керівник Кирюша Б. А.

АНОТАЦІЯ

бакалаврської дипломної роботи Архипова Романа Володимировича на тему

«Аналіз ризиків та переваг застосування носимих розумних речей та мереж в питаннях безпеки та виробничих ризиків»

Метою дипломної роботи є проаналізувати ризики та переваги використання носимих розумних пристроїв та мереж у сфері безпеки та виробничих ризиків. Дослідження спрямоване на виявлення потенційних небезпек, які можуть виникнути при застосуванні цих технологій, а також на визначення можливостей та вигод, які вони можуть принести.

Актуальність роботи полягає в постійно зростаючій ролі носимих розумних пристроїв та мереж у питаннях безпеки та виробничих ризиків. В сучасному світі, де безпека та ефективність на робочому місці є пріоритетом для багатьох організацій, використання цих пристроїв та мереж набуває все більшої ваги.

Результати дослідження дозволять отримати інформацію про ризики та переваги використання носимих розумних пристроїв та мереж у сфері безпеки та виробничих ризиків. Це допоможе підприємствам та організаціям приймати обґрунтовані рішення щодо впровадження цих технологій з метою забезпечення безпеки працівників та оптимізації виробничих процесів.

Загальний обсяг роботи 101 с., 5 рис., 1 табл., 54 джерела.

Ключові слова: носимі пристрої, виробничі ризики, аналіз ризиків, переваги застосування, безпека працівників, несанкціонований доступ, моніторинг здоров'я, мікроконтролер.

ANNOTATION

bachelor's thesis of Arkhypov Roman Volodymyrovych on the topic "Analysis of the risks and benefits of the wearable smart things usage for security and industrial risks"

The purpose of the thesis is to analyze the risks and benefits of using wearable smart devices and networks in the field of safety and industrial risks. The research is aimed at identifying potential dangers that may arise from the use of these technologies, as well as identifying the opportunities and benefits they can bring.

The relevance of the work lies in the ever-increasing role of wearable smart devices and networks in safety and industrial risks. In today's world, where safety and efficiency in the workplace is a priority for many organizations, the use of these devices and networks is becoming increasingly important.

The results of the study will provide information on the risks and benefits of using wearable smart devices and networks in the field of safety and operational risks. This will help businesses and organizations make informed decisions about the implementation of these technologies to ensure employee safety and optimize production processes.

The total volume of work is 101 pages, 5 figures, 1 table, 54 sources.

Keywords: wearable devices, industrial risks, risk analysis, benefits of use, employee safety, unauthorized access, health monitoring, microcontroller.

ЗМІСТ

Перелік умовних позначень, символів, скорочень і термінів 9
ВСТУП 11
РОЗДІЛ 1. Аналіз переліку носимих пристроїв, які можуть бути застосовані людиною під час перебування на робочому місці 12
1.1. Загальні відомості про носимі пристрої 12
1.2. Огляд доступних носимих пристроїв, які можуть бути використані працівниками для роботи 14
1.3. Аналіз ринку та класифікація основних типів носимих пристроїв за походженням 24
1.4. Порівняння функціоналу пристроїв від крупних виробників та аналогічних пристроїв бюджетного сегменту 27
Висновки до розділу 28
РОЗДІЛ 2. Аналіз платформ, на яких базуються носимі пристрої..... 30
2.1. Огляд платформ, на яких можуть базуватися носимі пристрої..... 30
2.2. Класифікація платформ на основі цінового сегменту: 45
2.3. Порівняння особливостей та функцій платформ 47
2.4. Порівняння можливостей носимих пристроїв на основі різних платформ 49
Висновки до розділу 51
РОЗДІЛ 3. Аналіз переліку вразливостей, які найчастіше мають місце для платформ, на яких побудовані носимі пристрої..... 53
3.1. Аналіз найпоширеніших вразливостей на платформі ESP32: 53
3.2. Аналіз найпоширеніших вразливостей на платформі AVR 54
3.3. Аналіз найпоширеніших вразливостей на платформі STM32..... 56
3.4. Аналіз найпоширеніших вразливостей на платформі PIC..... 57
3.5. Аналіз найпоширеніших вразливостей на платформі Nordic nRF52 ... 59
3.6. Аналіз вразливостей, що стосуються зберігання та передачі даних.... 60
3.7. Аналіз можливостей поширення вірусів на платформах 62
Висновки до розділу 64
РОЗДІЛ 4. Дослідження програмних та технічних засобів, придатних для подолання відомих вразливостей досліджених платформ..... 65
4.1. Виявлення та виправлення вразливостей 65

4.2. Створення бекапів даних 67
4.3. Оновлення безпеки та видалення шкідливих програм 69
4.4. Методи аутентифікації 72
4.5. Захист від шкідливих програм 74
4.6. Захист від крадіжки даних 76
4.7. Захист апаратної частини пристрою 77
Висновки до розділу 79
РОЗДІЛ 5. Економічне обґрунтування застосування носимих розумних речей та мереж в питаннях безпеки та виробничих ризиків 80
Вступ 80
5.1. Економічне обґрунтування результатів аналізу 81
5.2. Порівняння вартості та економічної доцільності використання підприємствами різних носимих пристроїв 86
Висновки до розділу 93
ВИСНОВКИ 95
ПЕРЕЛІК ПОСИЛАНЬ 96

Перелік умовних позначень, символів, скорочень і термінів

Носима технологія (англ. Wearable technology) – це будь-яка технологія, призначена для використання під час носіння.

Інтернет речей (англ. Internet of Things, IoT) — концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами в автоматичному режимі, за допомогою використання стандартних протоколів зв'язку.

Система на кристалі, або Система на чипі (від англ. System-on-a-chip, або іще SoC чи SOC) — дизайн електронної схеми, яка вміщує функціональні складові цілого пристрою (наприклад комп'ютера) на одній мікросхемі. Залежно від призначення SoC може оперувати як цифровими сигналами, так і аналоговими, аналого-цифровими, а також частотами радіодіапазону. Типовим застосуванням таких схем є широке різноманіття вбудованих систем.

Мікроконтролер (англ. microcontroller), або однокристальний мікрокомп'ютер — виконаний у вигляді мікросхеми спеціалізований комп'ютер, що включає мікропроцесор, оперативну та постійну пам'ять для збереження виконуваного коду програм і даних, порти вводу-виводу і блоки зі спеціальними функціями (лічильники, компаратори, АЦП та інші).

Bluetooth (англ. Bluetooth) — технологія бездротового зв'язку, створена у 1998 році групою компаній: Ericsson, IBM, Intel, Nokia, Toshiba.

Bluetooth з низьким енергоспоживанням (англ. Bluetooth low energy; скорочення BLE) — технологія цифрової бездротової передачі даних з наднизьким енергоспоживанням і малим радіусом передачі (10 м), заснована на недорогих мікросхемах в передавальних пристроях.

Вразливість (уразливість) — це нездатність системи або її частини витримувати впливи недружнього середовища; міра чутливості до уражень,

пошкоджень; слабке місце одного з елементів об'єкта захисту; фактор реалізації загрози.

ВСТУП

В сучасних умовах розвитку технологій та наукових досягнень все більше уваги приділяється здоров'ю та безпеці людей на робочому місці. Одним зі способів забезпечення цього є використання носимих пристроїв, таких як смарт-годинники, фітнес-браслети, електронні окуляри та інші, що надають користувачам нові можливості відстеження, контролю та збирання даних про своє здоров'я, активність, робочу продуктивність та інші показники.

Розробка та застосування носимих розумних речей та мереж зарекомендували себе як важливий тренд в інформаційних технологіях. Проте, разом з перевагами, використання носимих пристроїв також пов'язане з ризиками та викликами, зокрема у сфері безпеки та виробничих ризиків.

Метою цієї роботи є проаналізувати ризики та переваги використання носимих розумних пристроїв та мереж у сфері безпеки та виробничих ризиків. Дослідження спрямоване на виявлення потенційних небезпек, які можуть виникнути при застосуванні цих технологій, а також на визначення можливостей та вигод, які вони можуть принести.

Результати дослідження можуть бути корисними для компаній та працівників, що прагнуть забезпечити безпеку та здоров'я на робочому місці, а також для подальшого розвитку та вдосконалення носимих пристроїв.

РОЗДІЛ 1. Аналіз переліку носимих пристроїв, які можуть бути застосовані людиною під час перебування на робочому місці

1.1. Загальні відомості про носимі пристрої

Носима технологія - це будь-яка технологія, призначена для використання під час носіння. До поширених типів носимих технологій належать такі пристрої, як розумні годинники, розумні окуляри, фітнес-трекери та інші. Носимі електронні пристрої часто розташовуються близько або на поверхні шкіри, де вони виявляють, аналізують і передають інформацію, таку як життєво важливі показники та/або дані про навколишнє середовище, і в деяких випадках дозволяють користувачеві отримати негайний зворотний зв'язок про свої фізіологічні показники [49].

Носимі пристрої можна використовувати для збору даних про стан здоров'я користувача, включаючи [49]:

- частоту серцевих скорочень
- спалені калорії
- пройдені кроки
- артеріальний тиск
- виділення певних біохімічних речовин
- час, витрачений на фізичні вправи
- судоми
- фізичне навантаження

Носимі пристрої, такі як трекери активності, є прикладом Інтернету речей, оскільки "речі", такі як електроніка, програмне забезпечення, датчики та підключення, є засобами, які дозволяють об'єктам обмінюватися даними через Інтернет з виробником, оператором та/або іншими підключеними пристроями, не вимагаючи втручання людини [49].

Носимі технології пропонують широкий спектр можливих застосувань, від спілкування та розваг до покращення здоров'я та фітнесу, проте існують

побоювання щодо конфіденційності та безпеки, оскільки переносні пристрої мають можливість збирати персональні дані [49].

Носимі технології мають безліч варіантів використання, кількість яких зростає з розвитком технології та розширенням ринку. Вони стають дедалі популярнішими в побутовій електроніці, найчастіше у форм-факторах розумних годинників, розумних перстнів та імплантатів. Окрім комерційного використання, технології, що носяться, впроваджуються в навігаційні системи, сучасний текстиль (електронний текстиль) та охорону здоров'я. Оскільки носимі технології пропонуються для використання в критично важливих сферах, вони, як і інші технології, проходять перевірку на надійність і безпеку[14]. Швидке поширення таких пристроїв вивело носимі технології на передній план Інтернету речей (IoT) [49].

Можна сказати, що носимі технології існують з тих пір, як у 13 столітті були вперше розроблені окуляри. Годинники, достатньо маленькі, щоб їх можна було носити, з'явилися приблизно в 1500 році. Але сучасні носимі технології визначаються як такі, що включають в себе мікропроцесор і підключення до Інтернету [52].

Розвиток мобільних мереж, високошвидкісної передачі даних і мініатюрних мікропроцесорів активізував розвиток носимих технологій. Фітнес-трекери були першою великою хвилею носимих технологій, яка привернула увагу споживачів. Потім наручний годинник перетворився на екран, і з'явилися більш надійні мобільні застосунки. Bluetooth-гарнітури, смарт-годинники та окуляри з підтримкою Інтернету - все це дозволяє людям отримувати дані з мереж Wi-Fi. Ігрова індустрія додає більше носимих пристроїв з гарнітурами віртуальної та доповненої реальності [52].

З початку 2000-х років носимі камери використовуються як частина зростаючого спостереження за рухом [49].

У 2010 році компанія Fitbit випустила свій перший лічильник кроків. Носима технологія, яка відстежує таку інформацію, як ходьба та частота серцевих скорочень, є частиною кількісної частини руху [2].

У 2013 році компанія McLear, також відома як NFC Ring, випустила перший широко використовуваний сучасний носимий пристрій. Розумний перстень міг платити біткоїнами, розблоковувати інші пристрої, передавати особисту інформацію та інші функції[47]. McLear володіє найпершим патентом, поданим у 2012 році, який охоплює всі розумні перстні, а Джо Пренсіпе з Сіетла, штат Вашингтон, є єдиним винахідником [15].

У 2013 році одним з перших широкодоступних смарт-годинників став Samsung Galaxy Gear. У 2015 році Apple випустила Apple Watch[3].

Фокус у розвитку носимих технологій, зараз, схоже, зміщується від споживчих аксесуарів до більш спеціалізованих і практичних застосувань. Імплантати з мікрочіпами зараз використовуються для заміни ключів і паролів. Вбудовані в кінчик пальця, чіпи використовують технологію ближнього радіозв'язку (NFC) або радіочастотної ідентифікації (RFID) і схожі на чіпи, що використовуються для відстеження домашніх тварин, які загубилися [52].

1.2. Огляд доступних носимих пристроїв, які можуть бути використані працівниками для роботи

Існує багато різних типів носимих пристроїв, які можуть бути використані людиною під час роботи. Найбільш поширеними з них є:

1. Смарт-годинники - пристрої, які наділяють користувача багатьма функціями, такими як відстеження фізичної активності, серцевого ритму, споживання калорій, повідомлення та зв'язок з іншими пристроями. Вони можуть бути корисні для працівників, які проводять багато часу на ногах, або для тих, хто часто відривається від роботи, щоб перевірити повідомлення або телефонний дзвінок.

   Основні функції смарт-годинників включають:

- Відображення повідомлень: Смарт-годинники можуть підключатися до смартфона через Bluetooth або Wi-Fi і отримувати повідомлення, які надходять на смартфон, такі як SMS, електронна пошта, повідомлення з соціальних мереж і т.д. Користувач може швидко переглядати ці повідомлення без необхідності виймати смартфон з кишені.
- Календар та організація: Смарт-годинники можуть синхронізуватися з календарем користувача і відображати заплановані події, зустрічі, нагадування і т.д. Користувач може отримувати сповіщення про наближення подій і керувати своїм графіком безпосередньо з годинника.
- Фітнес-функції: Багато смарт-годинників оснащені датчиками, які відстежують фізичну активність користувача, таку як кроки, дистанція, калорії, пульс і інші параметри здоров'я. Вони можуть служити як фітнес-трекери, надаючи користувачеві інформацію про його фізичну форму та допомагаючи досягати здорових цілей.
- Музика та мультимедіа: Деякі смарт-годинники можуть відтворювати аудіофайли, такі як музика або подкасти. Вони можуть мати вбудовані гучномовці або підключатися до бездротових навушників, що дозволяє користувачам насолоджуватися своєю улюбленою музикою прямо з годинника.
- Повідомлення та виклики: Деякі смарт-годинники дозволяють здійснювати телефонні виклики або відправляти текстові повідомлення безпосередньо з годинника. Вони можуть мати вбудований мікрофон і динамік або підключатися до смартфона для цих операцій.
- Додаткові функції: Багато смарт-годинників мають додаткові функції, такі як відстеження сну, контроль стресу, погода, навігація, функції платежів, керування камерою смартфона і

багато інших. Вони можуть бути розширені за допомогою додатків та сторонніх розширень.

Залежно від моделі та виробника, смарт-годинники можуть мати інші специфічні функції та особливості. Важливо обрати смарт-годинник, який найкраще задовольняє потреби працівника та враховує його професійні вимоги.

2. Смарт-браслети – це пристрої, що відстежують людську активність, надають інформацію про серцевий ритм та споживання калорій. Вони також можуть відображати повідомлення та сповіщення від інших пристроїв.

   Основні функції фітнес-трекерів включають:

   - Вимірювання кроків: Фітнес-трекери використовують вбудовані акселерометри для вимірювання кількості кроків, які користувач робить протягом дня. Це дозволяє визначити загальну активність та подолану відстань.
   - Вимірювання пульсу: Більшість фітнес-трекерів мають оптичні сенсори, що вимірюють пульс через шкіру. Це дозволяє відстежувати серцевий ритм під час фізичної активності та відпочинку, що допомагає контролювати і поліпшувати загальне здоров'я.
   - Відстеження сну: Фітнес-трекери можуть аналізувати якість та тривалість сну користувача. Вони визначають фази сну, такі як легкий сон, глибокий сон та рем-сон, і надають звіт про якість сну та рекомендації для покращення.
   - Калорійний рахунок: За допомогою вбудованих алгоритмів та вимірювання активності, фітнес-трекери можуть надавати оцінку кількості спалених калорій під час різних видів фізичної активності. Це корисна інформація для тих, хто бажає

контролювати свою вагу або дотримуватися раціонального харчування.

- Нагадування про активність: Фітнес-трекери можуть надсилати нагадування та сповіщення, щоб підбадьорити користувача до фізичної активності. Вони можуть попереджати про тривалі періоди без руху та рекомендувати зробити паузу для розтяжки або зарядження.
- Водонепроникність та тривалість роботи: Багато фітнес-трекерів є водонепроникними, що дозволяє користувачам використовувати їх під час занять спортом під час дощу або навіть під час плавання. Вони зазвичай мають вбудовану акумуляторну батарею, яка забезпечує тривалу автономну роботу протягом декількох днів або навіть тижнів.
- Синхронізація з додатками та платформами: Більшість фітнес-трекерів можуть синхронізуватися зі смартфоном або комп'ютером за допомогою спеціальних додатків. Це дозволяє переглядати і аналізувати дані про фізичну активність, встановлювати фітнес-цілі та спілкуватися зі спільнотою користувачів.

Фітнес-трекери можуть мати різну конфігурацію та функціональність залежно від моделі та виробника. Вони допомагають користувачам бути більш освіченими про своє здоров'я, мотивувати їх до фізичної активності та досягати своїх фітнес-цілей.

3. Смарт-окуляри є інноваційними носимими пристроями, які поєднують функції традиційних окулярів зі смартфоном і розширеною реальністю. Вони надають користувачам можливість отримувати інформацію, сповіщення та взаємодіяти з цифровими об'єктами безпосередньо через візуальне поле.

Основні характеристики смарт-окулярів включають:

- Відображення інформації: Смарт-окуляри мають вбудований дисплей, який відображає інформацію прямо перед очима користувача. Цей дисплей може бути прозорим або напівпрозорим, що дозволяє бачити як реальний світ, так і цифрові елементи.
- Розширена реальність (AR): Смарт-окуляри можуть додавати цифрові об'єкти та інформацію до реального світу, створюючи ефект розширеної реальності. Користувачі можуть бачити віртуальні об'єкти, які інтегруються з реальними предметами навколо них.
- Голосовий та жестовий контроль: Користувачі можуть взаємодіяти з смарт-окулярами за допомогою голосових команд або жестів. Це дозволяє керувати функціями пристрою без потреби використовувати традиційні кнопки або сенсорний екран.
- Сповіщення та повідомлення: Смарт-окуляри можуть надсилати сповіщення про вхідні дзвінки, повідомлення, електронну пошту та інші важливі події. Це дозволяє користувачам отримувати інформацію без необхідності перевіряти свій смартфон.
- Навігація та допомога: Смарт-окуляри можуть надавати навігаційні вказівки та допомогу в режимі реального часу. Вони можуть відображати карти, напрямки руху та інші корисні інструкції, що допомагають користувачам орієнтуватися у незнайомих місцях.
- Мультимедійний вміст: Смарт-окуляри можуть відтворювати аудіо та відео контент. Користувачі можуть переглядати фільми, слухати музику або споживати інші типи розважального вмісту безпосередньо через окуляри.
- Підключення до інших пристроїв: Смарт-окуляри можуть бути підключені до смартфонів, планшетів або комп'ютерів, щоб

обмінюватися даними, синхронізувати контент та використовувати додатки.

Застосування смарт-окулярів є дуже широкими. Вони можуть бути використані в галузях, таких як медицина, промисловість, освіта, розваги та багато інших. Смарт-окуляри представляють нові можливості для взаємодії з цифровим світом, розширюючи можливості людей у багатьох сферах життя.

4. Спеціальні пристрої для відстеження руху - це пристрої, що можуть надійно відстежувати рухи користувача та повідомляти про небезпечні ситуації. Вони можуть бути корисними на виробничих підприємствах з високими рівнями ризику [45].
5. Крім того, на робочому місці можуть використовуватися також спеціальні носимі пристрої для контролю рівня шуму та вібрації, так звані "шумоміри" та "віброметри". Ці пристрої дозволяють вимірювати і контролювати рівень шуму та вібрації на робочому місці, що є важливим з погляду здоров'я та безпеки працівників.

   Деякі з можливих застосувань шумомірів та віброметрів включають:

   - Оцінка робочих умов: В промислових та виробничих середовищах шум та вібрації можуть бути шкідливими для здоров'я працівників. Шумоміри та віброметри використовуються для вимірювання рівнів шуму та вібрацій на робочих місцях, щоб встановити відповідні норми та вжити заходи для зниження ризиків.
   - Контроль якості: Вимірювання шуму та вібрацій можуть бути важливими для контролю якості виробів та обладнання. Наприклад, у виробництві автомобілів віброметри можуть використовуватися для перевірки рівня вібрацій автомобіля під час його руху.

- Оцінка екологічного впливу: У місцях зі значним рівнем шуму та вібрацій, таких як аеропорти, дороги або промислові об'єкти, шумоміри та віброметри використовуються для оцінки впливу цих факторів на довкілля та людей, і вживаються заходи для зниження шуму та вібрацій.
- Дослідження та аналіз: Шумоміри та віброметри використовуються в наукових дослідженнях, дослідженнях ринку та інженерних дослідженнях для збору даних про шум та вібрації з метою аналізу, моделювання та покращення продуктів і систем.
- Оцінка безпеки: В навколишньому середовищі, де шум та вібрації можуть бути небезпечними для здоров'я, таких як на будівельних майданчиках, шумоміри та віброметри використовуються для контролю рівнів та вжиття заходів для запобігання можливим ризикам.
- Використання шумомірів та віброметрів є важливим з медичної, промислової, науково-дослідницької та охорони довкілля. Ці пристрої допомагають виміряти, контролювати та керувати шумом та вібраціями для покращення безпеки, ефективності та якості життя.

Окрім цього, деякі пристрої можуть бути використані для контролю за здоров'ям працівників, наприклад, носимі пристрої для вимірювання температури тіла, пульсу та інших фізіологічних параметрів. Вони можуть бути особливо корисними у виробничих умовах, де можуть бути підвищені ризики для здоров'я працівників.

Також варто відзначити, що носимі пристрої можуть бути використані для забезпечення безпеки працівників у небезпечних умовах. Наприклад, носимі камери можуть використовуватися для запису обстановки на робочому місці та відстеження руху працівників, що дозволяє швидко виявляти потенційно небезпечні ситуації та уникати їх [50].

Аналізуючи застосування носимих пристроїв, таких як розумні годинники, фітнес-трекери, розумні окуляри, датчики руху, шумоміри, віброметри та носимі камери, в контексті їх використання на виробництві, можна виділити наступні важливі аспекти впливу:

- Вплив на безпеку працівників: Носимі пристрої можуть відігравати важливу роль у покращенні безпеки працівників. Наприклад, фітнес-трекери та датчики руху можуть виявляти небезпечні рухи або позиції тіла та сповіщати про них, що допомагає уникнути травм та нещасних випадків. Шумоміри та віброметри можуть виявляти шкідливі рівні шуму та вібрації, що дозволяє контролювати робоче середовище та запобігати виникненню проблем зі здоров'ям.
- Перспективи та можливості: Використання носимих пристроїв на виробництві відкриває нові перспективи для покращення ефективності та оптимізації робочих процесів. Наприклад, розумні годинники та розумні окуляри можуть надавати працівникам необхідну інформацію в режимі реального часу, таку як інструкції, плани роботи або нагадування про дедлайни. Датчики руху та віброметри можуть збирати дані про рухи працівників та використовувати їх для аналізу робочих процесів та вдосконалення робочого середовища.
- Оптимізація робочого процесу: Носимі пристрої можуть допомогти оптимізувати робочий процес шляхом автоматизації та збору даних. Вони можуть збирати дані про робочі параметри, які можна використовувати для аналізу та вдосконалення ефективності виробництва. Наприклад, носимі камери можуть використовуватись для запису робочих операцій або для підтримки дистанційного навчання та консультацій.

Окрім цього, далеко не кожний носимий пристрій буде придатний до використання на виробництві. Саме тому важливо виділити критерії, яким має відповідати пристрій для того, щоб бути придатним до використання на виробництві. Зокрема, носимий пристрій має відповідати таким критеріям як:

- Комунікація та інтеграція: Важливим аспектом є можливість комунікації та інтеграції носимих пристроїв з іншими системами на виробництві. Наприклад, важливо, щоб носимий пристрій мав підтримку бездротових технологій, таких як Bluetooth або Wi-Fi, для передачі даних до центральних систем або зв'язку з іншими пристроями.
- Витривалість та стійкість: На виробництві можуть бути небезпечні умови, такі як підвищена вологість, пил, вібрація тощо. Тому важливо, щоб носимі пристрої були витривалими та стійкими до таких умов, забезпечуючи надійну роботу впродовж тривалого часу.
- Енергоефективність: Оскільки носимі пристрої працюють від вбудованих джерел живлення, таких як батареї або акумулятори, важливо мати енергоефективну архітектуру та оптимізований режим споживання енергії. Це дозволить продовжити тривалість роботи пристрою без необхідності частої зарядки або заміни батареї.
- Захист даних та приватність: Носимі пристрої можуть збирати та передавати чутливі дані про працівників або виробничі процеси. Тому важливо мати високий рівень захисту даних та приватності, щоб уникнути можливого витоку інформації чи несанкціонованого доступу до системи.
- Розширені можливості: Деякі носимі пристрої можуть мати розширені можливості, такі як вбудовані сенсори для вимірювання різних параметрів (температури, вологості, тиску тощо), GPS для визначення місцезнаходження або дисплеї для відображення інформації. Ці можливості можуть сприяти більш точному моніторингу та керуванню робочими процесами.

Окрім перелічених вище переваг, носимі пристрої на виробництві можуть створювати і певні ризики, які варто враховувати. Основні ризики пов’язані з безпекою працівників, приватністю даних та впливом на виробничі процеси. Нижче наведено деякі приклади таких ризиків:

- Ризик відволікання: Носимі пристрої, такі як розумні годинники чи фітнес-трекери, можуть стати джерелом відволікання для працівників. Вони можуть займати їх увагу, що може призвести до необережності, помилок чи недотримання правил безпеки.
- Ризик збору та витоку даних: Носимі пристрої можуть збирати чутливі дані про працівників або виробничі процеси. Якщо ці дані не захищені належним чином, може виникнути ризик їх витоку чи недостатньої конфіденційності.
- Ризик несумісності з безпековими системами: Деякі носимі пристрої можуть впливати на роботу безпекових систем на виробництві, таких як системи контролю доступу, системи пожежної безпеки чи інші системи автоматизації. Несумісність може створювати проблеми з безпекою та працездатністю цих систем.
- Ризик використання незатверджених додатків або програмного забезпечення: Використання незатверджених додатків на носимих пристроях може відкривати двері для вразливостей та атак на систему. Це може стати джерелом загроз для безпеки даних та інфраструктури виробництва.
- Ризик втрати пристроїв: Носимі пристрої можуть бути втрачені або вкрадені, що може призвести до розголошення конфіденційної інформації, втрати даних або незаконного доступу до систем виробництва.
- Ризик ергономіки: Носимі пристрої повинні бути зручними та комфортними для користування, аби не створювати навантаження на тіло працівника або не перешкоджати виконанню робочих операцій. Неправильне проектування або використання носимих пристроїв може викликати проблеми з ергономікою та здоров'ям працівників.

Ці ризики варто враховувати при впровадженні носимих пристроїв на виробництві. Необхідно вживати заходів для забезпечення безпеки працівників,

захисту даних та інфраструктури, а також враховувати ергономічні аспекти. Ретельне планування, використання надійних технологій та забезпечення свідомого використання носимих пристроїв можуть допомогти зменшити ризики та забезпечити безпечні умови праці на виробництві.

1.3. Аналіз ринку та класифікація основних типів носимих пристроїв за походженням

Відповідно до останніх досліджень Strategy Analytics [44] протягом 2020 р. в усьому світі продано понад 527 млн шт. носимих пристроїв, що на 37 % більше, ніж у 2019 р. (384 млн шт.). Так, на навушники та розумні годинники в сукупності припадало 98 % усіх носимих пристроїв, реалізованих у 2020 р.

Домінуючий сегмент ринку в 2020 р. – розумні годинники, частка яких склала більш ніж 48.9 % [53].

Основними компаніями, які сьогодні представлені на ринку розумних годинників, є Apple Inc., Garmin, Fitbit, Motorola, Sony Corporation, Samsung Electronics, LG Electronics, Huawei Technologies Co. Ltd., Fossil Group, Inc. та Google Inc. [53]

За даними Strategy Analytics [40], світові поставки розумних годинників у другому кварталі 2021 р. зросли на 47 % і досягли 18.1 млн одиниць. Що стосується структури ринку за виробниками, то Apple зберіг перше місце з часткою на світовому ринку більш ніж 50 %, Samsung посів друге місце, а Garmin – третє (табл. 1.1) [53].

Таблиця 1.1 – Розподіл ринку розумних годинників за виробниками

Виробник	Частка ринку, %	
	2020	2021
Apple	52.8	52.5
Samsung	10.6	11.0

Garmin	9.8	8.3
Інші	26.8	28.2

Для подальшого аналізу носимих пристроїв важливим чинником буде їх правильна класифікація. Існує багато критерїв, за якими можна класифікувати носимі пристрої, одним з них є класифікація за походженням.

Класифікація носимих пристроїв за походженням може бути здійснена на основі брендів виробників.

Виробники з великим іменем зазвичай надають якісні продукти з більш розширеним функціоналом, тоді як виробники бюджетного сегменту намагаються зробити доступними продукти з набором основних функцій за більш прийнятну ціну.

Крупні виробники носимих пристроїв, такі як Apple, Samsung, Xiaomi та інші, часто використовують спеціалізовані мікроконтролери та SoC (System on a Chip), розроблені власними командами інженерів. Однак, конкретні моделі мікроконтролерів, які використовуються в їхніх пристроях, не розголошуються публічно. Це зазвичай комерційна інформація, яка є частиною внутрішньої розробки та комерційної стратегії компаній.

Проте, відомо, що крупні виробники носимих пристроїв активно використовують мікроконтролери та SoC, які мають високу продуктивність, низьке споживання енергії та багатофункціональність. Вони також часто поєднуються з власними операційними системами та програмними платформами, що дозволяє виробникам досягати високої оптимізації пристроїв та забезпечувати багатофункціональність.

Загалом, мікроконтролери та SoC, що використовуються в носимих пристроях крупних виробників, підбираються з урахуванням специфіки конкретного пристрою, його функціональності та потреб користувачів.

Носимі пристрої бюджетного сегменту можуть бути засновані на різних платформах. Багато з них використовують недорогі чіпи, які забезпечують базові функції пристрою, такі як вимірювання пульсу, кроків та інші заміри. Однак, для деяких бюджетних пристроїв використовуються платформи, які базуються на ARM-процесорах з меншою швидкістю та кількістю ядер, а також з меншим обсягом пам'яті.

Нижче наведені деякі приклади носимих пристроїв крупних виробників та пристроїв бюджетного сегменту:

1. Крупні виробники:
    - Apple Watch від Apple
    - Galaxy Watch від Samsung
    - Mi Band від Xiaomi
    - Watch GT від Huawei
    - Fitbit Smartwatches від Fitbit
2. Аналогічні пристрої бюджетного сегменту:
    - Amazfit Bip Lite від Amazfit
    - Letsfit Smartwatch
    - Letscom Smart Watch
    - Yamay Smartwatch
    - UMIDIGI Smartwatch

Доволі популярною платформою для бюджетних носимих пристроїв є система на мікроконтролері ESP32, яка є досить потужною та енергоефективною. Ця платформа підтримує ряд протоколів зв'язку, включаючи Wi-Fi, Bluetooth, NFC, і має вбудовані функції для вимірювання біометричних даних, таких як пульс та кроки [25].

Деякі виробники бюджетних носимих пристроїв також можуть використовувати спеціалізовані мікроконтролери, такі як AVR, для створення своїх продуктів. Ці мікроконтролери забезпечують достатній спектр

функціональних можливостей та простоту використання, що робить їх популярними серед розробників прототипів та експериментальних проектів.

Крім цього, досить популярними є рішення побудовані на мікроконтролерах STM32, Nordic nFR52, PIC та інших.

1.4. Порівняння функціоналу пристроїв від крупних виробників та аналогічних пристроїв бюджетного сегменту

Носимі пристрої від крупних виробників, таких як Apple, Samsung, і т.д. зазвичай мають більше функцій та можливостей, ніж аналогічні пристрої бюджетного сегменту. Основні відмінності між ними полягають у таких параметрах:

1. Якість екрану: носимі пристрої від відомих виробників зазвичай мають якісні екрани з високою роздільною здатністю та яскравістю, що забезпечує більш зручний та комфортний перегляд інформації. Бюджетні пристрої можуть мати екрани з меншою роздільною здатністю та яскравістю.
2. Обчислювальна потужність: носимі пристрої від крупних виробників зазвичай мають більш потужні процесори, які можуть працювати на вищих тактових частотах та з більшим обсягом оперативної пам'яті. Це дозволяє їм ефективно виконувати складні завдання, такі як обробка великого обсягу даних, запуск вимогливих додатків та забезпечення плавної роботи інтерфейсу користувача. З іншого боку, бюджетні пристрої, побудовані на мікроконтролерах, таких як ESP32, AVR, та інших, мають меншу обчислювальну потужність порівняно з пристроями від великих виробників. Ці мікроконтролери призначені для роботи з обмеженими ресурсами, зокрема обсягом пам'яті та швидкістю процесора, що забезпечує енергоефективність та низьку вартість пристроїв.

3. Функції та можливості: носимі пристрої від відомих виробників зазвичай мають більше функцій та можливостей, таких як функція ECG для вимірювання серцевої діяльності, водонепроникність, GPS-трекер, функція оплати через пристрій та інші. Бюджетні пристрої можуть не мати деяких з цих функцій.
4. Дизайн та матеріали: носимі пристрої від відомих виробників зазвичай мають більш привабливий та стильний дизайн, а також використовують високоякісні матеріали, такі як скло та метал, що забезпечує більш довговічну та надійну роботу пристрою. Бюджетні пристрої можуть мати менш привабливий дизайн та використовувати менш якісні матеріали.
5. Ціна: ціна на носимі пристрої від відомих виробників зазвичай вища, ніж на аналогічні пристрої бюджетного сегменту. Це пов'язано з більш високою якістю, функціональністю та обчислювальною потужністю пристроїв від крупних виробників. Однак, бюджетні носимі пристрої також мають свої переваги. Вони зазвичай коштують значно менше, і, залежно від конкретних потреб користувача, можуть виконувати ті самі функції, що й дорожчі моделі. Наприклад, деякі бюджетні смарт-годинники мають такі ж базові функції, як відстеження активності, серцевого ритму та навіть показники сну, які є в більш дорогих моделях.

Крім того, бюджетні носимі пристрої можуть бути більш доступні для більш широкого кола користувачів, зокрема для тих, хто тільки починає знайомитися з технологіями, або для тих, хто не хоче витрачати велику суму на новий гаджет.

Отже, хоча виробники, такі як Apple та Samsung, можуть пропонувати більше функцій та більш продумані дизайни, бюджетні носимі пристрої можуть бути достатніми для багатьох користувачів, особливо тих, хто шукає пристрій з базовими функціями та доступною ціною.

Висновки до розділу

Було проаналізовано доступні на ринку носимі пристрої, такі як розумні годинники, фітнес-браслети, розумні окуляри та інші. Були розглянуті функції та

можливості цих пристроїв, а також їх класифікація за походженням та ціновим сегментом.

При аналізі було звернуто увагу на ризики та переваги використання носимих пристроїв в питаннях безпеки та виробничих ризиків. Було виявлено, що носимі пристрої можуть допомогти у виявленні та попередженні ризиків на робочому місці, а також у покращенні продуктивності та комунікації між працівниками.

Наведені в цьому розділі приклади вказують на те, що використання різноманітних носимих пристроїв може допомогти збільшити ефективність та покращити умови праці на робочому місці.

Отже, можна зробити висновок, що носимі пристрої можуть стати важливим інструментом у поліпшенні робочого процесу та безпеки працівників на робочому місці. Проте, при використанні таких пристроїв необхідно враховувати певні ризики та переваги, а також враховувати індивідуальні потреби та вимоги кожного працівника.

Однак, варто бути уважним при виборі конкретного пристрою та його налаштуванням, щоб уникнути недоліків та проблем з безпекою. В цілому, аналіз переліку носимих пристроїв свідчить про те, що вони можуть стати корисними інструментами для покращення робочих умов та здоров'я працівників.

РОЗДІЛ 2. Аналіз платформ, на яких базуються носимі пристрої

2.1. Огляд платформ, на яких можуть базуватися носимі пристрої

У контексті аналізу платформ, на яких базуються носимі пристрої, термін "платформа" стосується апаратного та програмного середовища, на якому будуються та розробляються носимі пристрої. Він включає в себе мікроконтролери, мікропроцесори, операційні системи, фреймворки, інструменти програмування та інші компоненти, необхідні для створення та роботи носимих пристроїв [41].

Платформа визначає функціональні можливості, характеристики та обмеження пристрою. Вона надає розробникам інтерфейси програмування, набір бібліотек та інструментів для розробки програмного забезпечення, а також доступ до апаратних ресурсів, які дозволяють реалізувати різну функціональність носимих пристроїв.

Вибір платформи для розробки носимих пристроїв має велике значення, оскільки він визначає можливості, продуктивність та швидкість розробки. Різні платформи мають свої переваги та обмеження, і вибір залежить від конкретних потреб проекту та ресурсів, доступних розробникам.

Носимі пристрої бюджетного сегменту можуть бути побудовані на різних платформах, зокрема мікроконтролерах ESP32, AVR, STM32, PIC, Nordic nRF52 та інших.

Кожна з цих платформ має свої особливості та характеристики, що роблять їх придатними для використання в різних носимих пристроях. Нижче наведено загальний огляд цих платформ, їх технічних характеристик, переваг та недоліків у контексті розробки носимих пристроїв.

1. ESP32:

ESP32 – це серія мікроконтролерів, розроблених компанією Espressif Systems, яка широко використовується в розробці IoT-проектів та носимих пристроїв [26].

Архітектура мікроконтролерів ESP32 зображена на рисунку 2.1 [46].

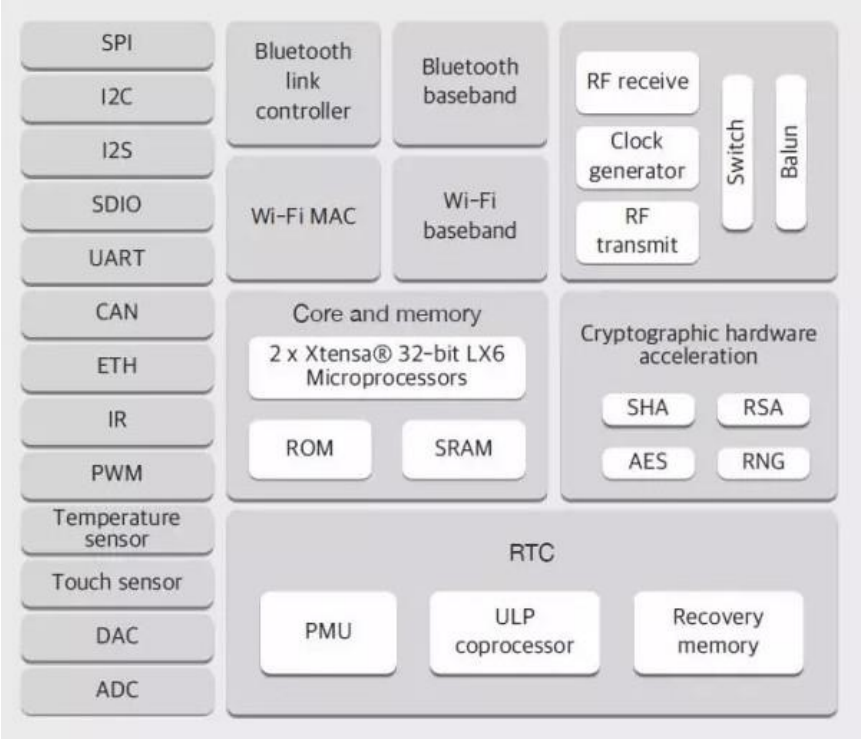

Рисунок 2.1 – Архітектура мікроконтролерів ESP32

Основні технічні характеристики ESP32 включають наступне [46]:

- Двоядерний мікропроцесор Xtensa LX6 з тактовою частотою до 240 МГц.
- Вбудовані Wi-Fi та Bluetooth модулі, що дозволяють бездротову комунікацію.
- Великий обсяг оперативної пам'яті (520 КБ) та флеш-пам'яті (4 МБ) для зберігання програмного забезпечення та даних.
- Розширені можливості введення-виведення, включаючи підтримку GPIO, SPI, I2C, UART та інших інтерфейсів.

- Вбудовані периферійні пристрої, такі як АЦП (аналого-цифровий перетворювач), ШІМ (широтно-імпульсна модуляція), таймери, сенсори каскаду пристроїв та багато іншого.
- Підтримка різних версій протоколів бездротового зв'язку, таких як Wi-Fi 802.11 b/g/n, Bluetooth Classic і Bluetooth Low Energy (BLE).

ESP32 мають ряд переваг для створення носимих пристроїв:

- Бездротові можливості: Наявність Wi-Fi та Bluetooth дозволяє забезпечити зв'язок з іншими пристроями, передавати дані, оновлювати програмне забезпечення та взаємодіяти з хмарними сервісами.
- Розширені можливості введення-виведення: Підтримка різних інтерфейсів та пристроїв введення-виведення дозволяє підключати датчики, дисплеї та інші зовнішні пристрої для вимірювання фізіологічних параметрів та взаємодії з користувачем.
- Розширюваність: Наявність роз'ємів GPIO та розширювальних роз'ємів дозволяє підключати додаткові модулі та сенсори для розширення функціональності носимих пристроїв.
- Великий ресурс пам'яті: ESP32 мають достатньо оперативної та флеш-пам'яті для зберігання програмного забезпечення, даних та виконання складних обчислень.
- Відкрита платформа: ESP32 базуються на відкритих стандартах та підтримується активною спільнотою розробників, що дозволяє отримати доступ до багатофункціональних бібліотек та ресурсів для швидкої розробки.

Хоча мікроконтролери ESP32 є потужною та популярною платформою для побудови носимих пристроїв, вони також мають деякі недоліки, зокрема:

- Енергоспоживання: ESP32 відомі своїм порівняно високим споживанням енергії. Це може бути проблемою для носимих

пристроїв, оскільки вони працюють на батарейці або акумуляторі й потребують енергоефективності для подовження тривалості роботи без заміни або зарядження джерела живлення. Однак, ESP32 мають різні режими енергоефективності, що дозволяє дещо подовжити тривалість використання носимих пристроїв без необхідності зарядки.

- Розмір: У порівнянні з деякими іншими мікроконтролерами, ESP32 має більшу фізичну площу. Це може бути проблемою для носимих пристроїв, які мають обмежений простір і потребують компактного дизайну.
- Вартість: Окремі моделі ESP32, порівняно з деякими аналогічними мікроконтролерами, можуть мати вищу вартість. Для деяких проектів в бюджетному сегменті це може бути недоліком.

Хоча ці недоліки можуть бути важливими факторами для окремих проектів, ESP32 все ж залишаються потужною платформою з великими можливостями для створення носимих пристроїв. Розробники можуть враховувати ці недоліки та шукати способи їх подолання, наприклад, шляхом оптимізації енергоспоживання або використання додаткових модулів для розширення функціональності.

Загалом, ESP32 є потужними мікроконтролерами з широким набором функцій і можливостей, який добре підходить для створення різних носимих пристроїв, включаючи смарт-годинники, фітнес-трекери, смарт-окуляри та інші.

2. AVR:

Мікроконтролери AVR (Alf and Vegard's RISC) є широко використовуваними мікроконтролерами, розробленими компанією Atmel (тепер Microchip Technology). Вони відомі своєю простотою використання, ефективністю ресурсів та широкою підтримкою відкритих інструментів розробки[11].

Мікроконтролери AVR є основою для платформи Arduino. Arduino є відкритою платформою розробки, яка використовує мікроконтролери AVR в якості основного компонента своїх плат. Ключовою особливістю Arduino є простота використання та розробки, що робить його популярним серед початківців та любителів.

Архітектура мікроконтролерів AVR зображена на рисунку 2.2 [1].

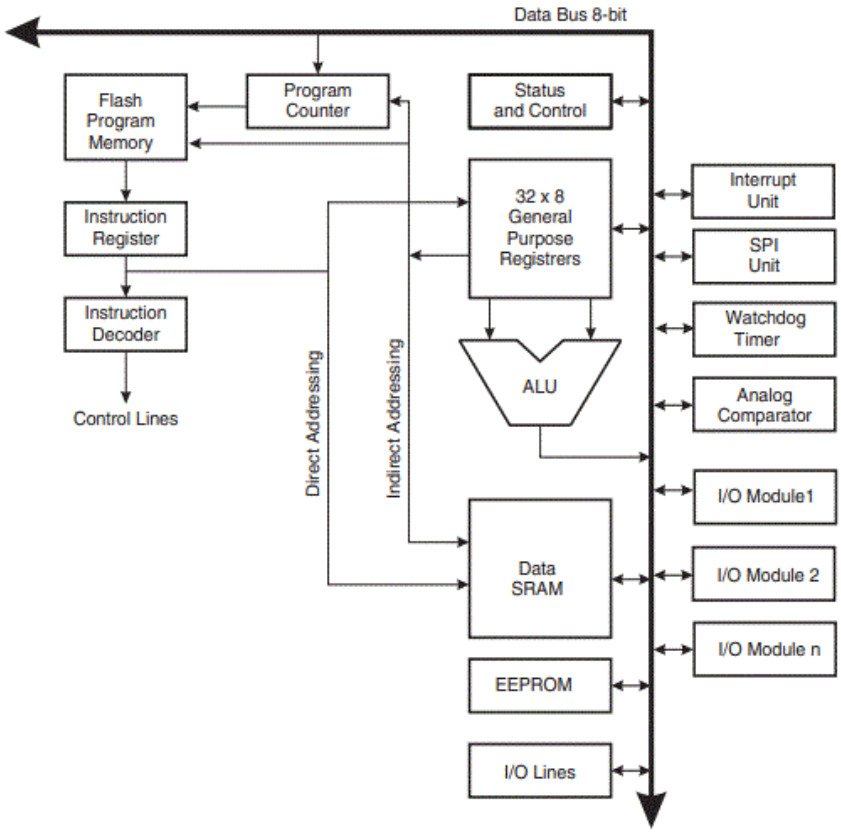

Рисунок 2.2 – Архітектура мікроконтролерів AVR

Основні технічні характеристики мікроконтролерів AVR включають наступне [11]:

- Архітектура RISC: AVR має просту та ефективну архітектуру RISC, що сприяє високій продуктивності та швидкому виконанню операцій.

- Низьке споживання енергії: AVR відомі своєю відносною енергоефективністю, що робить їх ідеальними для застосування в носимих пристроях з обмеженим джерелом живлення.
- Частота тактування: Зазвичай мікроконтролери AVR мають частоту тактування від 1 до 20 МГц, залежно від конкретної моделі.
- Пам'ять: AVR має вбудовану флеш-пам'ять для зберігання програмного забезпечення та EEPROM для зберігання даних. Розмір пам'яті може варіюватися від кількох кілобайт до кількох десятків кілобайт.
- Периферійні пристрої: AVR підтримує різні пристрої введення-виведення, такі як GPIO, UART, SPI, I2C, таймери, АЦП та інші. Це дозволяє підключати різні сенсори та пристрої для вимірювання фізіологічних параметрів та взаємодії з ними.

Мікроконтролери AVR мають декілька переваг для створення носимих пристроїв:

- Енергоефективність: Завдяки своєму відносно низькому споживанню енергії, AVR дозволяє подовжити час роботи носимих пристроїв від одного заряду батареї.
- Компактність: AVR мають невеликі розміри та малу кількість елементів, що робить їх ідеальними для використання в носимих пристроях з обмеженим простором.
- Легкість розробки: Мікроконтролери AVR мають простий та зрозумілий набір інструкцій, що спрощує процес розробки програмного забезпечення для носимих пристроїв.
- Відкрита спільнота: AVR підтримуються широкою спільнотою розробників, що забезпечує доступ до багатьох бібліотек та ресурсів для швидкої розробки.

Мікроконтролери AVR, хоча вони широко використовуються і мають свої переваги, також мають деякі недоліки для побудови носимих пристроїв. Основні недоліки мікроконтролерів AVR включають наступне:

- Обмежена продуктивність: AVR має обмежену швидкість обробки та кількість ресурсів порівняно з більш потужними мікроконтролерами, такими як ARM або MIPS. Це може бути недоліком для деяких вимогливих застосунків, особливо якщо потрібні висока швидкість обробки або обробка великого обсягу даних.
- Обмежена пам'ять: Більшість мікроконтролерів AVR мають обмежену кількість внутрішньої пам'яті. Це може бути недоліком, якщо потрібно зберігати великі обсяги даних або виконувати складні алгоритми, які вимагають багато пам'яті.
- Відсутність деяких функцій: AVR може бути обмежений у підтримці деяких передових функцій, таких як шифрування, віддалене керування або підтримка високошвидкісного інтерфейсу комунікації. Це може бути недоліком для деяких спеціалізованих додатків, які вимагають розширеної функціональності.
- Енергоефективність: AVR може бути менш енергоефективним порівняно з деякими сучасними мікроконтролерами, що може бути проблемою для носимих пристроїв, які працюють на батарейках або акумуляторах.
- Обмежена підтримка розширень: Іншим недоліком може бути обмежена підтримка розширень та додаткових модулів. Деякі мікроконтролери AVR можуть мати обмежені порти введення-виведення або не підтримувати певні типи зовнішніх пристроїв.

Незважаючи на ці недоліки, мікроконтролери AVR все ще є популярними та ефективними для багатьох простих та середньої складності носимих пристроїв.

Розробники можуть враховувати ці обмеження та знаходити компроміси для досягнення бажаних функцій та продуктивності.

Узагальнюючи, мікроконтролери AVR є популярним вибором для створення носимих пристроїв завдяки своїм технічним характеристикам, ціні та простоті використання. Вони дозволяють розробникам швидко створювати носимі пристрої, забезпечуючи розширені можливості введення-виведення для інтеграції з фізіологічними сенсорами та зовнішніми пристроями.

Мікроконтролери AVR є ключовим компонентом платформи Arduino, яка надає зручну та доступну засоби розробки для електроніки та носимих пристроїв.

3. STM32:

Мікроконтролери STM32, розроблені компанією STMicroelectronics, є потужними та універсальними пристроями для різноманітних застосувань, включаючи носимі пристрої. Вони базуються на архітектурі ARM Cortex-M та пропонують широкий спектр моделей з різними технічними характеристиками.

Архітектура мікроконтролерів STM32 зображена на рисунку 2.3 [10].

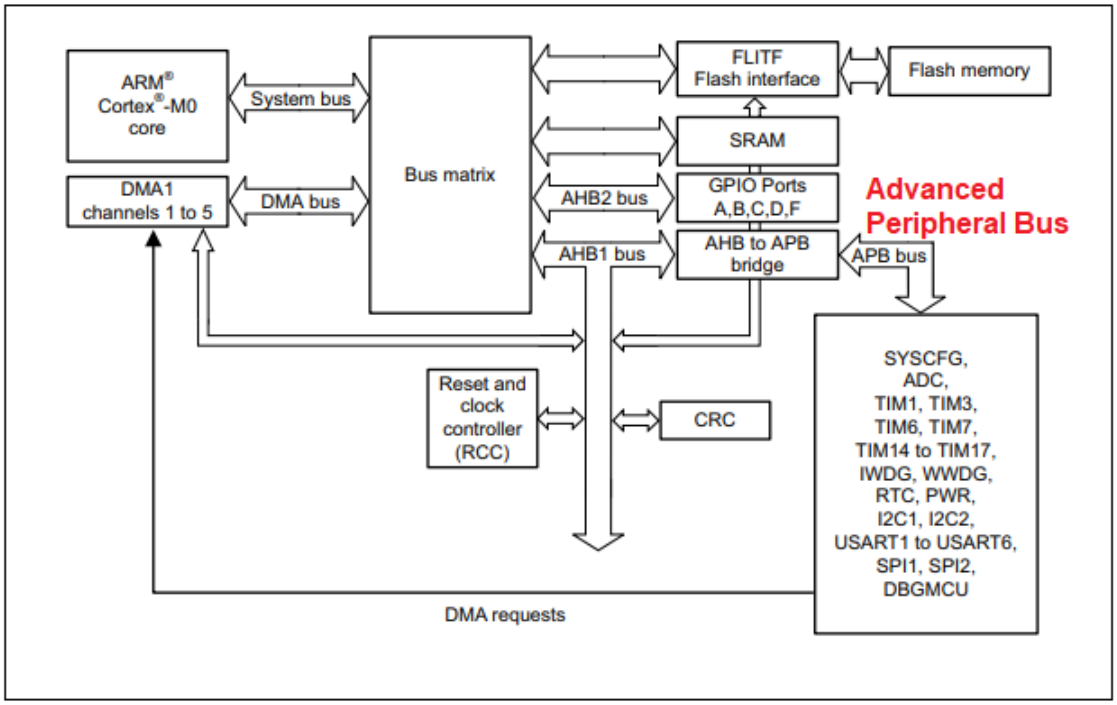

Рисунок 2.3 – Архітектура мікроконтролерів STM32

Основні технічні характеристики мікроконтролерів STM32 включають наступне [10]:

- Архітектура ARM Cortex-M: STM32 використовує ядро ARM Cortex-M, що забезпечує високу продуктивність та швидкість операцій.
- Частота тактування: Мікроконтролери STM32 можуть мати частоту тактування від 20 МГц до 550 МГц, залежно від конкретної моделі.
- Пам'ять: STM32 пропонують великий обсяг внутрішньої флеш-пам'яті для зберігання програмного забезпечення та EEPROM або FRAM для зберігання даних. Розмір пам'яті може варіюватися від кількох кілобайт до кількох мегабайт.
- Периферійні пристрої: STM32 підтримують різноманітні периферійні пристрої, такі як GPIO, UART, SPI, I2C, таймери, АЦП, ЦАП, USB та багато іншого. Це дозволяє підключати різні сенсори, дисплеї та інші пристрої до носимих пристроїв.

- Енергоефективність: STM32 мають режими низького споживання енергії, що дозволяє зберігати заряд батареї та продовжувати час роботи носимого пристрою.

Мікроконтролери STM32 мають декілька переваг для створення носимих пристроїв:

- Висока продуктивність: Завдяки потужному ядру ARM Cortex-M та великому обсягу пам'яті STM32 дозволяють розробляти досить складні програми та обробляти дані в реальному часі.
- Багатофункціональність: STM32 підтримують різноманітні периферійні пристрої, що дозволяє легко підключати датчики, дисплеї та інші пристрої до носимих пристроїв.
- Низьке споживання енергії: STM32 мають режими низького споживання енергії, що дозволяє ефективно використовувати енергію батареї та продовжувати час роботи носимого пристрою.
- Підтримка розробки: Компанія STMicroelectronics надає багатий набір інструментів для розробки, включаючи середовище розробки STM32CubeIDE, багато бібліотек та прикладів коду.

Мікроконтролери STM32, хоча вони мають багато переваг, також мають деякі недоліки для побудови носимих пристроїв. Основні недоліки мікроконтролерів STM32 включають наступне:

- Розмір: Деякі моделі мікроконтролерів STM32 можуть бути фізично більшими за розміром та мати більшу кількість ніжок, що може бути обмеженням для носимих пристроїв з обмеженим простором. Крім того, паяння та розміщення таких мікроконтролерів можуть бути складним на невеликих платах.
- Вартість: Зазвичай, мікроконтролери STM32 належать до вищого цінового сегменту порівняно з деякими іншими мікроконтролерами

на ринку. Це може вплинути на доступність для проектів з обмеженим бюджетом.

- Складність програмування: Для розробки програмного забезпечення для мікроконтролерів STM32 може знадобитися певний рівень експертизи та досвіду. Вони мають розширений набір функціональних можливостей, що може вимагати більшої складності у програмуванні та налагодженні.

Незважаючи на ці недоліки, мікроконтролери STM32 все ще є популярними та потужними засобами для розробки носимих пристроїв. За правильного підходу та оптимізації, ці недоліки можуть бути переважені значними перевагами STM32, такими як висока продуктивність, багатофункціональність та гнучкість.

4. PIC:

Мікроконтролери PIC (Peripheral Interface Controller) є серією мікроконтролерів, розроблених компанією Microchip Technology Inc. Вони відомі своєю надійністю, ефективністю та широким спектром застосувань.

Архітектуру мікропроцесорів PIC зображено на рисунку 2.4 [51].

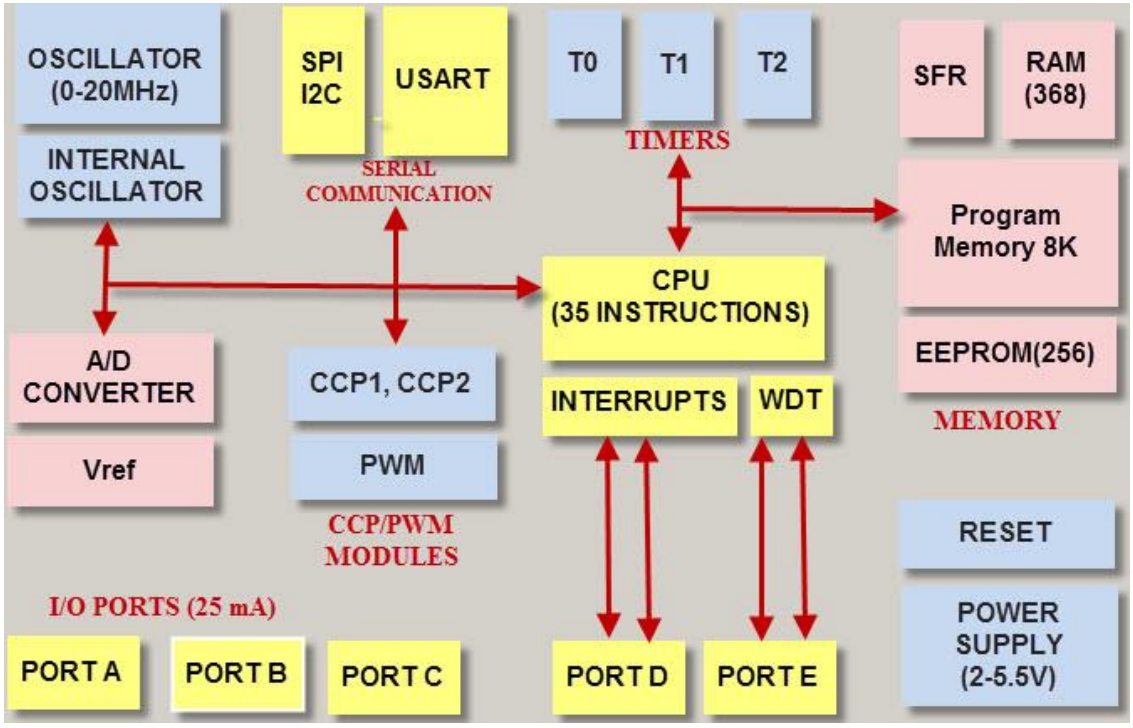

Рисунок 2.4 – Архітектура мікропроцесорів PIC

Мікроконтролери PIC можуть бути використані для створення різноманітних носимих пристроїв з різними функціями. Нижче наведені деякі загальні технічні характеристики та можливості мікроконтролера PIC [35]:

- Архітектура: Мікроконтролери PIC використовують 8-, 16- або 32-розрядну архітектуру. Вони мають вбудовану пам'ять програм та даних, а також різноманітні периферійні пристрої, такі як UART, SPI, I2C, таймери, АЦП та ШІМ-генератори.
- Швидкість: Мікроконтролери PIC працюють на різних швидкостях тактування, що залежить від конкретної моделі. Вони можуть мати велику швидкість виконання і дозволяють обробляти дані в реальному часі.
- Енергоефективність: Багато мікроконтролерів PIC мають низьке споживання енергії, що робить їх привабливим варіантом для носимих пристроїв, де тривалість роботи від батареї є важливою.
- Розширюваність: Мікроконтролери PIC підтримують різні інтерфейси, що дозволяють легко підключати зовнішні пристрої та сенсори. Вони також підтримують різні комунікаційні протоколи, такі як UART, SPI, I2C, що робить їх універсальними для взаємодії з іншими пристроями.
- Розробка та підтримка: Microchip надає розширену систему розробки програмного забезпечення (MPLAB X IDE) та набір бібліотек, що полегшують розробку на мікроконтролерах PIC. Також доступні документація, приклади коду та підтримка спільноти, що допомагають розробникам у роботі з мікроконтролерами PIC.

Мікроконтролери PIC мають деякі недоліки, які можуть вплинути на їх використання у побудові носимих пристроїв. Основні недоліки мікроконтролерів PIC включають наступне:

- Обмежена продуктивність: Деякі моделі мікроконтролерів PIC мають обмежену потужність та продуктивність порівняно з іншими

мікроконтролерами на ринку. Це може бути обмеженням для складніших функцій та завдань, які можуть виникати у носимих пристроях.

- Обмежені функціональні можливості: Деякі моделі мікроконтролерів PIC можуть мати обмежений набір функціональних можливостей порівняно зі спеціалізованими мікроконтролерами. Це може обмежувати гнучкість та розширені можливості, які можуть бути важливими для носимих пристроїв.
- Відсутність вбудованої бездротової комунікації: Деякі моделі мікроконтролерів PIC можуть не мати вбудованих модулів бездротової комунікації, таких як Bluetooth або Wi-Fi. Це може вимагати додаткових зусиль та витрат для додавання бездротового зв'язку до носимого пристрою.
- Обмежена підтримка спільноти та ресурсів: Порівняно з деякими іншими мікроконтролерами, PIC може мати обмежену кількість доступних ресурсів, бібліотек та прикладних програм. Це може ускладнити розробку та отримання допомоги під час роботи з ними.

Незважаючи на ці недоліки, мікроконтролери PIC залишаються популярними в різних додатках, включаючи носимі пристрої. З правильним плануванням, оптимізацією та вибором відповідних моделей, багато з цих недоліків можуть бути подолані.

- Nordic nRF52:

Мікроконтролер Nordic nRF52 є одним з популярних мікроконтролерів, розроблених компанією Nordic Semiconductor. Він має високий рівень інтеграції, дуже високу енергоефективність завдяки технології BLE (Bluetooth Low Energy) та широкий набір функцій, що робить його привабливим вибором для розробки носимих пристроїв.

Архітектура мікропроцесорів Nordic nRF52 наведена на рисунку 2.5[32].

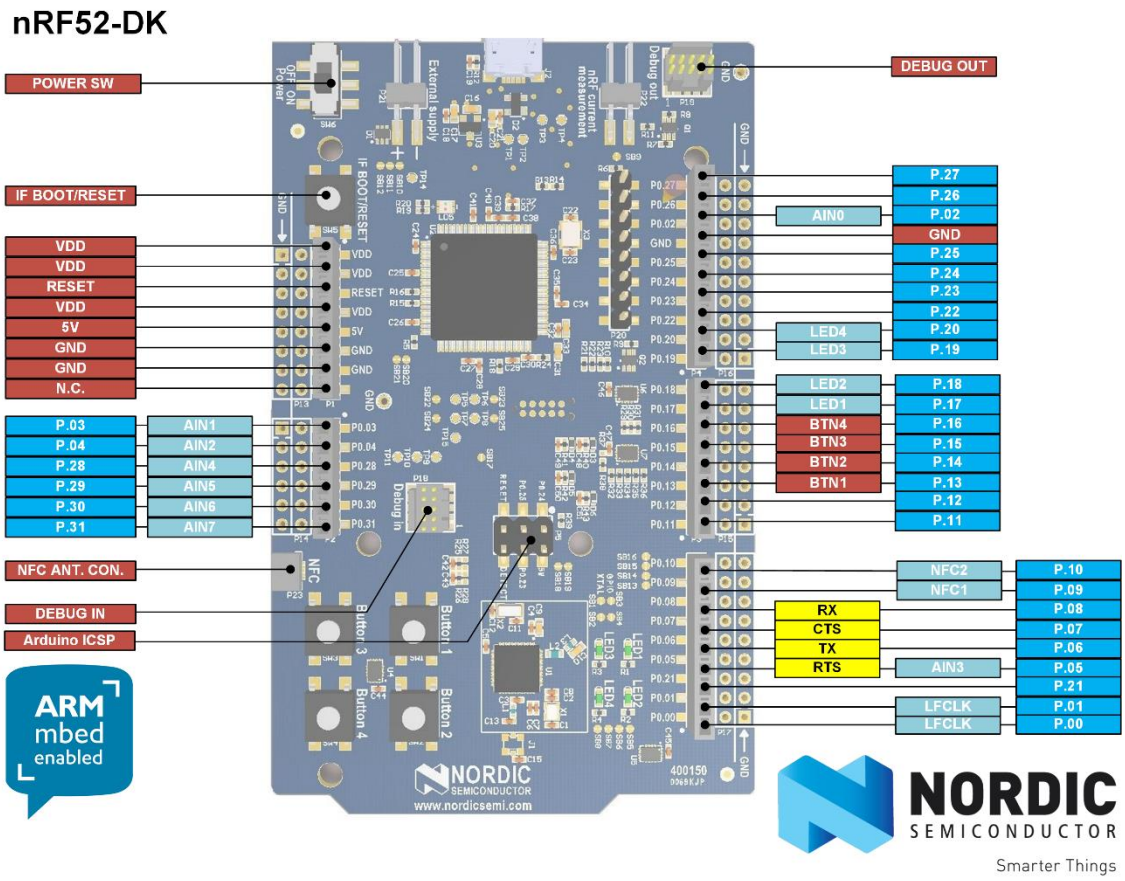

Рисунок 2.5 – Архітектура мікроконтролера Nordic nRF52

Основні технічні характеристики мікроконтролерів Nordic nRF52 включають наступне [32]:

- Архітектура: Nordic nRF52 використовує 32-розрядну архітектуру ARM Cortex-M4F. Це дозволяє виконувати складні операції і обробку даних в реальному часі.
- Частота тактування: Мікроконтролери Nordic nRF52 працюють на високих швидкостях тактування, зазвичай від 16 до 64 МГц. Вища швидкість дозволяє виконувати обчислення та завдання швидше.
- Вбудована пам'ять: Nordic nRF52 має вбудовану флеш-пам'ять для зберігання програмного забезпечення та даних. Розмір пам'яті може варіюватися в залежності від конкретної моделі мікроконтролера.

Мікроконтролери Nordic NRF52 мають декілька переваг для створення носимих пристроїв:

- Бездротові можливості: Однією з ключових особливостей Nordic nRF52 є вбудований радіомодуль, який підтримує бездротові комунікаційні протоколи, такі як Bluetooth Low Energy (BLE) і ANT. Це дозволяє носимим пристроям підключатися до інших пристроїв та взаємодіяти з ними.
- Енергоефективність: Мікроконтролери Nordic nRF52 відомі своїм дуже низьким споживанням енергії. Вони мають різні режими сну та функції оптимізації енергоспоживання, що дозволяють подовжити тривалість роботи носимих пристроїв на акумуляторах.
- Периферійні пристрої: Мікроконтролери Nordic nRF52 мають широкий набір периферійних пристроїв, таких як UART, SPI, I2C, GPIO, таймери, АЦП та ШІМ-генератори. Це дозволяє підключати різноманітні датчики, дисплеї та інші пристрої до носимих пристроїв.
- Розробне середовище: Nordic Semiconductor надає розробникам спеціальне розробне середовище - Nordic nRF5 SDK, яке містить набір інструментів, драйверів та прикладів коду для розробки програмного забезпечення для мікроконтролерів Nordic nRF52.

Мікроконтролери Nordic nRF52 мають декілька недоліків, які можуть вплинути на їх використання у побудові носимих пристроїв. Основні недоліки мікроконтролерів Nordic nRF52 включають наступне:

- Обмежена вбудована пам'ять: Деякі моделі мікроконтролерів Nordic nRF52 мають обмежену кількість вбудованої пам'яті. Це може стати обмеженням для зберігання великої кількості даних або виконання складних програм.
- Складніша програмна розробка: Розробка програм для мікроконтролерів Nordic nRF52 може бути складнішою порівняно з

іншими мікроконтролерами. Це пов'язано з їх особливими функціями і конфігурацією, що вимагає глибшого розуміння специфіки цих мікроконтролерів.

- Висока вартість: Nordic nRF52 відомий як мікроконтролер високого класу, і його вартість може бути вищою порівняно з іншими мікроконтролерами доступного сегменту. Це може вплинути на бюджет проекту, особливо для пристроїв бюджетного сегменту.
- Обмежена підтримка спільноти: Хоча у Nordic nRF52 є активна спільнота розробників, порівняно з деякими іншими мікроконтролерами вона може бути меншою. Це може ускладнити отримання підтримки, додаткових ресурсів та прикладних програм для розробки носимих пристроїв.

Незважаючи на ці недоліки, мікроконтролери Nordic nRF52 мають потужні можливості для розробки носимих пристроїв, зокрема щодо бездротового зв'язку, високої енергоефективності та підтримки різних сенсорів. З правильним підходом та розробкою, ці недоліки можуть бути зменшені, а мікроконтролери Nordic nRF52 можуть стати потужним інструментом для розробки ефективних та інноваційних носимих пристроїв.

2.2. Класифікація платформ на основі цінового сегменту:

На основі цінового сегменту можна провести наступну класифікацію мікроконтролерів:

1. Низький ціновий сегмент (бюджетні платформи). Ці платформи пропонують вигідні вартість та доступність для широкого кола розробників при наявності мінімального необхідного функціоналу для створення носимих пристроїв. :
   - AVR мікроконтролери, такі як ATmega328P, зазвичай доступні за низьку ціну і широко використовуються в бюджетних проектах.

- Деякі моделі STM32 і PIC мікроконтролерів також можуть бути доступними в низькому ціновому сегменті.

2. Середній ціновий сегмент (професійні платформи). Ці платформи мають більш просунуті функції та можливості, але вони можуть бути дорожчими.:
   - ESP32 мікроконтролери зазвичай пропонуються в середньому ціновому діапазоні з урахуванням їх функціональності та можливостей.
   - Деякі моделі STM32 мікроконтролерів можуть бути доступними в середньому ціновому сегменті залежно від їх характеристик та функціональних можливостей.
3. Високий ціновий сегмент (високопродуктивні платформи). Ці платформи розраховані на професійних розробників і мають потужні функції та великий обсяг пам'яті, різні режими живлення, що дозволяє забезпечити вищу енергоефективнсть. Вони можуть використовуватись для розробки носимих пристроїв зі складними функціями та великою кількістю датчиків. Зокрема, прикладами мікроконтролерів високого цінового сегменту є:
   - Nordic nRF52 мікроконтролери зазвичай пропонуються в високому ціновому діапазоні, оскільки вони надають широкий спектр функціональності та високий рівень продуктивності.
   - Деякі моделі STM32 та PIC мікроконтролерів, з особливими характеристиками або додатковими можливостями, також можуть бути доступними в високому ціновому сегменті.

Важливо зазначити, що цінова політика виробників може змінюватись з часом, а також можуть бути доступні різні моделі та варіанти кожного мікроконтролера з різними ціновими пропозиціями. Отже, перед вибором мікроконтролера важливо детально ознайомитись з цінами та можливостями конкретних моделей на ринку.

Класифікація платформ на основі бюджетного сегменту дозволяє розробникам знаходити оптимальні рішення для своїх проектів, враховуючи вартість та функціональні вимоги. Залежно від обсягу фінансування та потреб

проекту, розробники можуть вибрати платформу, яка найкраще відповідає їхнім потребам та можливостям.

2.3. Порівняння особливостей та функцій платформ

Кожен з досліджених мікроконтролерів має свої особливості та функціональні можливості, які варто порівняти. Нижче наведено порівняння деяких з них:

1. Процесор:
    - ESP32: Dual-core Tensilica LX6 (240 MHz)
    - AVR: Залежить від конкретної моделі, наприклад, ATmega328P (20 MHz)
    - STM32: Залежить від конкретної моделі, наприклад, ARM Cortex-M4 (частота до 180 MHz)
    - PIC: Залежить від конкретної моделі, наприклад, PIC18F4520 (40 MHz)
    - Nordic nRF52: ARM Cortex-M4F (64 MHz)
2. WiFi та Bluetooth:
    - ESP32: Вбудовані модулі WiFi та Bluetooth
    - AVR: Вбудованих модулів WiFi та Bluetooth немає
    - STM32: Залежить від конкретної моделі, деякі моделі мають вбудовані модулі WiFi та Bluetooth
    - PIC: Вбудованих модулів WiFi та Bluetooth немає
    - Nordic nRF52: Вбудовані модулі Bluetooth, деякі моделі мають вбудовані модулі WiFi
3. Швидкість розробки:

- ESP32: Широкий спектр документації, підтримка Arduino IDE
- AVR: Широкий спектр документації, велика спільнота користувачів, підтримка Arduino IDE
- STM32: Розширена документація, підтримка різних IDE (наприклад, STM32CubeIDE), має розширений набір функціональних можливостей, що може вимагати більшої складності у програмуванні та налагодженні.
- PIC: Зріла та широка спільнота користувачів, підтримка MPLAB IDE
- Nordic nRF52: Добре документована, підтримка Nordic SDK та IDE (наприклад, nRF5 SDK, Segger Embedded Studio)

4. Об'єм пам'яті:
    - ESP32: Залежить від конкретної моделі, наприклад, Flash пам'ять до 4MB, RAM до 520KB
    - AVR: Обмежений об'єм Flash та RAM пам'яті в залежності від конкретної моделі
    - STM32: Залежить від конкретної моделі, наприклад, Flash пам'ять від 32KB до 2MB, RAM від 2KB до 640KB
    - PIC: Залежить від конкретної моделі, наприклад, Flash пам'ять від 2KB до 512KB, RAM від 128B до 128KB
    - Nordic nRF52: Залежить від конкретної моделі, наприклад, Flash пам'ять від 128KB до 1MB, RAM від 16KB до 256KB
5. Енергоефективність:
    - ESP32: Придатний для носимих пристроїв, але споживання енергії може бути вищим у порівнянні з деякими іншими мікроконтролерами

- AVR: Добра енергоефективність, споживання енергії залежить від конкретної моделі та налаштувань
- STM32: Добра енергоефективність, можливість роботи в режимі низького споживання енергії
- PIC: Добра енергоефективність, споживання енергії залежить від конкретної моделі та налаштувань
- Nordic nRF52: Висока енергоефективність, спеціалізований на роботі з Bluetooth Low Energy та низьким споживанням енергії

Важливо враховувати, що конкретні моделі мікроконтролерів можуть мати різні технічні характеристики, тому рекомендується звертатись до документації виробника та додаткових ресурсів для отримання детальної інформації перед вибором мікроконтролера для конкретного проекту.

2.4. Порівняння можливостей носимих пристроїв на основі різних платформ

Можливості носимих пристроїв на основі мікроконтролерів ESP32, AVR, STM32, PIC та Nordic nRF52 залежать від конкретних моделей та реалізацій. Нижче наведено загальний огляд можливостей цих мікроконтролерів для створення носимих пристроїв:

1. ESP32:
    - Потужні процесори з двома ядрами
    - Вбудовані модулі WiFi та Bluetooth для забезпечення зв'язку
    - Широкі можливості розробки, підтримка Arduino IDE та інших фреймворків
    - Підтримка низького споживання енергії
    - Підтримка різних сенсорів та інтерфейсів, таких як GPIO, I2C, SPI, UART

2. AVR:
    - Надійні та добре відомі мікроконтролери
    - Підтримка широкого спектру периферійних пристроїв
    - Велика спільнота користувачів, що сприяє доступності документації та підтримки
    - Широкий вибір розробних платформ, зокрема Arduino
    - Знижена споживання енергії для батарейного живлення
3. STM32:
    - Потужні процесори ARM Cortex-M з високою частотою роботи
    - Розширені можливості розробки та розширена документація
    - Великий обсяг пам'яті для зберігання програмного коду та даних
    - Підтримка різних інтерфейсів та протоколів зв'язку, включаючи USB, Ethernet, CAN, I2C, SPI
    - Можливість використання режимів низького споживання енергії для продовження роботи від батарейного живлення
4. PIC:
    - Широкий спектр моделей з різними розмірами пам'яті та функціональними можливостями
    - Велика кількість периферійних пристроїв та інтерфейсів, включаючи ADC, PWM, I2C, SPI, UART
    - Підтримка низького споживання енергії
    - Висока надійність та відповідність стандартам безпеки
5. Nordic nRF52:
    - Спеціалізований на роботі з Bluetooth Low Energy (BLE)

- Вбудовані модулі BLE та низького споживання енергії
- Підтримка різних сенсорів та інтерфейсів, таких як GPIO, I2C, SPI, UART
- Можливість розробки на основі фреймворків, таких як Arduino та Nordic SDK
- Додаткові можливості, такі як високочастотне радіо, NFC та інші

Вибір мікроконтролера для носимих пристроїв залежить від конкретних вимог проекту, включаючи функціональність, споживання енергії, розмір, наявність необхідних інтерфейсів та розробних інструментів. Рекомендується ознайомитись з документацією виробників та спробувати прототипування на різних платформах для знаходження найбільш підходящого варіанту для конкретного проекту.

Вибір між платформою для носимих пристроїв залежить від конкретних вимог вашого проекту, таких як бездротові можливості, потужність, кількість GPIO-портів та доступність розширень.

Висновки до розділу

Аналіз платформ, на яких базуються носимі пристрої, дозволяє розробникам вибрати найбільш підходящу платформу для своїх проектів, зрозуміти різні можливості та обмеження кожної платформи.

Існує широкий вибір платформ, що підходять для розробки носимих пристроїв, включаючи мікроконтролери ESP32, AVR, STM32, PIC та Nordic nRF52. Кожна платформа має свої унікальні характеристики, переваги та обмеження.

Порівнюючи носимі пристрої на основі цих платформ, можна сказати, що кожна платформа може бути успішно використана для створення різних типів носимих пристроїв, включаючи смарт-годинники, фітнес-трекери, смарт-

окуляри тощо. Вибір платформи залежить від конкретних вимог та функцій, які потрібні для проекту.

Класифікація платформ на основі бюджетного сегменту дозволяє вибрати оптимальну платформу залежно від вимог проекту та доступних ресурсів. Незалежно від обраної платформи, носимі пристрої забезпечують широкі можливості в галузі моніторингу здоров'я, відстеження активності та взаємодії з користувачем.

РОЗДІЛ 3. Аналіз переліку вразливостей, які найчастіше мають місце для платформ, на яких побудовані носимі пристрої

Разом із зростанням популярності носимих пристроїв, з'являються й нові виклики щодо їхньої безпеки. Як і будь-які інші підключені пристрої, носимі пристрої можуть бути вразливими до різних видів атак, що може ставити під загрозу як конфіденційні дані користувача, так і його фізичний добробут.

У цьому розділі розглянуто найпоширеніші вразливості, які можуть впливати на носимі пристрої, побудовані на платформах ESP32, AVR, STM32, PIC та Nordic nRF52, а також ризики, пов'язані з цими платформами.

3.1. Аналіз найпоширеніших вразливостей на платформі ESP32:

Можна розглянути найпоширеніші вразливості конкретної платформи ESP32 та їх можливі наслідки для безпеки носимих пристроїв:

- Незахищений доступ до Wi-Fi мережі: Деякі версії програмного забезпечення ESP32 мають вразливості, які можуть дозволити зловмиснику отримати несанкціонований доступ до Wi-Fi мережі, до якої підключений ESP32. Це може призвести до зловживання мережевими ресурсами, перехоплення трафіку або навіть зламу зв'язку з пристроями, пов'язаними з мережею [13].
- Вразливість SSL/TLS: Деякі версії ESP32 можуть мати проблеми з реалізацією SSL/TLS протоколів, які використовуються для шифрування трафіку. Це може призвести до витоку конфіденційної інформації, такої як паролі або особисті дані, якщо зловмисник здійснить атаку перехоплення трафіку.
- Уразливості Bluetooth: ESP32 підтримує бездротовий протокол Bluetooth, і деякі версії можуть мати вразливості, що дозволяють зловмисникам перехоплювати або навіть контролювати з'єднання Bluetooth з пристроями. Це може призвести до несанкціонованого

доступу до носимого пристрою або його функціоналу, а також до витоку конфіденційних даних.

- Недостатня перевірка даних вводу: Деякі програми, розроблені для ESP32, можуть мати вразливості, пов'язані з недостатньою перевіркою даних вводу. Це може призвести до атак типу "впровадження зловмисного коду" або "переповнення буфера", що дозволить зловмисникам виконувати власний код на пристрої і зламувати його функціональність.
- Вразливості веб-інтерфейсу: Деякі версії ESP32 можуть мати вразливості веб-інтерфейсу, які дозволяють зловмисникам отримувати несанкціонований доступ до налаштувань пристрою або впливати на його роботу. Це може призвести до зміни параметрів, витоку конфіденційних даних або навіть знищення пристрою.

Аналіз цих вразливостей є важливим кроком у забезпеченні безпеки носимих пристроїв на базі ESP32. Розробники та виробники повинні бути обізнані з цими проблемами і вживати заходів для їх вирішення, таких як оновлення програмного забезпечення, застосування захисних механізмів та аудит безпеки програмного забезпечення.

3.2. Аналіз найпоширеніших вразливостей на платформі AVR

Аналіз найпоширеніших вразливостей на мікроконтролері AVR допомагає виявити ризики, пов'язані з безпекою та захистом цієї платформи. Деякі з найбільш поширених вразливостей на мікроконтролері AVR включають:

- Вразливість переповнення буфера: Мікроконтролери AVR можуть піддаватися атакам типу "переповнення буфера", коли зловмисник намагається записати більше даних у буфер, ніж він може вмістити. Це може призвести до перезапису важливих даних та виконання

зловмисного коду, що може вразити безпеку пристрою та його функціональність.

- Уразливості зворотного інжинірінгу: Мікроконтролери AVR можуть мати уразливості, які дозволяють зловмисникам здійснювати зворотний інжинірінг пристрою. Це може призвести до розкриття конфіденційної інформації, такої як алгоритми шифрування, ключі безпеки або захищений вміст пам'яті.
- Вразливості безпеки мережевого з'єднання: Мікроконтролери AVR, які підтримують мережеві протоколи, такі як Ethernet або Wi-Fi, можуть бути піддаються вразливостям у мережевому з'єднанні. Це може включати незахищені канали зв'язку, недостатню аутентифікацію або можливість зловмисника перехопити або змінити передаванні дані.
- Вразливості фізичного доступу: Уразливості, пов'язані з фізичним доступом до мікроконтролера AVR, можуть включати можливість несанкціонованого доступу до його пам'яті, зміну флеш-пам'яті або конфігураційних налаштувань, а також злам фізичних захисних механізмів.
- Вразливості програмного забезпечення: Вразливості у програмному забезпеченні, що виконується на мікроконтролері AVR, можуть включати недостатню перевірку даних вводу, уразливості шифрування, можливість виконання зловмисного коду або недостатню автентифікацію та контроль доступу.

Ці вразливості можуть мати потенційно серйозні наслідки для безпеки пристроїв, побудованих на мікроконтролері AVR, включаючи можливість втрати конфіденційних даних, зниження функціональності, порушення приватності користувача та можливість використання пристрою для злочинних дій.

3.3. Аналіз найпоширеніших вразливостей на платформі STM32

В ході аналізу носимих пристроїв, побудованих на платформі STM32 було виявлено наступні потенційні вразливості:

- Вразливості переповнення стеку: Мікроконтролери STM32 можуть бути піддаються атакам типу "переповнення стеку", коли зловмисник збільшує обсяг даних, які записуються в стек, понад його ліміти. Це може призвести до перезапису важливих даних та виконання зловмисного коду, що може вразити безпеку пристрою та його функціональність.
- Вразливості управління пам'яттю: Мікроконтролери STM32 можуть мати вразливості, пов'язані з недостатнім управлінням пам'яттю. Це може включати виток пам'яті, доступ до недозволених областей пам'яті або неправильне використання пам'яті, що може призвести до збоїв у роботі пристрою або розкриття конфіденційної інформації.
- Вразливості мережевих протоколів: Мікроконтролери STM32, які підтримують мережеві протоколи, такі як Ethernet або Wi-Fi, можуть бути піддаються вразливостям у мережевому з'єднанні. Це може включати незахищені канали зв'язку, недостатню аутентифікацію або можливість зловмисника перехопити або змінити передаванні дані.
- Вразливості шифрування та безпеки даних: Мікроконтролери STM32 можуть мати вразливості, що стосуються шифрування та безпеки даних. Це може включати недостатню довжину ключів шифрування, недостатню перевірку цілісності даних або можливість зламу шифрування, що може призвести до витоку конфіденційних даних або несанкціонованого доступу до пристрою.

- Уразливості фізичного доступу: Уразливості, пов'язані з фізичним доступом до мікроконтролера STM32, можуть включати можливість виконання несанкціонованого програмного коду, зміну налаштувань пристрою або навіть заміну фізичних компонентів. При недостатній фізичній захисті пристрою, зловмисник може мати можливість зламати систему та отримати несанкціонований доступ до її функціональності та даних.

Ці вразливості можуть становити серйозну загрозу безпеці мікроконтролерів STM32 та пристроїв, що використовують ці мікроконтролери. Проактивне застосування належних заходів безпеки, таких як регулярне оновлення програмного забезпечення, використання захищених протоколів зв'язку, належне управління пам'яттю та обмеження фізичного доступу можуть значно зменшити ризик впливу цих вразливостей на мікроконтролери STM32.

3.4. Аналіз найпоширеніших вразливостей на платформі PIC

В ході дослідження носимих пристроїв, побудованих на основі мікроконтролерів PIC, було виявлено наступні вразливості:

- Вразливості переповнення буфера: Мікроконтролери PIC можуть бути піддаються атакам типу "переповнення буфера", коли зловмисник вводить більшу кількість даних, ніж є місця в буфері для їх зберігання. Це може призвести до перезапису важливих даних, виконання зловмисного коду та збоїв у роботі пристрою.

- Вразливості управління пам'яттю: Мікроконтролери PIC можуть мати вразливості, пов'язані з недостатнім управлінням пам'яттю. Це може включати витік пам'яті, неправильне використання пам'яті або можливість зловмисників отримати доступ до недозволених областей пам'яті, що може призвести до збоїв у роботі пристрою та витоку конфіденційної інформації.

- Вразливості мережевих протоколів: Мікроконтролери PIC, які підтримують мережеві протоколи, такі як Ethernet або Wi-Fi, можуть бути піддаються вразливостям у мережевому з'єднанні. Це може включати незахищені канали зв'язку, недостатню аутентифікацію або можливість зловмисників перехопити або змінити передаванні дані.
- Вразливості шифрування та безпеки даних: Мікроконтролери PIC можуть мати вразливості, що стосуються шифрування та безпеки даних. Це може включати недостатню довжину ключів шифрування, недостатню перевірку цілісності даних або можливість зламу шифрування, що може призвести до витоку конфіденційних даних або несанкціонованого доступу до пристрою.
- Недостатня перевірка даних вводу: Деякі програми, розроблені для мікроконтролерів PIC, можуть мати уразливості, пов'язані з недостатньою перевіркою даних вводу. Це може відкривати можливості для атак типу "впровадження зловмисного коду", "переповнення буфера" або "використання збитків", що дозволяють зловмисникам виконувати власний код на пристрої та впливати на його функціональність.

Ці вразливості можуть становити серйозну загрозу безпеці мікроконтролерів PIC та пристроїв, що використовують ці мікроконтролери. З метою забезпечення належного рівня безпеки, розробники повинні приділяти увагу ретельному тестуванню, використанню захищених протоколів, вдосконаленню управління пам'яттю та впровадженню механізмів перевірки даних вводу. Також важливо систематично оновлювати програмне забезпечення для виправлення виявлених вразливостей та забезпечення найновіших заходів безпеки.

3.5. Аналіз найпоширеніших вразливостей на платформі Nordic nRF52

В ході аналізу платформи Nordic nRF52 було виявлено наступні вразливості:

- Вразливості Bluetooth: Мікроконтролери Nordic nRF52 підтримують бездротовий протокол Bluetooth, і деякі версії можуть мати вразливості, що дозволяють зловмисникам перехоплювати або навіть контролювати з'єднання Bluetooth з пристроями. Це може призвести до несанкціонованого доступу до носимих пристроїв або їх функціональності, а також до витоку конфіденційних даних.
- Вразливості зворотного зв'язку: Nordic nRF52 може мати уразливості, пов'язані з недостатнім забезпеченням захисту зворотного зв'язку. Це може відкривати можливості для атак типу "впровадження зловмисного коду", "переповнення буфера" або "використання збитків", що дозволяють зловмисникам впливати на пристрої та порушувати їх безпеку.
- Вразливості шифрування та безпеки даних: Nordic nRF52 може мати вразливості, пов'язані з шифруванням та безпекою даних. Це може включати недостатній рівень шифрування, недостатню перевірку цілісності даних або можливість зламу шифрування, що призводить до витоку конфіденційних даних або несанкціонованого доступу до пристроїв.
- Вразливості мережевого стеку: Nordic nRF52 включає в себе мережевий стек, такий як Bluetooth Low Energy (BLE) або Zigbee. Деякі версії стеку можуть мати вразливості, що дозволяють зловмисникам здійснювати атаки на мережевий протокол або перехоплювати комунікацію. Це може призвести до

несанкціонованого доступу до пристроїв, втрати конфіденційності даних або порушення приватності користувачів.

- Вразливості фізичної безпеки: Nordic nRF52 може мати вразливості, пов'язані з фізичною безпекою, такі як недостатній захист від фізичного доступу до мікроконтролера або можливість неправильного використання входів-виходів пристрою. Це може дозволити зловмисникам здійснювати атаки, такі як викрадення апаратного забезпечення, зміна налаштувань або навіть отримання конфіденційної інформації.

Враховуючи ці вразливості, важливо, щоб розробники мікроконтролерів Nordic nRF52 докладали особливу увагу до безпеки та проводили ретельну перевірку та тестування пристроїв перед їх використанням. Регулярне оновлення програмного забезпечення та впровадження заходів безпеки є також критичними для забезпечення належного рівня безпеки мікроконтролерів Nordic nRF52 та пристроїв, що на них ґрунтуються.

3.6. Аналіз вразливостей, що стосуються зберігання та передачі даних

Було проаналізовано вразливості, пов'язані з зберіганням та передачею даних, для кожного з наведених мікроконтролерів:

1. ESP32:
   - Недостатня захищеність збережених даних: ESP32 має різні методи зберігання даних, такі як EEPROM, SPIFFS та внутрішня пам'ять. Однак, недостатній рівень шифрування або відсутність механізмів контролю доступу можуть призвести до витоку конфіденційної інформації, такої як паролі, ключі або особисті дані користувача.
   - Несанкціонований доступ до передачі даних: ESP32 підтримує протоколи передачі даних, такі як Wi-Fi та Bluetooth. Неправильна

конфігурація цих протоколів може призвести до несанкціонованого доступу до переданих даних та порушення їх конфіденційності.

2. AVR:
   - Недостатня захищеність пам'яті: AVR-мікроконтролери мають обмежену внутрішню пам'ять, і використання ненадійних методів зберігання даних, таких як відсутність шифрування або недостатній рівень контролю доступу, може призвести до витоку конфіденційної інформації.
   - Недостатня захищеність передачі даних: AVR-мікроконтролери можуть використовувати різні протоколи для передачі даних, такі як UART або SPI. Неправильна конфігурація цих протоколів може призвести до перехоплення або модифікації переданих даних.
3. STM32:
   - Вразливості програмного забезпечення: STM32-мікроконтролери використовують різні програмні стеки та бібліотеки, які можуть мати вразливості безпеки. Недостатня обробка вхідних даних або виконання ненадійного коду може призвести до збоїв системи або витоку конфіденційної інформації.
   - Незахищена передача даних: STM32-мікроконтролери підтримують різні протоколи комунікації, такі як UART, SPI, I2C та Ethernet. Недостатній рівень шифрування або неналежна автентифікація можуть призвести до перехоплення або модифікації переданих даних.
4. PIC:
   - Недостатня захищеність EEPROM: Деякі PIC-мікроконтролери мають EEPROM для зберігання даних. Однак, недостатній рівень шифрування або відсутність механізмів контролю доступу можуть призвести до витоку конфіденційної інформації.
   - Незахищена передача даних: PIC-мікроконтролери можуть використовувати різні протоколи комунікації, такі як UART, SPI або I2C.

Неправильна конфігурація цих протоколів може призвести до перехоплення або модифікації переданих даних.

5. Nordic nRF52:
   - Вразливості BLE-протоколу: Nordic nRF52 мікроконтролери підтримують Bluetooth Low Energy (BLE), який має свої вразливості. Некоректна обробка BLE-запитів або недостатнє шифрування можуть призвести до зловживання атаками на конфіденційні дані.
   - Незахищена передача даних: Nordic nRF52 підтримує різні протоколи передачі даних, такі як UART, SPI та I2C. Недостатній рівень шифрування або неправильна конфігурація цих протоколів можуть призвести до перехоплення або модифікації переданих даних.

Загальна рекомендація щодо запобігання вразливостей полягає у використанні надійних джерел коду, перевірці програмного забезпечення на вразливості, застосуванні шифрування та контролі доступу до збережених та переданих даних, а також у використанні актуальних версій прошивки та оновленнях системи при виявленні вразливостей.

3.7. Аналіз можливостей поширення вірусів на платформах

Аналіз можливостей поширення вірусів на мікроконтролерах ESP32, AVR, STM32, PIC і Nordic nRF52 показує, що можливість імплементації вірусів залежить від різних факторів, таких як архітектура, операційна система та застосовані заходи безпеки. Нижче наведений огляд цих мікроконтролерів з точки зору вразливостей і поширення вірусів:

1. ESP32:

- Вразливості в програмному забезпеченні: Неправильна обробка вхідних даних, вразливості пам'яті та інші програмні помилки можуть призвести до імплементації вірусів на ESP32. Недостатня аутентифікація і авторизація можуть також забезпечити можливість поширення шкідливого коду.

- Вразливості мережевого стеку: Недостатній рівень безпеки Wi-Fi, Bluetooth або інших мережевих протоколів, використаних на ESP32, може призвести до поширення вірусів через мережу або зараження підключених пристроїв.

2. AVR:

- Обмежена потужність: Мікроконтролери AVR мають обмежені ресурси і можливості, що робить їх менш вразливими до поширення вірусів порівняно з більш потужними платформами. Однак, вразливості в програмному забезпеченні та можливості шкідливого коду все ж можуть існувати.

3. STM32:

- Вразливості програмного забезпечення: Неправильна обробка даних, баги в програмному забезпеченні або недостатні заходи безпеки можуть створювати можливість поширення вірусів на STM32. Вразливості, пов'язані з протоколами комунікації та мережевим стеком, також можуть бути використані для поширення шкідливого коду.

4. PIC:

- Обмежена можливість вибору опцій безпеки: Деякі мікроконтролери PIC можуть мати обмежені функції безпеки, що можуть зробити їх вразливими до впровадження вірусів. Недостатня аутентифікація, шифрування або захист пам'яті можуть дозволити поширення шкідливого коду на пристроях PIC.

5. Nordic nRF52:

- Вразливості в мережевому стеку: Nordic nRF52 підтримує бездротові протоколи, такі як Bluetooth і Zigbee. Вразливості в реалізації цих протоколів можуть призвести до поширення вірусів через бездротові з'єднання та інфікування підключених пристроїв.

Важливо зазначити, що виявлення і використання вразливостей залежить від знань та намірів зловмисника, а також від заходів безпеки, прийнятих

розробниками та виробниками мікроконтролерів. Регулярне оновлення прошивки та застосування найкращих практик забезпечення можуть допомогти у запобіганні поширенню вірусів і захисті від вразливостей.

Висновки до розділу

Разом із зростанням популярності носимих пристроїв, з'являються й нові виклики щодо їхньої безпеки. Як і будь-які інші підключені пристрої, носимі пристрої можуть бути вразливими до різних видів атак, що може ставити під загрозу як конфіденційні дані користувача, так і його фізичний добробут.

Усі перераховані платформи мають різні методи зберігання даних, такі як внутрішня пам'ять, флеш-пам'ять, EEPROM тощо. Однак, важливою вразливістю є недостатня захищеність збережених даних. Недостатній рівень шифрування, незахищений доступ або помилки в програмному забезпеченні можуть призвести до витоку конфіденційної інформації.

Кожна з розглянутих платформ підтримує різні протоколи передачі даних, такі як Wi-Fi, Bluetooth, серійний порт тощо. Протоколи безпеки, такі як шифрування, аутентифікація та авторизація, грають важливу роль у запобіганні перехопленню або модифікації переданих даних. Несанкціонований доступ до бездротових мереж або вразливості в мережевих стеках можуть спричинити порушення конфіденційності та цілісності даних.

Загроза поширення вірусів на мікроконтролерах існує на всіх розглянутих платформах. Вразливості в програмному забезпеченні, недостатній контроль доступу, помилки у вхідних даних або протоколах комунікації можуть бути використані для інфікування пристроїв. Однак, потужність обмеження ресурсів на деяких мікроконтролерах може ускладнити розповсюдження вірусів порівняно з більш потужними платформами.

РОЗДІЛ 4. Дослідження програмних та технічних засобів, придатних для подолання відомих вразливостей досліджених платформ

4.1. Виявлення та виправлення вразливостей

Виявлення та виправлення вразливостей є критичним аспектом забезпечення безпеки усіх платформ, на яких базуються носимі пристрої. Цей процес включає ідентифікацію можливих вразливостей у програмному забезпеченні та розробку відповідних заходів для їх усунення.

Для виявлення вразливостей існують різні програмні рішення, які пропонують автоматизовані засоби сканування та аналізу програмного забезпечення. Ці засоби можуть перевіряти код на наявність вразливих місць, виявляти підозрілі дії або потенційні джерела атак. Вони використовують різні методи, такі як статичний аналіз коду, динамічний аналіз під час виконання та аналіз протоколів зв'язку.

Після виявлення вразливостей необхідно розробити та впровадити відповідні заходи для їх виправлення. Це може включати в себе патчі, оновлення програмного забезпечення, зміни в налаштуваннях безпеки або переробку коду. Важливо визначити пріоритетність вразливостей, оцінити можливі наслідки та ризики, а також виробити ефективні стратегії для їх виправлення.

Окрім автоматизованих засобів, також необхідно проводити регулярний аудит безпеки для виявлення вразливостей, які можуть бути пропущені автоматичними методами. Це може включати ручний аналіз коду, перевірку конфігураційних файлів та перевірку відповідності безпекових стандартів.

При виявленні та виправленні вразливостей необхідно забезпечити постійний моніторинг безпеки, оновлювати програмне забезпечення та застосовувати патчі, що виправляють відомі вразливості. Важливо пам'ятати, що безпека є постійним процесом, і необхідно вдосконалювати заходи безпеки залежно від змін у загрозах та вразливостях.

У процесі аналізу було виявлено декілька програмних рішень, які можуть бути використані для виявлення та виправлення вразливостей досліджених платформ. Ці рішення допомагають ідентифікувати потенційні проблеми безпеки та надають рекомендації щодо виправлення. Деякі з розглянутих програмних засобів включають:

- OpenVAS: Це інструмент відкритого коду для сканування вразливостей та аналізу безпеки мереж та систем. OpenVAS надає можливість активно сканувати пристрої та виявляти наявність вразливостей, що допомагає розробникам своєчасно реагувати на потенційні проблеми безпеки[31].
- Nessus: Це комерційний продукт, який надає широкий спектр функціональності для виявлення вразливостей, ідентифікації загроз та перевірки безпеки систем. Nessus дозволяє проводити глибоке сканування пристроїв та аналізувати знайдені вразливості[12].
- Cppcheck: Це безкоштовний інструмент статичного аналізу коду C/C++, який може допомогти виявити потенційні помилки, вразливості та недоліки в програмному забезпеченні [17].
- Coverity: Цей комерційний інструмент статичного аналізу може виявити вразливості, помилки та потенційні проблеми безпеки в коді програмного забезпечення [16].
- Polyspace: Це інструмент статичного аналізу, який використовує принципи формального верифікування для виявлення помилок, включаючи вразливості безпеки, вбудовані в код програмного забезпечення [37].
- Програми розробників мікроконтролерів: Багато виробників мікроконтролерів, таких як Microchip (для PIC), STMicroelectronics (для STM32) та Nordic Semiconductor (для Nordic nRF52), надають власні набори програмних засобів, включаючи компілятори, відлагоджувачі та аналізатори коду, які можуть виявляти певні вразливості та допомагати в їх виправленні.

- Мережеві інструменти безпеки: Для виявлення вразливостей, пов'язаних з передачею даних, можна використовувати мережеві інструменти безпеки, такі як Wireshark або Burp Suite. Вони дозволяють перехоплювати та аналізувати мережевий трафік, виявляти можливі вразливості в протоколах та зв'язку.

Ці інструменти можуть бути використані для виявлення вразливостей та виправлення помилок у програмному забезпеченні для платформ AVR, STM32, PIC, Nordic nRF52. Проте важливо пам'ятати, що жоден інструмент не є повністю вичерпним і не може гарантувати повну безпеку. Регулярний аудит безпеки, розробка безпечного коду та застосування найкращих практик безпеки є необхідними для забезпечення належного рівня безпеки на носимих пристроях.

4.2. Створення бекапів даних

Забезпечення безпеки даних є одним із найважливіших аспектів розробки та використання носимих пристроїв. Важливо мати надійну стратегію резервного копіювання або бекапів для збереження цінної інформації та забезпечення можливості відновлення даних у разі втрати або пошкодження.

Для створення бекапів даних на досліджуваних платформах існує кілька програмних рішень. Одним із найпоширеніших підходів є зберігання даних на зовнішніх носіях, таких як SD-карти або флеш-пам'ять. Це дозволяє зробити копію важливих даних і зберегти їх у безпечному місці, окрім основної пам'яті пристрою.

Крім зберігання на зовнішніх носіях, можливо використовувати хмарні сервіси для резервного копіювання даних. Це дозволяє автоматично синхронізувати дані з носимого пристрою на хмарний сервер, забезпечуючи доступ до них з будь-якого пристрою з підключенням до Інтернету. Хмарні сервіси також забезпечують додатковий рівень безпеки шляхом шифрування та зберігання даних на надійних серверах[20].

Під час розгляду програмних рішень для бекапів даних варто враховувати такі аспекти, як автоматичність процесу, можливість планування резервного копіювання, захист даних шляхом шифрування, можливість відновлення даних з резервних копій та легкість використання. Важливо підібрати рішення, яке відповідає конкретним потребам безпеки та зручності використання для даного носимого пристрою.

Бекапи даних є необхідною складовою для забезпечення безпеки носимих пристроїв. Регулярне створення резервних копій дозволяє зберегти важливі дані та забезпечити їх можливе відновлення у разі втрати чи пошкодження. Обраний метод бекапів повинен бути надійним, зручним у використанні та відповідати конкретним потребам безпеки даного носимого пристрою.

Декілька програмних рішень, які можуть бути використані для створення бекапів даних, включають:

- ESP32 Data Logging: Ця бібліотека розроблена спеціально для платформи ESP32 та дозволяє зберігати дані на внутрішньому флеш-накопичувачі або зовнішніх носіях даних. Вона дозволяє зберігати дані в реальному часі та створювати бекапи для забезпечення безпеки даних [21].
- Arduino: На платформі Arduino існує багато бібліотек та інструментів, що дозволяють здійснювати збереження даних та створення резервних копій. Наприклад, SD бібліотека дозволяє взаємодіяти з SD-картами для збереження даних. Також існують бібліотеки, які дозволяють взаємодіяти з хмарними сервісами, наприклад, бібліотека ArduinoCloud для роботи з Arduino IoT Cloud [7].
- STM32: Для платформи STM32 можна використовувати різні бібліотеки та інструменти. Наприклад, HAL (Hardware Abstraction Layer) бібліотека містить функції для роботи з різними пристроями, включаючи зовнішні носії даних. Також можна використовувати спеціалізовані бібліотеки, які дозволяють працювати з SD-картами, флеш-пам'яттю тощо [42].

- PIC: Для мікроконтролерів PIC також існують бібліотеки та інструменти для забезпечення безпеки даних. Наприклад, PICkit включає в себе різні інструменти, в тому числі PICkit Serial Analyzer, який дозволяє аналізувати та відлагоджувати передачу даних через UART-інтерфейс. Також можна використовувати бібліотеки для роботи з зовнішніми носіями даних, які підтримуються на платформі PIC [36].
- Nordic nRF52: Для мікроконтролерів Nordic nRF52 можна використовувати бібліотеки, такі як nRF5 SDK, які надають засоби для роботи з різними пристроями та зовнішніми носіями даних. Зокрема, SDK містить функції для роботи з флеш-пам'яттю та SD-картами [34].

Варто зазначити, що конкретний вибір програмного рішення для створення резервних копій даних залежить від конкретних вимог та можливостей платформи, а також від вимог безпеки та зручності використання. Рекомендується ознайомитись з документацією, прикладами та специфікаціями зазначених програмних рішень для кожної платформи, щоб зробити найбільш відповідний вибір.

4.3. Оновлення безпеки та видалення шкідливих програм

Оновлення безпеки є важливою складовою для забезпечення безпеки носимих пристроїв, оскільки розробники постійно виявляють нові вразливості та випускають виправлення для своїх платформ. Оновлення безпеки можуть містити виправлення програмних помилок, заповнення потенційних вразливостей та вдосконалення заходів безпеки.

Для оновлення безпеки платформ ESP32 та Arduino існує кілька способів. Один з них - це оновлення прошивки пристрою. Виробники платформ надають оновлення прошивки, які можна завантажити та встановити на носимий пристрій. Ці оновлення можуть містити нові функції, виправлення безпеки та покращення продуктивності. Важливо

періодично перевіряти наявність оновлень та встановлювати їх для забезпечення актуальності заходів безпеки.

Крім оновлення прошивки, також можливе встановлення програмних патчів або виправлень безпеки, які розробляються спеціально для виявлених вразливостей. Ці патчі можуть бути надані виробником платформи або спільнотою розробників. Встановлення таких патчів дозволяє заповнити вразливості та забезпечити більш високий рівень безпеки носимого пристрою.

Окрім оновлення безпеки, важливо також мати засоби для виявлення та видалення шкідливих програм на носимих пристроях. Шкідливі програми можуть бути встановлені непередбачено або поширюватися через інтернетові джерела, такі як недовірені додатки чи пошкоджені файли. Програмні рішення для виявлення та видалення шкідливих програм допомагають сканувати систему пристрою, виявляти потенційно небезпечні файли та програми, інформувати користувача про можливі загрози та надавати можливість їх видалення.

Також важливі такі аспекти, як наявність автоматичного оновлення безпеки, можливість встановлення патчів та виправлень, зручність використання та ефективність виявлення та видалення шкідливих програм.

Декілька програмних рішень, які можуть бути використані для цих цілей, включають:

- ArduinoOTA: Це бібліотека Arduino, яка дозволяє оновлювати програмне забезпечення Arduino через мережу безпосередньо з Arduino IDE. Вона надає зручний спосіб встановлення оновлень безпеки на платформі Arduino [8].
- ESP-IDF (ESP32 IoT Development Framework), який є офіційним комплектом розробки програмного забезпечення (SDK) для ESP32, надається ESP-IDF. Він містить бібліотеки, приклади та інструменти для полегшення розробки та програмування програм на основі

ESP32 [54]. Він має вбудовану систему оновлення (OTA - Over-the-Air), яка дозволяє оновлювати прошивку безпосередньо на пристрої через Wi-Fi або інші мережеві з'єднання. Це дозволяє встановлювати оновлення безпеки та виправлення безпекових помилок [19].

- STM32Cube (STM32): STM32Cube - це набір інструментів та бібліотек для розробки на мікроконтролерах STM32. Він містить систему оновлення (OTA) - STM32CubeProgrammer, яка дозволяє оновлювати прошивку через різні інтерфейси, такі як USB, UART або CAN. Це дозволяє встановлювати оновлення безпеки та виправлення безпекових помилок на платформі STM32 [43].
- MPLAB X (PIC): MPLAB X - це інтегроване середовище розробки для мікроконтролерів PIC. Воно має функціональність для програмування та оновлення прошивки PIC-пристроїв. Виробник мікроконтролерів Microchip також надає оновлення прошивки та патчі для виправлення безпекових помилок на своєму веб-сайті [30].
- nRF Connect (Nordic nRF52): nRF Connect - це набір інструментів, який включає в себе серію програм для розробки та тестування пристроїв на базі мікроконтролерів Nordic nRF52. Він має функцію надання оновлень прошивки через Bluetooth Low Energy (BLE) з використанням DFU (Device Firmware Update) і може використовуватися для оновлення безпеки та виправлення помилок на платформі Nordic nRF52 [33].
- Зовнішні програмні рішення: Також можна використовувати сторонні програмні рішення, такі як Mender, Resin.io, Particle.io та інші, які спеціалізуються на оновленні безпеки та управлінні вбудованими системами. Ці рішення надають функціональність для оновлення прошивки через мережу, керування версіями, виявлення і виправлення помилок безпеки тощо.

Вибір конкретного програмного рішення залежить від специфічних вимог вашого проекту та платформи, на якій ви розробляєте. Рекомендується ознайомитись з документацією та прикладами для кожного рішення, щоб зрозуміти, яке найкраще відповідає вашим потребам безпеки та зручності використання.

4.4. Методи аутентифікації

Методи аутентифікації виконують важливу роль у забезпеченні безпеки будь-яких платформ. У цьому пункті здійснюється аналіз різних методів аутентифікації, зокрема їх переваг, недоліків та прикладів використання на платформах ESP32, AVR, STM32, PIC та Nordic nRF52.

1. Використання паролів: Цей метод є одним з найпоширеніших і включає в себе використання парольної аутентифікації. На платформах можна реалізувати механізми введення паролів за допомогою клавіатури або інших вхідних пристроїв. Для зберігання та порівняння паролів можна використовувати EEPROM пам'ять. Проте важливо враховувати рекомендації щодо безпеки паролів, такі як складність, довжина та застосування механізмів хешування для збереження паролів у безпечному вигляді.
   - На платформі ESP32 та AVR можна використовувати бібліотеку Arduino Password, яка надає функціональність для створення та перевірки паролів на основі введення користувача.
   - Для платформи STM32 можна використовувати бібліотеку STM32Cube супроводжувану мікроконтролерами STM32. Вона надає функціональність для роботи з EEPROM та збереження паролів [43].
   - Для платформи PIC можна використовувати бібліотеку Microchip Libraries for Applications (MLA), яка містить різноманітні функції для роботи з пам'яттю та реалізації парольної аутентифікації [29].

- На платформі Nordic nRF52 можна використовувати Nordic SDK, який надає інструменти та функції для зберігання та перевірки паролів.

2. Біометричні дані: У носимих пристроях, побудованих на більшості платформ, можна використовувати біометричні дані для аутентифікації користувача, наприклад, за допомогою відбитка пальця. Також можна використовувати модулі для розпізнавання обличчя, які дозволяють встановлювати ідентичність користувача на основі фізичних рис обличчя [39].
   - Для платформи ESP32 можна використовувати бібліотеку ESP32 Biometrics, яка надає можливість роботи з датчиками відбитків пальців для аутентифікації користувача.
   - На платформі AVR можна використовувати сторонні бібліотеки, які підтримують біометричні датчики, наприклад, бібліотеку Adafruit Fingerprint Sensor для роботи з датчиками відбитків пальців.
   - Для платформи STM32 можна використовувати бібліотеку STM32CubeAI, яка містить інструменти для розпізнавання обличчя та інших типів біометричних даних.
   - На платформі PIC можна використовувати сторонні бібліотеки, які підтримують біометричні датчики, наприклад, Neurotechnology SDK для відбитків пальців.

3. Двофакторна аутентифікація: Цей метод використовує два або більше фактори аутентифікації для забезпечення вищого рівня безпеки. На платформах можна реалізувати двофакторну аутентифікацію за допомогою комбінації пароля та іншого фактору, такого як одноразовий код, отриманий через SMS або електронну пошту.

   - Для реалізації двофакторної аутентифікації на платформі ESP32 можна використовувати бібліотеку ESP32 OTP, яка дозволяє генерувати одноразові паролі та використовувати їх як другий фактор аутентифікації [23].

- На платформі AVR можна використовувати сторонні бібліотеки для генерації одноразових паролів або використовувати комунікаційні модулі для отримання одноразових кодів через SMS або електронну пошту. Наприклад, бібліотеку Arduino TOTP [9].
- На платформі PIC можна використовувати сторонні бібліотеки для генерації одноразових паролів або комунікаційні модулі для отримання одноразових кодів.

Кожен з цих методів має свої переваги та недоліки, і їх вибір залежить від конкретних потреб та вимог безпеки для носимих пристроїв на базі різних платформ. Важливо забезпечити достатню складність та надійність механізмів аутентифікації, а також регулярно оновлювати паролі та застосовувати рекомендації щодо безпеки для збереження біометричних даних [38].

4.5. Захист від шкідливих програм

В цьому пункті проводиться аналіз різних програмних рішень, які допомагають підвищити безпеку досліджуваних платформ шляхом виявлення та блокування шкідливих програм. Основний акцент робиться на антивірусах та антишпигунах.

1. Антивіруси: Для захисту від шкідливих програм можна використовувати антивірусне програмне забезпечення, яке виявляє, блокує та видаляє віруси, трояни та інші шкідливі програми. На платформах ESP32 та AVR доступні деякі легкі антивірусні бібліотеки, такі як ESP32 Antivirus Suite, які надають базовий рівень захисту. Наприклад, можна періодично сканувати пам'ять пристрою на наявність вірусів та специфічних шаблонів шкідливих програм [24].
2. Антишпигуни: Для запобігання небажаним перехопленням даних та збереженню конфіденційності користувача можна використовувати антишпигунське програмне забезпечення. На платформах ESP32 та AVR

можна використовувати бібліотеки, які аналізують мережевий трафік та виявляють небажані спроби перехоплення даних або несанкціонованого доступу до пристрою.

Крім програмного захисту від шкідливих програм, також розглядаються механізми контролю доступу та обмежень, що дозволяють запобігати виконанню небезпечних дій шкідливими програмами:

- Права доступу: На платформах можна використовувати механізми прав доступу, щоб обмежити можливості шкідливих програм. Наприклад, можна використовувати принцип найменших привілеїв, де шкідлива програма має обмежений доступ до ресурсів та функцій пристрою [5].
- Перевірка цілісності: Важливим аспектом безпеки є забезпечення цілісності даних, тобто виявлення несанкціонованих змін в даних. Для запобігання внесенню змін шкідливими програмами можна використовувати методи перевірки цілісності програм та даних на пристрої. Наприклад, можна використовувати хеш-функції, які генерують унікальний хеш-код для кожного набору даних, для перевірки цілісності програмного забезпечення та виявлення можливих модифікацій. Якщо дані були змінені, хеш-код також зміниться [27].

  На платформах доступні різні бібліотеки для обчислення хеш-функцій, наприклад, бібліотека ArduinoHash [6].
- Санкціонований доступ: Налаштування санкціонованого доступу до ресурсів пристрою може допомогти обмежити можливості шкідливих програм. Це можна досягти за допомогою розумного керування привілеями та ролевою базовою системою.

Вивчення різних програмних та технічних рішень для захисту від шкідливих програм на платформах дозволяє забезпечити вищий рівень безпеки для носимих пристроїв та їх користувачів. Комбінація антивірусних програм, антишпигунського програмного забезпечення та механізмів контролю доступу

дозволяє виявляти, блокувати та запобігати діям шкідливих програм, зберігаючи конфіденційність та безпеку пристрою.

4.6. Захист від крадіжки даних

Захист конфіденційних даних є важливим аспектом безпеки на платформах ESP32 та Arduino. В цьому пункті проводиться дослідження різних методів шифрування та розглядаються рішення для захисту комунікації між носимими пристроями та зовнішніми пристроями з метою запобігання перехопленню та зламу інформації.

1. Методи шифрування: Використання методів шифрування дозволяє захистити конфіденційні дані, що зберігаються на платформах ESP32 та Arduino. Наприклад, можна використовувати алгоритми шифрування, такі як Advanced Encryption Standard (AES), для захисту даних. Прикладом може бути шифрування файлів з використанням AES-256 бібліотекою, такою як "AESLib" [4].
   - На платформі ESP32 та AVR можна використовувати бібліотеку Arduino Crypto для реалізації різних алгоритмів шифрування, включаючи AES, DES, RSA та інші [18].
   - На платформах STM32, PIC та Nordic nRF52 також є доступні криптографічні бібліотеки, які підтримують різні алгоритми шифрування та хешування, такі як AES, RSA, SHA, MD5 та інші.
2. Захист комунікації: Для запобігання перехопленню та зламу інформації під час комунікації між носимими пристроями та зовнішніми пристроями можна використовувати протоколи шифрування та аутентифікації. Наприклад, можна використовувати протоколи SSL/TLS для захищеної передачі даних через мережу.

- На платформі ESP32 можна використовувати бібліотеку ESPAsyncWebServer для створення захищених веб-серверів з підтримкою SSL/TLS [22].
- Для безпечної передачі даних через мережу на інших платформах можна використовувати бібліотеки, які підтримують SSL/TLS, наприклад, mbed TLS (раніше PolarSSL) для STM32 [28].

3. Криптографічні ключі: Криптографічні ключі відіграють важливу роль у захисті даних. Для забезпечення безпеки можна використовувати криптографічно стійкі випадкові ключі та забезпечити їх безпечне зберігання на пристрої.
4. Захист пам'яті: Важливим аспектом захисту даних є захист пам'яті пристрою від несанкціонованого доступу. На платформах ESP32 та AVR можна використовувати механізми захисту пам'яті, такі як використання фізичних адрес та контроль доступу до пам'яті, щоб запобігти несанкціонованій зміні або читанню даних.

Ці рішення можуть бути реалізовані за допомогою наявних криптографічних бібліотек та інструментів для відповідних платформ. Варто також враховувати обмеження ресурсів платформи та вимоги щодо швидкості та продуктивності при виборі відповідних рішень.

Дослідження різних методів шифрування та захисту комунікації досліджених платформах дозволяє забезпечити високий рівень безпеки для носимих пристроїв та захистити конфіденційні дані від крадіжки та несанкціонованого доступу.

4.7. Захист апаратної частини пристрою

Захист апаратної частини пристрою є ще одним важливим аспектом забезпечення безпеки носимих пристроїв на платформах ESP32, AVR, STM32, PIC і Nordic nRF52. Для досягнення цього заходу безпеки можна використовувати наступні технічні рішення:

1. Спеціальні модулі безпеки:
    - Криптографічні прискорювачі: Деякі платформи, такі як STM32 або Nordic nRF52, можуть мати вбудовані апаратні криптографічні прискорювачі. Ці прискорювачі забезпечують апаратну підтримку різних алгоритмів шифрування і підпису, що полегшує реалізацію безпеки в програмному забезпеченні.
    - Модулі безпеки TPM: Trusted Platform Module (TPM) - це апаратний модуль безпеки, який забезпечує криптографічні функції, включаючи генерацію ключів, шифрування та підписи. Використання TPM може забезпечити апаратний захист ключів і конфіденційних даних на платформі.
2. Фізичні механізми захисту:
    - Фізичне замикання доступу: Деякі платформи можуть мати фізичні механізми захисту, такі як фізичне замикання доступу до компонентів пристрою. Це може включати механізми блокування або фізичного запечатування корпусу, що ускладнює несанкціонований доступ до внутрішніх компонентів.
    - Захищені корпуси: Деякі платформи можуть використовувати спеціально розроблені корпуси, що мають покращені фізичні характеристики, такі як міцні матеріали або вбудовані механізми виявлення несанкціонованого доступу.

Застосування таких захисних методів може залежати від конкретних можливостей кожної платформи. Необхідність використання додаткових модулів або компонентів для забезпечення апаратного захисту може бути визначена характеристиками платформи і вимогами до безпеки [48].

Дослідження та використання різних технічних рішень для підвищення безпеки на платформах допомагають забезпечити захист носимих пристроїв від вразливостей та зловмисного використання, зберегти конфіденційність

даних користувача та забезпечити безпечну комунікацію з іншими пристроями.

Висновки до розділу

У цьому розділі було проведено дослідження програмних та технічних засобів, які можуть допомогти підвищити безпеку платформ, на яких базуються носимі пристрої бюджетного сегменту.

В ході роботи були розглянуті такі аспекти безпеки, як аутентифікація, захист від шкідливих програм, захист від крадіжки даних, виявлення та виправлення вразливостей, створення бекапів даних, оновлення безпеки, видалення шкідливих програм та захист апаратної частини пристрою.

Отже, використання відповідних програмних засобів дозволяє підвищити безпеку носимих пристроїв на базі досліджених платформ. Продумана стратегія виявлення та виправлення вразливостей, створення бекапів даних, оновлення безпеки та виявлення шкідливих програм допоможе забезпечити надійну та безпечну роботу носимих пристроїв для користувачів. Для досягнення максимального рівня безпеки рекомендується постійно вдосконалювати та оновлювати програмні засоби, слідкувати за випуском нових версій програмного забезпечення та виконувати рекомендації виробників щодо безпеки.

Результати дослідження свідчать про наявність різноманітних програмних та технічних засобів, які можуть бути використані для подолання відомих вразливостей на платформах, на яких базуються носимі пристрої. Розробка та застосування цих засобів можуть сприяти підвищенню безпеки носимих пристроїв та забезпеченню захисту конфіденційної інформації користувачів.

РОЗДІЛ 5. Економічне обґрунтування застосування носимих розумних речей та мереж в питаннях безпеки та виробничих ризиків

В даному розділі наведено економічне обґрунтування дослідження з теми «Аналіз ризиків та переваг носимих розумних речей та мереж в питаннях безпеки та виробничих ризиків».

Вступ

У сучасному світі, де конкуренція на ринку зростає з кожним днем, підприємствам доводиться постійно шукати нові шляхи для підвищення ефективності та зниження витрат. Швидкі технологічні зміни ставлять перед бізнесом виклик — необхідність адаптуватися до нових умов і забезпечувати продуктивність на високому рівні. В цьому контексті, впровадження носимих розумних пристроїв в робочому середовищі виявляється одним із інноваційних рішень, яке привертає увагу економістів та підприємців.

Носимі розумні пристрої, такі як розумні годинники, фітнес-браслети, окуляри, здатні забезпечити сполучення між реальним та віртуальним світом, використовуючи сучасні технології. Їх можна використовувати для відстеження фізичних параметрів, контролю здоров'я, спостереження за робочим процесом, отримання повідомлень та нагадувань, а також для доступу до інформації зі сторонніх джерел.

Впровадження носимих розумних пристроїв в робочому середовищі відкриває широкі перспективи для покращення ефективності та оптимізації бізнес-процесів. Наприклад, працівникам, які мають доступ до розумних годинників або фітнес-браслетів, можна надати можливість відстежувати свою фізичну активність та рівень стресу, що дозволить підвищити їх робочу продуктивність та знизити ризик виникнення проблем зі здоров'ям. Крім того, використання носимих розумних пристроїв може допомогти в управлінні

ресурсами, покращенні комунікації та спільної роботи між співробітниками, а також забезпечити швидкий доступ до важливої інформації.

Однак, перед впровадженням носимих розумних пристроїв у робочому середовищі необхідно ретельно проаналізувати економічні аспекти. Зокрема, слід врахувати вартість придбання пристроїв, витрати на навчання персоналу, а також можливі витрати на обслуговування та підтримку. Крім того, важливим аспектом є захист конфіденційної інформації та забезпечення безпеки даних, оскільки носимі пристрої можуть збирати та передавати чутливу інформацію.

У світлі цих обставин, варто ретельно зважити на переваги та можливі ризики впровадження носимих розумних пристроїв у робочому середовищі. Це допоможе прийняти обґрунтоване рішення, яке враховуватиме економічну доцільність, технологічні можливості та специфіку бізнесу.

5.1. Економічне обґрунтування результатів аналізу

Економічний аналіз ризиків та переваг застосування носимих розумних речей та мереж в питаннях безпеки та виробничих ризиків є важливим аспектом при визначенні вартості та вигод від використання цих технологій. Нижче розглянуто деякі аргументи, що підкреслюють економічну сторону цього питання.

1. Зменшення виробничих ризиків:

- Моніторинг здоров'я працівників: Використання носимих розумних пристроїв дозволяє в режимі реального часу контролювати фізичний стан працівників. Це може включати виявлення підвищеного рівня стресу, падіння енергії або ознак втоми. За допомогою датчиків, розташованих на носимих пристроях, можна вимірювати показники, такі як пульс, кров'яний тиск, рівень активності тощо. За наявності небажаних змін у цих показниках, система може виявити потенційні проблеми та сповістити працівника або відповідні служби, щоб запобігти негативним наслідкам,

таким як нещасні випадки, втрата продуктивності та зниження якості роботи.

- Виявлення небезпечних умов: Носимі пристрої можуть бути обладнані різними датчиками, які реагують на небезпечні умови в робочому середовищі. Наприклад, датчики можуть виявляти підвищену температуру, високий рівень шуму або наявність шкідливих речовин у повітрі. Якщо датчики виявляють такі умови, система може надати сповіщення працівникам та відповідним службам, щоб оперативно реагувати на потенційно небезпечну ситуацію та запобігти виникненню аварій або професійних захворювань.
- Моніторинг безпеки працівників: За допомогою носимих пристроїв можна забезпечити постійний моніторинг місцезнаходження працівників, а також надати можливість виклику допомоги у разі надзвичайних ситуацій. Наприклад, пристрої можуть мати вбудовані GPS-чіпи або інші технології визначення місцезнаходження, які дозволяють в реальному часі відстежувати розташування працівників на робочій території. У разі надзвичайних ситуацій, таких як травма або загроза безпеці, працівники можуть активувати тривожний сигнал або викликати допомогу, і система негайно повідомить відповідні служби про цю ситуацію, що сприяє підвищенню безпеки працівників і зменшенню ризиків нападів, нещасних випадків або загублених робочих годин.

2. Підвищення продуктивності та ефективності:

- Оптимізація робочих процесів: Використання носимих розумних пристроїв дозволяє автоматизувати рутинні завдання та оптимізувати робочі процеси. Наприклад, носимі пристрої можуть надавати інформацію про час виконання певних завдань, розташування робочих матеріалів або інструментів, а також надавати сповіщення та нагадування про важливі

події або дедлайни. Це допомагає працівникам бути більш організованими і ефективними, що в свою чергу підвищує продуктивність.

- Оптимізація процесів навчання та навчальної документації: Носимі пристрої можуть спрощувати процес навчання нових працівників та поліпшувати доступ до навчальних матеріалів. За допомогою цих пристроїв можна надавати навчальні матеріали та інструкції безпосередньо на робочому місці, що дозволяє працівникам отримувати актуальну інформацію без необхідності переривати роботу. Крім того, носимі пристрої можуть допомагати у зборі даних та автоматизації документаційних процедур, таких як заповнення звітів або контроль якості, що сприяє підвищенню якості документації та забезпечує точність та достовірність даних.

3. Зменшення витрат на охорону праці:

- Економія на обладнанні: Застосування носимих розумних пристроїв може замінити дороге обладнання, що використовується для моніторингу та безпеки працівників. Наприклад, замість великих систем відеоспостереження або дорогих пристроїв моніторингу, можна використовувати носимі пристрої зі вбудованими камерами та сенсорами для виконання багатьох функцій моніторингу та безпеки. Це дозволяє зменшити витрати на придбання та підтримку обладнання.
- Зменшення ризику нещасних випадків та професійних захворювань: Моніторинг фізичного стану працівників за допомогою носимих пристроїв дозволяє виявляти показники, що свідчать про підвищений ризик нещасних випадків або професійних захворювань. Раннє виявлення таких сигналів дозволяє вжити відповідних заходів для запобігання та мінімізації ризиків, що зменшує витрати, пов'язані з лікуванням, відшкодуванням та втратою робочих годин.

4. Покращення взаємодії та комунікації:

- Швидка та зручна комунікація: Завдяки носимим пристроям, працівники можуть легко спілкуватися один з одним у режимі реального часу. Вони можуть обмінюватися повідомленнями, використовувати голосові чи відеодзвінки, надсилати файли та документи, що дозволяє швидко передавати важливу інформацію та отримувати відповіді на запитання без затримок.
- Краща координація робочих процесів: Носимі пристрої дозволяють створювати спеціальні групи та команди, де працівники можуть обмінюватися інформацією та координувати свої дії. Це сприяє покращенню організації та координації робочих процесів, зокрема при виконанні спільних завдань, проектів або вирішенні проблем.
- Зручність під час зустрічей та нарад: Носимі пристрої можуть допомагати працівникам під час зустрічей та нарад. Наприклад, вони можуть надавати доступ до розкладу зустрічей, документів або презентацій, а також функцію записування та передачі протоколів зустрічей. Це спрощує процес організації та участі в зустрічах, забезпечуючи більш ефективну комунікацію та збереження важливої інформації.
- Розширені можливості співпраці: Носимі пристрої можуть підтримувати спільну роботу над проектами та завданнями. Вони можуть надавати доступ до спільних ресурсів, документів та інструментів, що дозволяє працівникам співпрацювати над одними та тими ж завданнями в режимі реального часу. Це сприяє покращенню колективної праці та збільшенню продуктивності команди.

5. Відкритість для інновацій:

- Впровадження нових функцій та сервісів: Носимі пристрої можуть бути використані для впровадження нових функцій та сервісів, які покращують робочі процеси або пропонують нові можливості. Наприклад, це може бути функція відстеження робочого часу, автоматичне розпізнавання об'єктів або виявлення аномалій у виробничих процесах. Такі інноваційні рішення дозволяють підприємствам бути конкурентоспроможними та реагувати на зміни вимог ринку.
- Адаптація до змінних потреб клієнтів: Носимі пристрої та мережі можуть допомогти підприємствам швидко адаптуватися до змінних потреб своїх клієнтів. Вони можуть збирати дані про споживання, поведінку та відгуки клієнтів, що дозволяє підприємствам аналізувати ці дані та впроваджувати нові продукти або послуги, що відповідають потребам ринку.
- Сприяння творчості та інновацій: Носимі пристрої можуть стати платформою для розвитку та сприяння творчості працівників. Вони можуть надавати інструменти для створення та використання інноваційних ідей, наприклад, мобільні додатки для генерації та обміну ідеями, віртуальні середовища для спільного творчого процесу або можливість носити пристрої, які допомагають працівникам працювати з більшою ефективністю та натхненням.

Загалом, економічний аналіз ризиків та переваг застосування носимих розумних речей та мереж підтверджує значні можливості для покращення безпеки, продуктивності та ефективності виробничих процесів. Однак, необхідно уважно розглянути всі аспекти і розробити належні стратегії безпеки та ризик-менеджменту для максимізації переваг і мінімізації негативних наслідків.

Результати цього економічного аналізу підкріплюються висновками основного дослідження, зокрема, такими аспектами, як вплив на безпеку

працівників, відкриття перспектив та можливостей, а також оптимізація робочого процесу.

5.2. Порівняння вартості та економічної доцільності використання підприємствами різних носимих пристроїв

Аналіз ризиків та переваг застосування носимих розумних речей та мереж в питаннях безпеки та виробничих ризиків може включати порівняння вартості та економічної доцільності застосування різних носимих пристроїв на підприємствах. Ось деякі аспекти, які можна врахувати при такому порівнянні:

1. Вартість:
    - Порівнюючи вартість придбання, слід розглянути ціни різних моделей та виробників.
    - Також варто враховувати операційні витрати, які включають заміну акумуляторів, підписки на програмне забезпечення та обслуговування.
    - Тривалість служби пристрою також має значення, оскільки пристрій з більшою тривалістю служби може виправдати високу вартість придбання.
2. Функціональні можливості:
    - Порівнюючи моніторинг фізичних показників, слід звернути увагу на наявність вимірювань, таких як пульс, кров'яний тиск, рівень кисню в крові та рівень активності.
    - Дослідження можливості автоматичного виявлення небезпечних ситуацій, таких як падіння або перевтомленість, також має значення.

- Важливо перевірити наявність можливості віддаленого моніторингу та нагляду, що дозволяє передавати дані в реальному часі для швидкого реагування на небезпечні ситуації.

3. Надійність та безпека:
    - Фізична стійкість пристрою, зокрема до фізичних пошкоджень та вологи, має велике значення, особливо при використанні виробничому середовищі.
    - Захист персональних даних та відповідність стандартам безпеки, наприклад, GDPR, також слід враховувати.
4. Інтеграція та сумісність:
    - Важливо з'ясувати, наскільки легко можна інтегрувати носимі пристрої в існуючу інфраструктуру підприємства.
    - Сумісність з мережами та протоколами, які використовуються в підприємстві, також має значення.
5. Тривалість роботи та енергоспоживання:
    - Тривалість роботи акумуляторів є важливим фактором, оскільки короткий час роботи може вимагати частішого заряджання або заміни.
    - Загальне енергоспоживання пристроїв слід враховувати, оскільки воно може вплинути на тривалість роботи та продуктивність співробітників.
6. Легкість використання та навчання:
    - Інтуїтивно зрозумілий інтерфейс та взаємодія з пристроєм сприяють легкості використання і зменшують час навчання та помилки.
    - Важливо враховувати, наскільки швидко та ефективно можна навчити персонал використовувати пристрої.

Ці аспекти допоможуть провести детальний аналіз ризиків та переваг застосування різних носимих пристроїв та мереж в питаннях безпеки та виробничих ризиків для підприємства. Важливо враховувати специфіку підприємства та його потреб для того, щоб зробити обґрунтований вибір.

Було розглянуто 5 популярних носимих пристроїв за їх функціями, вартістю та економічною доцільністю для впровадження на підприємствах.

1. Apple Watch Series 6:
    - Функції: Apple Watch Series 6 пропонує широкий спектр функцій, включаючи моніторинг здоров'я, фітнес-трекінг, ECG-вимірювання та GPS. Це робить його потужним інструментом для підприємств, які покладають великий акцент на здоров'я та безпеку працівників.
    - Вартість: Apple Watch Series 6 є одним з найвищих за вартістю носимих пристроїв на ринку. Його висока ціна може бути обмежуючим фактором для деяких підприємств, пристрій коштує приблизно від 399 доларів США.
    - Економічна доцільність: Впровадження Apple Watch Series 6 може бути економічно доцільним для підприємств, які активно залучені до здоров'я та безпеки працівників і готові інвестувати в продуктивність та благополуччя персоналу.
2. Samsung Galaxy Watch Active2:
    - Функції: Samsung Galaxy Watch Active2 пропонує розширені функції для фітнесу, моніторингу серцевого ритму, GPS і спортивних трекерів. Він може бути цікавим вибором для підприємств, які акцентують увагу на фітнесі та активному способі життя.
    - Вартість: Вартість Samsung Galaxy Watch Active2 є помірною, що робить його доступним для більш широкого кола підприємств, вартість починається від 249 доларів США.

- Економічна доцільність: Впровадження Samsung Galaxy Watch Active2 може бути економічно доцільним для підприємств, які цінують фітнес-компонент та моніторинг здоров'я своїх співробітників.

3. Fitbit Versa 3:

- Функції: Fitbit Versa 3 пропонує широкі можливості для фітнес-трекінгу, сну, стресу та моніторингу здоров'я. Він може бути вигідним вибором для підприємств, які акцентують увагу на фітнесі та добробуті працівників.
- Вартість: Fitbit Versa 3 має помірну вартість, що робить його доступним для більшості підприємств, вартість починається приблизно від 229 доларів США.
- Економічна доцільність: Впровадження Fitbit Versa 3 може бути економічно доцільним для підприємств, які ставлять собі за мету покращення фітнесу та добробуту своїх співробітників.

4. Garmin Forerunner 945:

- Функції: Garmin Forerunner 945 зосереджений на функціях спортивного трекінгу, GPS, моніторингу здоров'я та навігації. Він може бути корисним для підприємств, пов'язаних з активним способом життя та спортом.
- Вартість: Garmin Forerunner 945 є висококласним носимим пристроєм і має набагато вищу вартість в порівнянні з аналогами, що може бути обмежуючим фактором для деяких підприємств, вартість починається приблизно від 599 доларів США.
- Економічна доцільність: Впровадження Garmin Forerunner 945 може бути економічно доцільним для підприємств, які активно працюють у спортивній галузі та пов'язані зі здоров'ям та фітнесом.

5. Xiaomi Mi Band 6:

    - Функції: Xiaomi Mi Band 6 пропонує базові функції фітнес-трекінгу, сну та пульсометр. Це може бути економічним варіантом для підприємств з обмеженим бюджетом, які потребують базових функцій моніторингу здоров'я.
    - Вартість: Xiaomi Mi Band 6 має низьку вартість, що робить його дуже доступним для багатьох підприємств, вартість починається від приблизно 49 доларів США.
    - Економічна доцільність: Впровадження Xiaomi Mi Band 6 може бути економічно доцільним для підприємств з обмеженим бюджетом, які шукають базові функції моніторингу здоров'я та фітнесу.

Варто пам'ятати, що вплив на безпеку та ризики залежить від специфіки, потреб та бюджету підприємства та конкретних умов роботи. Перед впровадженням носимих пристроїв варто здійснити оцінку ризиків та проконсультуватися з фахівцями з безпеки, щоб забезпечити їх відповідність стандартам та вимогам безпеки на робочому місці.

Нижче наведений порівняльний аналіз носимих пристроїв Apple Watch Series 6, Samsung Galaxy Watch Active2, Fitbit Versa 3, Garmin Forerunner 945 та Xiaomi Mi Band 6 за наступними аспектами:

1. Вартість:

- Apple Watch Series 6: Висока вартість.
- Samsung Galaxy Watch Active2: Помірна вартість.
- Fitbit Versa 3: Помірна вартість.
- Garmin Forerunner 945: Висока вартість.
- Xiaomi Mi Band 6: Низька вартість.

2. Функціональні можливості:

- Apple Watch Series 6: Широкий спектр функцій, включаючи моніторинг здоров'я, фітнес-трекінг, ECG-вимірювання та GPS.
- Samsung Galaxy Watch Active2: Розширені функції для фітнесу, моніторинг серцевого ритму, GPS і спортивні трекери.
- Fitbit Versa 3: Функції фітнесу, моніторинг сну, GPS, сповіщення та підтримка голосового асистента.
- Garmin Forerunner 945: Спеціалізовані функції для бігу, плавання, тренувань, GPS, серцевий ритм та маршрутизація.
- Xiaomi Mi Band 6: Базові функції фітнес-трекера, моніторинг сну, пульсу та трекер кров'яного тиску.

3. Надійність та безпека:

- Apple Watch Series 6: Висока надійність та захист даних.
- Samsung Galaxy Watch Active2: Висока надійність та захист даних.
- Fitbit Versa 3: Висока надійність та захист даних.
- Garmin Forerunner 945: Висока надійність та захист даних.
- Xiaomi Mi Band 6: Помірна надійність та захист даних.

4. Інтеграція та сумісність:

- Apple Watch Series 6: Інтеграція з екосистемою Apple та підтримка додатків сторонніх розробників.
- Samsung Galaxy Watch Active2: Інтеграція зі смартфонами Samsung та підтримка додатків сторонніх розробників.
- Fitbit Versa 3: Інтеграція зі смартфонами Android та підтримка додатків сторонніх розробників.
- Garmin Forerunner 945: Інтеграція зі смартфонами Android та підтримка спортивних додатків.

- Xiaomi Mi Band 6: Інтеграція зі смартфонами Android та деякими додатками сторонніх розробників.

5. Тривалість роботи та енергоспоживання:

- Apple Watch Series 6: Помірна тривалість роботи батареї (до 18 годин).
- Samsung Galaxy Watch Active2: Помірна тривалість роботи батареї (до 2 днів).
- Fitbit Versa 3: Помірна тривалість роботи батареї (до 6 днів).
- Garmin Forerunner 945: Висока тривалість роботи батареї (до 2 тижнів).
- Xiaomi Mi Band 6: Висока тривалість роботи батареї (до 14 днів).

6. Легкість використання та навчання:

- Apple Watch Series 6: Інтуїтивний інтерфейс та легкість використання.
- Samsung Galaxy Watch Active2: Інтуїтивний інтерфейс та легкість використання.
- Fitbit Versa 3: Інтуїтивний інтерфейс та легкість використання.
- Garmin Forerunner 945: Навігаційне меню може бути складним для деяких користувачів.
- Xiaomi Mi Band 6: Інтуїтивний інтерфейс та легкість використання.

В кінцевому підсумку, вибір носимого пристрою для впровадження на підприємстві залежить від конкретних потреб та бюджету компанії. При вагомості функціональності, вартості та економічної доцільності, Apple Watch Series 6 та Samsung Galaxy Watch Active2 можуть бути привабливими варіантами для підприємств, які покладають великий акцент на здоров'я та фітнес працівників. Fitbit Versa 3 і Xiaomi Mi Band 6 можуть бути більш доступними альтернативами з базовими функціями для тих, хто має обмежений бюджет або не потребує розширеного функціоналу. Garmin Forerunner 945 може бути

вигідним вибором для підприємств, пов'язаних з активним способом життя та спортом, але вимагає більш значних інвестицій.

Висновки до розділу

Аналізуючи економічні аспекти використання носимих розумних пристроїв у робочих умовах, можна зробити висновок про потенційну вигоду їх застосування для підприємств. Перш за все, ці пристрої дозволяють підвищити продуктивність працівників шляхом забезпечення доступу до необхідної інформації в режимі реального часу. Це сприяє ефективнішій організації робочих процесів та зниженню часу, витраченого на пошук інформації.

Крім того, носимі розумні пристрої допомагають уникнути деяких витрат. Наприклад, вони можуть замінити дорогі стаціонарні пристрої або інструменти, що знижує витрати на їх придбання та обслуговування. Також, вони сприяють зменшенню витрат на охорону праці, оскільки деякі моделі носимих пристроїв мають функції моніторингу безпеки та запобігання нещасним випадкам.

Зважаючи на перелічені переваги, впровадження носимих розумних пристроїв у робочому середовищі може бути вигідним рішенням для підприємств. Однак, слід також враховувати фактори, пов'язані з конфіденційністю даних та безпекою. Ефективне впровадження цих пристроїв вимагає обережного планування та розробки політики безпеки, щоб забезпечити захист інформації та уникнути можливих ризиків.

В цілому, використання носимих розумних пристроїв у робочому середовищі може мати значний вплив на економічну ефективність підприємств. Залежно від специфіки бізнесу та конкретних умов, впровадження цих пристроїв може бути вигідним рішенням, яке допоможе забезпечити конкурентні переваги та покращити результативність діяльності підприємства.

Було проаналізовано 5 популярних на ринку носимих пристроїв у питаннях вартості та економічної доцільності впровадження їх на підприємствах.

В кінцевому підсумку, вибір носимого пристрою для впровадження на підприємстві залежить від конкретних потреб та бюджету компанії. При вагомості функціональності, вартості та економічної доцільності, Apple Watch Series 6 та Samsung Galaxy Watch Active2 можуть бути привабливими варіантами для підприємств, які покладають великий акцент на здоров'я та фітнес працівників. Fitbit Versa 3 і Xiaomi Mi Band 6 можуть бути більш доступними альтернативами з базовими функціями для тих, хто має обмежений бюджет або не потребує розширеного функціоналу. Garmin Forerunner 945 може бути вигідним вибором для підприємств, пов'язаних з активним способом життя та спортом, але вимагає більш значних інвестицій.

Таким чином, результати економічного аналізу підкріплюють основну гіпотезу дослідження, що носимі пристрої можуть бути успішно використані для покращення умов праці та забезпечення безпеки працівників на робочому місці.

ВИСНОВКИ

У ході дослідження було проведено аналіз різних носимих пристроїв, доступних на ринку, таких як розумні годинники, фітнес-браслети, розумні окуляри та інші. Були розглянуті їх функції та можливості, а також класифікація за походженням та ціновим сегментом.

У процесі аналізу було приділено увагу ризикам та перевагам використання носимих пристроїв у питаннях безпеки та виробничих ризиків. Виявлено, що такі пристрої можуть допомогти виявляти та попереджувати ризики на робочому місці, покращувати продуктивність та комунікацію між працівниками.

Крім того, було проведено аналіз платформ, на яких базуються носимі пристрої. Було виокремлено різні платформи, такі як мікроконтролери ESP32, AVR, STM32, PIC та Nordic nRF52, кожна з яких має свої унікальні характеристики, переваги та обмеження. Зроблено висновок, що кожна платформа може бути успішно використана для створення різних типів носимих пристроїв залежно від вимог проекту та доступних ресурсів.

Також було виявлено, що використання відповідних програмних та технічних засобів є важливим аспектом для підвищення безпеки носимих пристроїв та забезпечення надійної роботи для користувачів. Застосування програмного забезпечення для виявлення та попередження небезпечних ситуацій, а також застосування захисних механізмів, таких як шифрування даних та захист від несанкціонованого доступу, можуть забезпечити високий рівень безпеки для користувачів.

Таким чином, зроблено висновок, що носимі пристрої можуть бути успішно використані для покращення умов праці та забезпечення безпеки працівників на робочому місці. Однак, при виборі та використанні носимих пристроїв необхідно враховувати ризики та переваги, а також індивідуальні потреби та вимоги кожного працівника для досягнення найкращих результатів.

ПЕРЕЛІК ПОСИЛАНЬ

1. 1. AVR Architecture [Електронний ресурс] – Режим доступу до ресурсу: http://www.exploreembedded.com/wiki/1._AVR_Architecture.
2. A comparison of wearable fitness devices [Електронний ресурс] – Режим доступу до ресурсу: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4877805/.
3. A timeline of how the Apple Watch was created [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.businessinsider.com/a-timeline-of-how-the-apple-watch-was-created-2015-3.
4. Arduino AESLib [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/DavyLandman/AESLib.
5. Arduino Cloud Security Considerations [Електронний ресурс] – Режим доступу до ресурсу: https://docs.arduino.cc/arduino-cloud/features/security-considerations.
6. Arduino Cryptography Library: Hash Class Reference [Електронний ресурс] – Режим доступу до ресурсу: https://rweather.github.io/arduinolibs/classHash.html.
7. Arduino Documentation [Електронний ресурс] – Режим доступу до ресурсу: https://docs.arduino.cc/.
8. Arduino library to update the sketch over the network to a supported Arduino board [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/JAndrassy/ArduinoOTA.
9. Arduino TOTP Library [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/lucadentella/TOTP-Arduino.
10. ATmega versus STM32: Which Microcontroller is Best for Your Application [Електронний ресурс] – Режим доступу до ресурсу: https://predictabledesigns.com/atmega-versus-stm32-which-microcontroller-is-best-for-your-application/.

11. AVR microcontrollers [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/AVR_microcontrollers.
12. Balatska V. ДОСЛІДЖЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ СКАНЕРОМ ВРАЗЛИВОСТІ NESSUS / Balatska V, Shabatura M. // Львівський державний університет безпеки життєдіяльності. – 2019 – С. 3-4.
13. Barybin O. ТЕСТУВАННЯ БЕЗПЕКИ ПРИСТРОЇВ ІНТРЕНЕТУ РЕЧЕЙ НА БАЗІ МІКРОКОНТРОЛЕРА ESP32 / O. Barybin, E. Zaitseva, V. Brazhnyi. // Кібербезпека: освіта, наука, техніка. – 2019. – №2. – С. 71–81.
14. Characterizing Smartwatch Usage in the Wild / Xing Liu, Tianyu Chen, Feng Qian та ін.]. // MobiSys '17: Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services. – 2017. – С. 385–398.
15. Contact information social exchange method and system [Електронний ресурс] – Режим доступу до ресурсу: https://patents.google.com/patent/US9313609B2/en.
16. Coverity Scan - Static Analysis [Електронний ресурс] – Режим доступу до ресурсу: https://scan.coverity.com/.
17. Cppcheck - A tool for static C/C++ code analysis [Електронний ресурс] – Режим доступу до ресурсу: https://cppcheck.sourceforge.io/.
18. Crypto [Електронний ресурс] – Режим доступу до ресурсу: https://reference.arduino.cc/reference/en/libraries/crypto/.
19. ESP HTTPS OTA [Електронний ресурс] – Режим доступу до ресурсу: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/system/esp_https_ota.html.
20. ESP32: How to Log Data (9 Different Ways) [Електронний ресурс] – Режим доступу до ресурсу: https://randomnerdtutorials.com/esp32-how-to-log-data/.
21. ESP32_Data_Logging_Webserver [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/G6EJD/ESP32_Data_Logging_Webserver.

22. ESPAsyncWebServer [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/me-no-dev/ESPAsyncWebServer.

23. ESP-TOTP [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/huming2207/esp-totp.

24. Hardware Security By Design: ESP32 Guidance [Електронний ресурс] – Режим доступу до ресурсу: https://research.nccgroup.com/2022/05/31/hardware-security-by-design-esp32-guidance/.

25. Khakurel J. The Use of Wearable Devices in the Workplace - A Systematic Literature Review / J. Khakurel, S. Pöysä, J. Porras. // Lecture Notes of the Institute for Computer Sciences. – 2017.

26. Kurniawan A. Internet of Things Projects with ESP32: Build exciting and powerful IoT projects using the all-new Espressif ESP32 / Agus Kurniawan., 2019. – 252 с.

27. Lesson 14. EEPROM in Arduino. Data integrity control. [Електронний ресурс] – Режим доступу до ресурсу: https://mypractic.com/lesson-14-eeprom-in-arduino-data-integrity-control/.

28. Mbed TLS [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Mbed_TLS.

29. Microchip Libraries for Applications [Електронний ресурс] – Режим доступу до ресурсу: https://www.microchip.com/en-us/tools-resources/develop/libraries/microchip-libraries-for-applications.

30. MPLAB® X IDE [Електронний ресурс] – Режим доступу до ресурсу: https://www.microchip.com/en-us/tools-resources/develop/mplab-x-ide.

31. Necessity of Automated Vulnerability Assessment in Healthcare with the Emergence of 5G. // 2021 IEEE International Smart Cities Conference (ISC2). – 2021.

32. Nordic nRF52-DK [Електронний ресурс] – Режим доступу до ресурсу: https://os.mbed.com/platforms/Nordic-nRF52-DK/.
33. nRF Connect for Desktop [Електронний ресурс] – Режим доступу до ресурсу: https://www.nordicsemi.com/Products/Development-tools/nrf-connect-for-desktop.
34. nRF5 SDK [Електронний ресурс] – Режим доступу до ресурсу: https://www.nordicsemi.com/Products/Development-software/nrf5-sdk.
35. PIC microcontrollers [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/PIC_microcontrollers.
36. PICKIT SERIAL ANALYZER [Електронний ресурс] – Режим доступу до ресурсу: https://www.microchip.com/en-us/development-tool/DV164122.
37. Polyspace [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Polyspace.
38. PPGPass: Nonintrusive and Secure Mobile Two-Factor Authentication via Wearables / [Y. Cao, Q. Zhang, F. Li та ін.]. // IEEE IEEE INFOCOM 2020 - IEEE Conference on Computer Communications - Toronto, ON, Canada. – 2020. – №2020. – С. 1917–1926.
39. Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices / [H. Liu, H. Ning, Y. Yue та ін.]. // Future Generation Computer Systems. – 2018. – №2018.
40. Smart Watch Global Market Report 2021: COVID 19 Growth And Change to 2030 [Електронний ресурс] – Режим доступу до ресурсу: https://www.reportlinker.com/p06070190/Smart-Watch-Global-Market-Report-COVID-19-Growth-And-Change-to.html.
41. Stern B. Getting Started with Adafruit FLORA Making Wearables with an Arduino-Compatible Electronics Platform / B. Stern, T. Cooper., 2015
42. STM32 HAL-based library for SDHC/SDXC-cards [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/afiskon/stm32-sdcard.

43. STM32CubeProgrammer software for all STM32 [Електронний ресурс] – Режим доступу до ресурсу: https://www.st.com/en/development-tools/stm32cubeprog.html.
44. Strategy Analytics: Half-Billion Wearables Sold Worldwide in 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://www.businesswire.com/news/home/20210322005828/en/Strategy-Analytics-Half-Billion-Wearables-Sold-Worldwide-in-2020.
45. Tapping into the Wearable Device Revolution in the Work Environment: A systematic review [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/319332148_Tapping_into_the_Wearable_Device_Revolution_in_the_Work_Environment_A_systematic_review.
46. The Internet of Things with ESP32 [Електронний ресурс] – Режим доступу до ресурсу: http://esp32.net/.
47. This NFC Ring Puts Wireless Transfer Tech On Your Finger So You Can Fist-Bump Phones [Електронний ресурс] – Режим доступу до ресурсу: https://techcrunch.com/2013/07/23/put-an-nfc-ring-on-it/.
48. Trusted Platform Module - Wikipedia [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Trusted_Platform_Module.
49. Wearable technology [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Wearable_technology.
50. Wearable technology. Health-care solutions for a growing global population [Електронний ресурс] – Режим доступу до ресурсу: https://pubmed.ncbi.nlm.nih.gov/20659854/.
51. What is PIC Microcontroller and Its Architecture [Електронний ресурс] – Режим доступу до ресурсу: https://www.watelectronics.com/pic-microcontroller-architecture-and-applications/.
52. What Is Wearable Technology (Wearables)? Definition and Examples [Електронний ресурс] – Режим доступу до ресурсу: https://www.investopedia.com/terms/w/wearable-technology.asp.

53. Марчук Н. КЛАСИФІКАЦІЯ НОСИМИХ ЕЛЕКТРОННИХ ПРИСТРОЇВ / Н. Марчук, В. Осієвська, Г. Михайлова. // Міжнародний науково-практичний журнал «Товари і ринки». – 2021. – №4. – С. 68–78.
54. Як ESP32 IoT змінює гру для підключених пристроїв [Електронний ресурс] – Режим доступу до ресурсу: https://www.dusuniot.com/uk/blog/how-esp32-iot-is-changing-the-game-for-connected-devices/.