DOI: https://doi.org/10.36910/6775-2524-0560-2023-53-41
УДК 004.93
Левицька Тетяна Олександрівна, к.т.н., доцент
https://orcid.org/0000-0003-3359-1313
Парахін Руслан Олегович, студент
ДВНЗ «Приазовський державний технічний університет», м. Дніпро, Україна

СИСТЕМА ВИМІРЮВАННЯ ДОКЛАДЕНИХ ЗУСИЛЬ, РУХУ ТА ВІБРАЦІЙНОГО ВІДГУКУ ВЕСЛА З BLUETOOTH®-КОМУНІКАЦІЄЮ

Левицька Т.О., Парахін Р.О. Система вимірювання докладених зусиль, руху та вібраційного відгуку весла з Bluetooth®-комунікацією. Дана стаття присвячена огляду окремих аспектів реалізації вбудованої системи вимірювання спортивних параметрів для "розумного" весла з Bluetooth®-комунікацією. Досліджено особливості функціонування протоколу Bluetooth® Low energy для пристроїв публічного використання**,** розроблено систему безпечної комунікації між смартфоном користувача та веслом, проведено аналіз поведінки сенсорів навантаження (прикладеного зусилля), гіроскопу та акселерометра. Проаналізовано умови зовнішньої середи функціонування пристроїв та проведено відповідні корекції програмного коду для подовження часу повноцінного функціонування. Планується впровадження методів самоперевірки стану сенсорів "розумних" весел.
Ключові слова: вбудовані системи, Bluetooth® Low Energy, вимірювання зусиль, відстежування руху, калібрування

Levitska T., Parakhin R. A system for measuring the effort, movement and vibration response of the paddle with Bluetooth® communication. This article is devoted to an overview of certain aspects of the implementation of a built-in system for measuring sports parameters for a "smart" paddle with Bluetooth® communication. The features of the Bluetooth® Low energy protocol for public use devices were studied, a secure communication system was developed between the user's smartphone and the paddle, and the behavior of load sensors (applied force), gyroscope and accelerometer were analyzed. The conditions of the external environment for the functioning of the devices were analyzed and appropriate corrections were made to the software code to extend the time of full functioning. It is planned to introduce methods of self-checking the state of sensors of "smart" oars.
Keywords: embedded systems, Bluetooth® Low Energy, effort measurement, motion tracking, calibration

Постановка проблеми. Кількісна та якісна оцінка зусиль веслувальника під час тренування є важливою частиною процесу підготовки до змагань та покращення власних результатів. Однак на теперішній момент, більшість тренувань з веслування на воді проходять без можливості оцінити показники веслувальника у конкретних цифрах. Тренери повинні використовувати стаціонарні тренажери[1], аби побачити зусилля, які докладає веслувальник; або, якщо тренування проходить у човні на воді - лише на власний зір та відчуття від того, на скільки спортсмен докладає зусилля для досягнення результату. Ситуація ускладнюється тим, що веслування є командним видом спорту, де в одному човні знаходяться по 6 (а інколи й більше) веслувальників, за якими потрібно стежити одночасно.

Стаціонарні тренажери не здатні у повній мірі відтворити обставини реальних змагань на воді, а обладнання, яке можна тимчасово встановити на човен для замірів показників під час повноцінних тренувань, є дуже коштовним та потребує виклику команди спеціалістів, що будуть займатися замірами.

Метою даної роботи було створити дешеву, компактну, надійну та енергоефективну систему, яку можна встановити у весла на постійній основі, аби під час кожного тренування можливо було у конкретних цифрах оцінити показники кожного з веслувальників. Пристрій повинен витримувати занурення у воду, бути стійким до морозів, не потребувати частих підзарядок чи іншого обслуговування.

Виклад основного матеріалу.

Протокол Bluetooth® Low Energy[2] було обрано для комунікації з "розумним" веслом через його відповідність низці потреб, які не змогли задовільнити інші методи комунікації. В таблиці 1 порівняно ключові аспекти протоколів комунікації, що розглядаються у порівнянні з Bluetooth® Low Energy. Варто окремо зазначити, що йдеться саме про BLE - оновлену версію технології, що відрізняється низьким енергоспоживанням та принципово іншими методами побудови комунікації.

Таблиця 1 – Приклади результатів навчання багатошарового персептрону

Метод	Шлях даних	Час надходження даних на смартфон	Використання на відстані 1 км. від берега	Захист від втручання третіх осіб	Вартість підтримки	Енерго-споживання
BLE	Весло - Смартфон	< 100 мс	Можливе	Частковий	0 грн / міс.	Низьке
LTE	Весло - Сотова станція - Смартфон	Від 200 мс, погіршується зі збільшенням відстані від сотової станції	Майже неможливе	Достатній	Від 30 грн / міс. [3]	Високе
Local Wi-Fi	Весло - Роутер - Смартфон	100-200 мс	Неможливе вже за декілька десятків метрів від роутера	Достатній	0 грн / міс.	Високе

З порівняльної таблиці 1 бачимо, що серед підтримуваних смартфонами методів комунікації, лише Bluetooth® дає можливість обмінюватися даними на достатній швидкості в умовах великої дистанції від берега.

Комунікацію за даним протоколом побудовано за схемою на рисунку 1

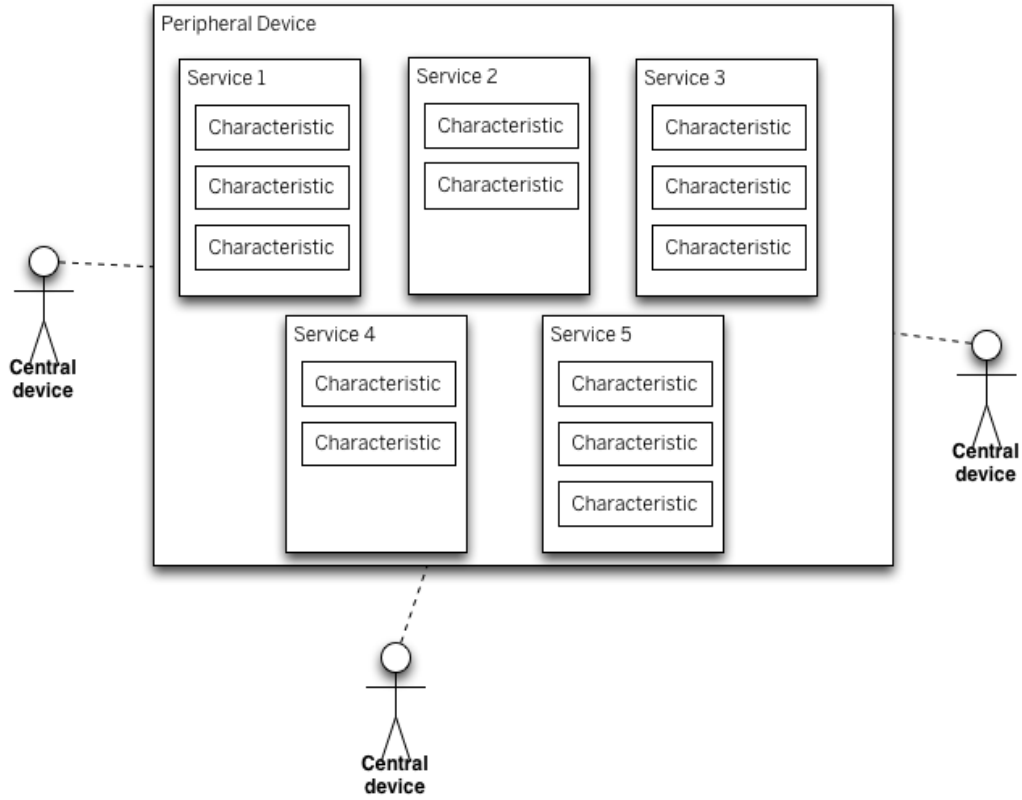

Рис.1. Схема побудови протоколу BLE

Переферійний девайс (в нашому випадку - весло) має певний набір сервісів. Кожен сервіс є групуванням характеристик за певною тематикою. Він включає в себе власне характеристики - окремі гілки даних, які можна зчитувати. Центральні девайси (в нашому випадку - смартфон) під'єднуються до переферійного та зчитують значення його характеристик. Вони можуть зробити це одноразово чи підписатися на постійні оновлення.

Особливістю реалізації "розумного" весла є те, що весло є девайсом публічного користування. Воно не належить певному веслувальнику, а закріплене за човном, і використовуються будь ким, хто побажає розпочати тренування з ним. Ця умова не дозволяє використовувати вбудовану в Bluetooth® функцію парування (pairing), адже ця функція

1. Сповільнює початкове підключення до весла
2. Викликає показ системного діалогу
3. Залишає весло у списку відомих девайсів у смартфоні, що є проблемою для користувачів, які підключаються до великої кількості різних весел і не хочуть потім бачити їх у списку відомих

Окрім цього, хоча функція парування й могла би захистити шифруванням канал обміну даними між смартфоном та веслом, це не вирішує основної проблеми. Як тільки дані надійшли до смартфона, він повинен взяти їх на власний аналіз та відправити на сервер тренування, аби інші могли їх побачити. Але нічого не заважає достатньо компетентному користувачу модифікувати додаток на смартфоні і довільним чином змінювати отримані показання з весла, аби завищувати власні спортивні результати. Окрім цього, ніщо не заважає достатньо компетентному користувачу надіслати на весло адміністративну команду для зміни калібрування чи інших шкідливих дій.

Смартфон користувача виступає проміжним пристроєм у комунікації між веслом та сервером тренування, і цей пристрій не може бути довіреним. Шифрування даних на веслі перед відправленням їх на сервер через смартфон також не є можливим, адже смартфон повинен бачити власне самі дані для їх локального аналізу та виводу в інтерфейс додатку.

Постає завдання створити систему верифікації та автентифікації повідомлень у каналі зв'язку Весло - Смартфон - Сервер таким чином, аби самі дані були повністю відкритим, але підмінити їх на бажані зловмиснику було неможливо. Сервер теж може надсилати деякі команди веслу через смартфон, тож захист повинен працювати в обидві сторони. Оскільки за суттю функціонування додатку деякі функції (наприклад - вібрація весла у відгук на низьке зусилля) повинні працювати моментально та навіть при відсутності зв'язку з сервером, також потрібно створити систему, що дозволить тимчасово надавати авторитет на виконання веслом певних команд за запитом користувача минаючи етап авторизації через сервер.

Для реалізації поставлених завдань з захисту було створено систему "квитків" (tickets). Квиток являє собою структуру даних, містить в собі набір умов використання (максимальна тривалість дії, максимальна кількість використань, мінімальний проміжок часу між використаннями) та секретний ключ. Під терміном "використання" мається наувазі виконання авторизованої дії за допомогою квитка. Наприклад, для квитка системи вібрації, "використанням" є один виклик функції вібрації. Квиток має функції sign (підписати), derive (наслідувати) та verify (верифікувати). Функція sign приймає аргументом повідомлення (дані, команду тощо) та додає до нього 32-байтовий HMAC-SHA256[4, 5] код верифікації, використовуючи секретний ключ цього квитка. Запобігання replay атакам досягається використанням штампу UNIX-часу, що є у кожного повідомлення. Цей штамп дозволяє чітко розуміти, коли було створено повідомлення, а також дозволяє мати абсолютно різні верифікаційні коди для двох в усьому іншому ідентичних повідомлень з ідентичним набором даних.

У системі існує root ticket - кореневий квиток - створений заздалегідь квиток, що має спільний секретний ключ, який є унікальним для кожного весла та записаним у його внутрішню пам'ять. Цей ключ також є в базі даних на сервері, що дозволяє серверу верифікувати дані за допомогою функції verify того самого квитка. Ця функція порівнює самостійно згенерований код верифікації з тим кодом верифікації, що надійшов разом із повідомленням. Якщо повідомлення було змінено смартфоном користувача, він не зможе додати до нього дійсний код верифікації, адже у нього немає спільного секретного ключа сервера та весла, який було використано для накладання оригінального коду. Також ця система дозволяє перевіряти повноваження користувача в коді на сервері, тож, наприклад, якщо неавторизований користувач сформує запит на калібрування весла,

сервер просто відмовиться додавати у цей запит вірний код верифікації, що зробить неможливим його виконання цього запиту веслом та захистить пристрій від несанкціонованих змін налаштувань.

Як було зазначено раніше, у деяких випадках користувачу все ж потрібно надавати тимчасову можливість керувати певними функціями весла без верифікації його запитів сервером. Для цього потрібно створити новий "квиток", який буде відповідати за керування лише певними підсистемами весла, і який додаток користувача зможе використати для самостійного накладання верифікаційних кодів на повідомлення. При цьому, коли смартфон та весло будуть "узгоджувати" створення такого квитка, жодної секретної інформації не повинно бути передано, адже її потенційно може перехопити третя особа. Для створення нового квитка у відповідних умовах використовується механізм "наслідування" (команда derive). Сервер генерує команду для створення квитка, що містить операційний код створення, умови користування та штамп часу, накладає верифікаційний код за допомогою спільного секретного ключа з кореневого квитка - та надсилає її крізь смартфон користувача на весло. Також сервер ділиться з користувачем тимчасовим секретом. Весло, використовуючи цю команду, спільний секрет та штамп часу створює новий тимчасовий секрет, попередньо верифікуючи команду за допомогою кореневого квитка. Тепер користувач може використовувати тимчасовий секрет, який надав йому сервер, для самостійного виклику окремих команд за тимчасовим квитком. Якщо комунікацію не було спотворено, то весло наслідує новий тимчасовий секрет, що буде ідентичним тому секрету, яким сервер поділився з користувачем. При цьому жодних секретних даних за відкритою частиною каналу комунікації (зв'язок Смартфон - Сервер захищено HTTPS) не було передано, а була передана лише команда наслідування з параметрами. Оскільки сервер сам встановлює параметри та верифікує їх тим самим методом, що й звичайні повідомлення, у користувача немає можливості їх змінити. Завдяки цьому система безпеки весла розуміє, коли тимчасовий квиток потрібно деактивувати і скільки раз його можна використати. Тимчасовий секрет є дійсним впродовж відносно невеликого проміжку часу (10-15 хв.), тож якщо володар смартфону, на який було надіслано тимчасовий секрет, модифікує додаток та почте використовувати секрет у незапланованих цілях, його дії будуть суворо обмежені повноваженнями тимчасового квитка, які задав сервер, та часом дії цього квитка. У прикладі з вібрацією, якщо додаток буде модифіковано, тимчасовий секрет можна буде використати максимум для "спаму" вібраціями впродовж тих хвилин, у які він є дійсним. Жоден інший компонент системи не буде поставлено у ризик.

Маючи систему захисту комунікацій від підроблення, можна переходити до власне змісту комунікацій - показів сенсорів на веслі. Поточна модель весла обладнана наступними сенсорами:

1. Тензодатчик - датчик, що згинається під дією зовнішньої ваги, змінюючи свій електричний спротив. Цю зміну можна виміряти та використати для отримання зусилля, яке докладає веслувальник під час тренування.
2. Гіроскоп - датчик, що має у собі невеликий рухомий елемент, який відхиляється при обертанні. Дозволяє виміряти, з якою кутовою швидкістю обертається пристрій.
3. Акселерометр - датчик, що має у собі невеликий рухомий елемент, який відхиляється при русі. Дозволяє виміряти, з яким прискоренням рухається пристрій.

В таблиці 2 розглянуто особливості кожного з сенсорів.

Ще однією фізичною особливістю використаних тензодатчиків є невелике відхилення від лінійності, яке все ж таки не є бажаним і потребує корегування. Для цього використовується крива з декількох коефіцієнтів множення. Маючи відоме "сире" значення з тензодатчику та компенсуючи базовий зсув, на кривій коефіцієнтів коригування лінійною інтерполяцією вираховується оптимальний коефіцієнт множення саме для цієї ваги, після чого, власне, і рахується сама вага. Така корекція допомагає збільшити точність вимірювань, при цьому уникаючи стрибків показань, які були б можливі на точках "переходу" між різними коефіцієнтами множення, якби не була задіяна лінійна інтерполяція.

Таблиця 2 - Особливості сенсорів, присутніх у веслі

Сенсор	Метод калібрування	Суть калібрування	Комунікація	Стабільність

Тензодатчик	Спокоєм та навантаженням відомою вагою	Виміряти базовий зсув (тара) та коефіцієнт множення (за відомою вагою)	Проміжний АЦП-підсилювач	Шуми ± 10 грамів
Акселерометр	Не потрібне	-	I²C	Шуми та накопичення помилки у разі прямого послідовного додавання показів
Гіроскоп	Спокоєм	Визначити швидкість "фантомного обертання", яке вимірює сенсор у спокої		

Ще однією фізичною особливістю використаних тензодатчиків є невелике відхилення від лінійності, яке все ж таки не є бажаним і потребує корегування. Для цього використовується крива з декількох коефіцієнтів множення. Маючи відоме "сире" значення з тензодатчику та компенсуючи базовий зсув, на кривій коефіцієнтів коригування лінійною інтерполяцією вираховується оптимальний коефіцієнт множення саме для цієї ваги, після чого, власне, і рахується сама вага. Така корекція допомагає збільшити точність вимірювань, при цьому уникаючи стрибків показань, які були б можливі на точках "переходу" між різними коефіцієнтами множення, якби не була задіяна лінійна інтерполяція.

Проблемою також є невелика стабільність вимірювань гіроскопа та акселерометра, що не дозволяє просто додавати їх показання з надходженням кожного нового, хоча за фізичним сенсом саме так потрібно і робити - складати прискорення (помножені на дельту часу з попереднього вимірювання), аби отримати швидкість, та швидкості обертання (також помножені на дельту часу з попереднього вимірювання), аби отримати кут, на який обернувся пристрій за проміжок часу. Втім, в реальності для цього існують набагато більш комплексні алгоритми фільтрації та взаємокомпенсування показників, що дозволяють отримати абсолютні кути повороту пристрою. Один з них - complementary filter [6-9] - використовується в даній системі для досягнення результату. Запорукою правильного функціонування системи є часті вимірювання з незмінюваним регулярним проміжком. Вимірювання проводяться з раз на 10 мс, для забезпечення такої великої частоти вимірювань, код цих операцій винесено в окремий потік. Це стає можливим завдяки використанню FreeRTOS [10] - невеликої системи реального часу, що дозволяє виокремити обчислення в окремий потік та раз на 10 мс переривати виконання будь якого іншого коду, оновлювати поворот пристрою і повертатись до основного потоку.

Ще одним вбудованим "сенсором" є вимірювач напруги на вбудованому акумуляторі, що використовується для визначення рівня заряду. Оскільки зміна напруги під час розрядки акумулятора не є лінійною, було виміряно та побудовано криву, яка відображає реальне співвідношення напруги до рівня заряду, що залишився в акумуляторі (рисунок 2). Ця крива використовується для розрахунку реального відсотку заряду весла, аби надавати користувачам та персоналу водної станції розуміння того, скільки днів роботи від нього можна очікувати.

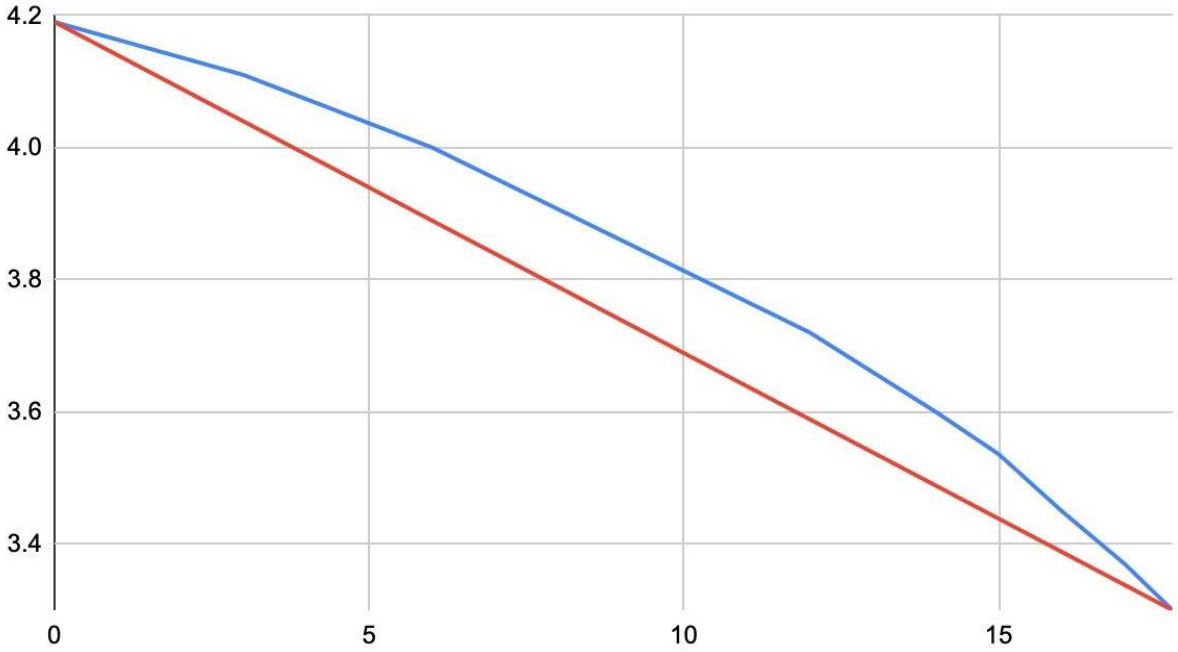

Рис.2. Співвідношення кількості днів (вісь X) безперервного функціонування до напруги на акумуляторі (вісь Y). Синє - реальні вимірювання, червоне - ідеальна пряма

Описані методи роботи з сенсорами дозволяють досягти їх стабільного функціонування у незвичайних для них умовах. Специфіка використання "розумних весел" передбачає їх функціонування у холодній та вологій середі. Також не передбачено регулярне перезарядження акумуляторів пристрою чи регулярне перекалібрування його сенсорів. Для оптимізації енергоспоживання пристрою використовуються наступні програмні методи:

- Інтервал 2 секунди між надсиланням рекламних пакетів весла, коли до нього не під'єднано жодного пристрою (зазвичай, такі інтервали більш притаманні BLE-маячкам, у яких взагалі не передбачено підключення)
- Перехід потоків у режим сну
- Виклик вбудованих у сенсори режимів сну

Висновки та напрямок подальших покращень.

Створено систему, що дозволяє чітко виміряти основні характеристики взаємодії з веслом під час тренування. Пристрій може місяцями працювати від одного заряду батареї, а водонепроникний дизайн робить його стійким до суворих умов навколишнього середовища. Система верифікації даних та авторизації керування веслом дозволяє чітко контролювати його функціонування та протистояти спробам підробки показань, при цьому комунікуючи за частково відкритим каналом.

Подальші покращення необхідно проводити в сфері самотестування сенсорів для виявлення збоїв у їх роботі. Оскільки системі чітко відомо, коли до неї не підключений користувач та коли вона знаходилася у стані спокою впродовж тривалого часу, перебування у стані спокою можна використати для запуску невеликих тестів самоперевірки, що можуть ідентифікувати аномалії у показаннях сенсорів та сповіщати про ці аномалії веслувальників та працівників водної станції.

Список бібліографічного опису

1. "Concept 2 Indoor Rowers" https://www.concept2.com/indoor-rowers
2. "Bluetooth® Wireless Technology" https://www.bluetooth.com/learn-about-bluetooth/tech-overview
3. "Lifecell Тариф Ґаджет Безпека" https://www.lifecell.ua/uk/mobilnij-zvyazok/taryfy/gadget-bezpeka
4. National Institute of Standards and Technology. Secure Hash Standard (SHS). // Information Technology Laboratory. 2015. №180-4 DOI: http://dx.doi.org/10.6028/NIST.FIPS.180-4

5. Bellare Mihir, Canetti Ran, Krawczyk Hugo. Message Authentication using Hash Functions—The HMAC Construction. // RSA Laboratories 'CryptoBytes. №2(1). 1996. https://cseweb.ucsd.edu/~mihir/papers/hmac-cb.pdf
6. Tae Suk Yoo, Sung Kyung Hong, Hyok Min Yoon. Gain-Scheduled Complementary Filter Design for a MEMS Based Attitude and Heading Reference System // MDPI. 2011, №11(4), С. 3816-3830 DOI: https://doi.org/10.3390/s110403816
7. Baerveldt, AJ; Klang, R. A low-cost and low-weight attitude estimation system for an autonomous helicopter // Proceedings of IEEE International Conference on Intelligent Engineering Systems. 15.09.1997. С. 391–395.
8. Demoz, GE. A low-cost GPS/inertial Attitude Heading Reference System (AHRS) for general aviation applications // Proceedings of Position Location and Navigation Symposium. 20.04.1998. С. 518–525.
9. Euston, M; Coote, P; Mahony, R; Kim, J; Hamel, T. A complementary filter for attitude estimation of a fixed-wing UAV // Proceedings of IEEE/RSJ International Conference on Intelligent Robots and Systems, 22.09.2008. С. 340–345.
10. "About FreeRTOS Kernel" https://www.freertos.org/RTOS.html