УДК 629.7.02+004.056.5 DOI: https://doi.org/10.32515/2414-3820.2021.51.216-226

Є.В. Мелешко, проф., д-р техн. наук, **О.О. Майданик,** магістрант, **О.Г. Собінов,** викл., **Р.М. Минайленко,** доц., канд. техн. наук
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна
e-mail: elismeleshko@gmail.com, maidanyksmail@gmail.com, sagcob14@gmail.com, aron70@ukr.net

Метод шифрування трафіку квадрокоптерів через аналоговий тракт впродовж моніторингу сільськогосподарських наземних об’єктів

Метою даної роботи є розробка методу шифрування трафіку квадрокоптерів через аналоговий тракт під час моніторингу стану сільськогосподарських наземних об’єктів. Використання безпілотних літальних пристроїв квадрокоптерного типу для моніторингу наземних об’єктів у сільському господарстві стає все більш поширеною практикою та дозволяє ефективно вирішувати велике коло задач, зокрема, використовуючи аерофотозйомку відеозйомку, тепловізійну зйомку, лазерне сканування тощо. В той же час квадрокоптери дуже вразливі до різних кібератак, що зумовлює необхідність розробки дієвих методів їх інформаційного захисту. У цій роботі для захисту даних, якими дрон обмінюється з іншими пристроями, запропоновано використовувати шифр Вернама та генерацію ключів шифрування на основі математичного більярду Сіная. Було розроблено відповідні алгоритми та програмне забезпечення для шифрування даних, а також створені робочі макети пристроїв для проведення експериментів. Для створення макету обрано модуль на основі мікроконтролера STM32F103C8T6, дані між пристроями передавалися через радіомодуль.
шифрування, генерація ключів, трафік, квадрокоптер, аналоговий тракт, моніторинг, сільськогосподарські наземні об’єкти

Постановка проблеми. Використання безпілотних літальних пристроїв квадрокоптерного типу для моніторингу наземних об’єктів у сільському господарстві стає все більш поширеною практикою та дозволяє ефективно вирішувати велике коло задач. В той же час квадрокоптери вразливі до інформаційних атак, що можуть здійснюватися з різними цілями, зокрема, для крадіжки дрону, використання його у мережі ботів для атак на інші пристрої, або для перехвату інформації, яку він збирає для оператора пристрою. Це все зумовлює необхідність розробки дієвих методів інформаційного захисту дронів від кібератак.

Аналіз останніх досліджень і публікацій. Використання дронів у сільському господарстві для вирішення задач моніторингу наземних об’єктів – один із найперспективніших напрямів, на який активно зростає попит. Технологічно оснащені безпілотники у сільському господарстві здатні виконувати різноманітні операції моніторингу [1-4], зокрема: аерофотозйомку відеозйомку, тепловізійну зйомку, лазерне сканування тощо. Такий моніторинг дозволяє здійснювати оцінку якості посівів та виявляти факти пошкоджень чи загибелі культур, виявляти дефекти посіву та проблемні зони, аналізувати ефективність заходів для на захисту рослин, перевіряти відповідності планам сівозміни, виявляти відхилення та порушення у процесі агротехнічних робіт, аналізувати рельєф та створювати карти, проводити аудит та інвентаризацію земель, здійснювати охоронні заходи та збирати інформацію для служби безпеки тощо.

Кіберзлочинці часто зламують дрони та використовують їх у своїх цілях, у тому числі для злому інших пристроїв [5]. Безпілотники сповнені вразливостей, які використовують зловмисники. Захоплення одного безпілотника за допомогою іншого значно розширює потенціал загрози. Ботнети з приватних пристроїв, захоплених зловмисниками, можуть здійснювати різні атаки, наприклад, інформаційні атаки DDOS. Чим більше незахищених дронів у небі – тим більшу небезпеку вони становлять. Також зловмисники можуть перехоплювати дані, які дрон передає на базову станцію, наприклад, відеозапис, що транслюється на контролер системою First Person View (FPV). Часто виробники звичайних дронів, які продаються в магазинах, не захищають їх шифруванням, а незашифровані дані – легкий здобуток для зловмисників [5]. Тому інформацію, якою обмінюється дрон з іншими пристроями треба обов'язково захищати шифруванням.

У даній роботі пропонується метод шифрування трафіку квадрокоптерів через аналоговий тракт для захисту даних, якими він обмінюється з іншими пристроями, а також передає оператору. Особливу увагу при розробці методу шифрування було приділено методу генерації ключів шифрування, адже саме на них базується стійкість будь-якого алгоритму шифрування. Найчастіше при генерації ключів шифрування використовують генератори псевдовипадкових чисел (ГПВЧ) Дуже часто ГПВЧ є найбільш слабким місцем у системах шифрування. Послідовності, отримані в результаті роботи ГПВЧ повинні бути непередбачуваними та мати довгий період, щоб їх можна було використовувати в криптографічних системах захисту інформації [6-7].

У 1976 році відомий математик Сінай Ю.Г. довів, що поведінка більярдної кулі у динамічному більярді, яка визначається детермінованим рівнянням, та поведінка більярдної кулі, яка керується процесом Маркова першого порядку, нерозрізнимі [8]. Оскільки марковський процес першого порядку є ймовірнісним процесом, який залежить тільки від попереднього зіткнення з перепоною, то він є як недетермінованим, так і непередбачуваним. Системи динамічного більярду виявили добре розвинену хаотичну поведінку [9]. Незважаючи на хороші характеристики, ці системи ще не застосовуються у криптографії. Головною причиною є складність вираження рівняння руху частинок в явній формі, але тим не менш таке використання є можливим [10].

Постановка завдання. Таким чином, метою даної роботи є створення методу шифрування трафіку квадрокоптерів через аналоговий тракт з використанням генератора випадкових чисел на основі математичного більярду Сіная для захисту даних під час здійснення моніторингу сільськогосподарських наземних об'єктів.

Виклад основного матеріалу. В даній роботі було створено апаратні пристрої з безпровідним каналом зв'язку та програмне забезпечення для шифрування даних на мікроконтролерах (МК).

Для реалізації програмного забезпечення, яке повинне виконуватися на мікроконтролері було обрано середовище розробки STM32CubeIDE від компанії STMicroelectronics – вдосконалену платформу розробки C/C++ [11] з периферійною конфігурацією, генерацією коду, складанням коду та налагодженням для мікроконтролерів та мікропроцесорів STM32.

Для побудови розроблюваної системи створено робочі макети пристроїв. Для створення макету обрано модуль на основі мікроконтролера STM32F103C8T6 [12]. Модуль має:

- Виводи портів A0-A12, B0-B1, B3-B15, C13-C15.

- Micro-USB через який можна живити плату. На платі присутній стабілізатор напруги на 3.3В. Живлення 3.3В або 5В можна подавати на відповідні виводи на платі.

- Кнопку RESET.
- Два перемички BOOT0 і BOOT1. Використовувати під час прошивки через UART.
- Два кварци 8МГц і 32768Гц. У мікроконтролера є множник частоти, тому на кварці 8 МГц можливо досягти максимальної частоти контролера 72Мгц.
- Два світлодіоди. PWR - сигналізує про подачу живлення. PC13 - підключений до виходу C13.

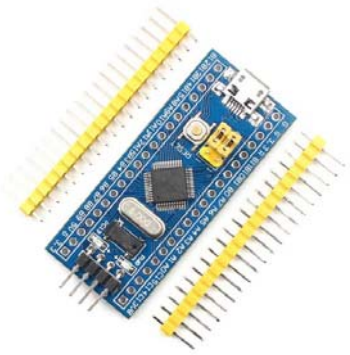

Рисунок 1 – Модуль на основі мікроконтролера STM32F103C8T6
Джерело: розроблено автором

Важливою частиною пристрою є радіомодуль. Вирішено використовувати радіомодуль JDY-40. Так як цей модуль має низьку ціну та відносно просте керування.

Модуль JDY-40 [13] дуже компактний і можна його живити від будь-якого літій-іонного акумулятора на 3,7 В, що дозволяє вбудувати його в будь-які моделі. Радіус дії радіомодуля до 120 метрів в прямій видимості, що для більшості пристроїв цілком достатньо, якщо потрібна велика дальність то можна застосувати зовнішню антену.

Для обміну даними з мікроконтролером модуля JDY-40 здійснюється по UART інтерфейсу з максимальною швидкістю 19200 біт. Для підключення периферії до модулю є 8 портів введення-виведення. На рис. 2 зображено модуль зв’язку JDY-40.

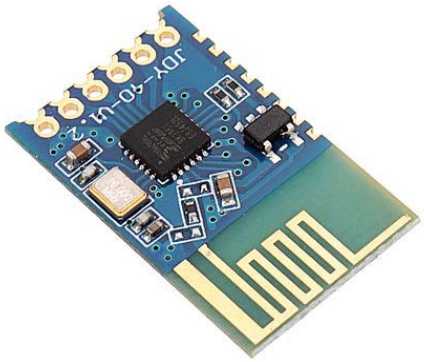

Рисунок 2 – Радіомодуль JDY-40
Джерело: розроблено автором

На основі модулів JDY-40 та макетної плати розроблено робочі макети пристроїв. На рис. 3 зображено макети пристроїв для передачі даних по радіоканалу.

На рис. 3 присутні програматори та логічний аналізатор, за допомогою яких здійснювалася наладка схеми. Обидва пристрої підключені до ПК, на якому відкрито два термінали. В кожному із терміналів необхідно обрати відповідний номер COM порту та відкрити його. Після відкриття COM порту можна передавати данні від ПК до мікроконтролера, який в свою чергу передасть їх на радіомодуль.

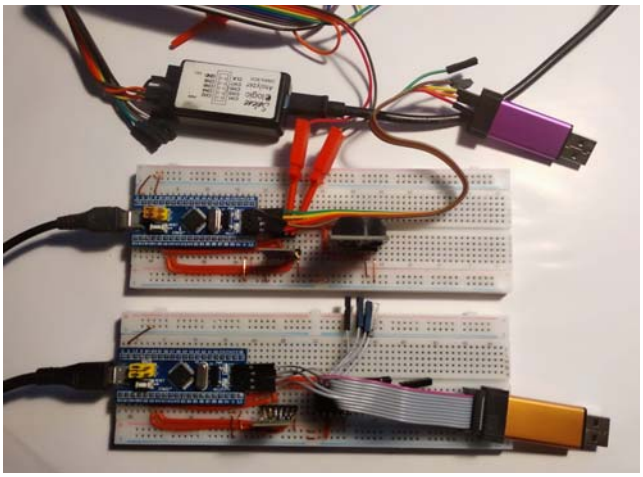

Рисунок 3 – Робочі макети пристроїв для передачі даних по радіоканалу
Джерело: розроблено автором

Для шифрування даних було використано шифр Вернама. А у якості ключа шифрування псевдовипадкову послідовність, що генерувалася за допомогою математичного більярду Сіная.

Розглянемо використану математичну модель генератора псевдовипадкових чисел на основі більярду Сіная.

Програма моделювання руху кулі у більярді Сіная базується на твердженнях, що рух кулі здійснюється без втрати швидкості (тертя відсутнє) та кут падіння дорівнює куту відбиття. Таким чином приймаємо, що рух кулі має швидкості по координатах $V_x = \cos(\acute{\alpha})$; $V_y = \sin(\acute{\alpha})$. Звідси $V_{x2} + V_{y2} = 1$. Приймаємо для побудови алгоритму руху кулі наступні вхідні параметри:

- напрямок руху кулі $-V = \{V_x, V_y\}$,
- початкове положення кулі у більярді – $P = \{P_x, P_y\}$.

Для розробки алгоритму побудуємо математичну модель руху математичної точки в полі опуклого більярду Сіная.

Точка частинки рухається по більярду з постійною швидкістю v. Коли вона досягає кордону поля більярда, зазнає пружного зіткнення з дзеркальним відображенням відповідно до закону відбиття, кут падіння дорівнює куту відбиття. Між двома зіткненнями точка рухається прямим шляхом. Спочатку точка орієнтована під кутом $\theta_0 = \left(\vec{i}, \overrightarrow{v_0}\right)$, де $\vec{i}$ одиничний вектор осі x.

З цього маємо: $\overrightarrow{v_0} = \cos(\theta_0)\vec{i} + \sin(\theta_0)\vec{j}$

Після зіткнення маємо рівняння (1):

$$\left(\vec{i}, \overrightarrow{v_{new}}\right) = \left(\vec{i}, \overrightarrow{v_{old}}\right) + \left(\overrightarrow{v_{old}}, \vec{N}\right) + \left(\vec{N}, \overrightarrow{v_{old}}\right) \bmod 2\pi . \quad (1)$$

Після правила зіткнення маємо: $\left(\vec{N}, \overrightarrow{v_{new}}\right) = \left(-\overrightarrow{v_{old}}, \vec{N}\right)$.

Також є:

$$\left(-\overrightarrow{v_{old}}, \vec{N}\right) = \left(-\overrightarrow{v_{old}}, \overrightarrow{v_{old}}\right) + \left(\overrightarrow{v_{old}}, \vec{N}\right) \bmod 2\pi = \pi + \left(\overrightarrow{v_{old}}, \vec{N}\right) \bmod 2\pi .$$

Тому рівняння (1) стає:

$$\left(\vec{i}, \overrightarrow{v_{new}}\right) = \left(\vec{i}, \overrightarrow{v_{old}}\right) + 2\left(\overrightarrow{v_{old}}, \vec{N}\right) + \pi \bmod 2\pi . \quad (2)$$

При $(n+1)$ зіткненні, де $n \geq 0$, приймаємо $\theta_0 = \left(\vec{i}, \overrightarrow{v_{new}}\right)$ і отримуємо: $\theta_{n+1} = \left(\vec{i}, \overrightarrow{v_{new}}\right)$ і тому рівняння (2) стає:

$$\theta_{n+1} = \theta_n + 2\left(\overrightarrow{v_n}, \overrightarrow{N_{n+1}}\right) + \pi \bmod 2\pi, \tag{3}$$

$$\overrightarrow{v_n} = \cos(\theta_0)\vec{i} + \sin(\theta_0)\vec{j},$$

де $\overrightarrow{N_{n+1}}$ одиничний нормальний вектор на кордоні до $(n+1)$ зіткнення. Після геометричної форми маємо більярд:

$$\overrightarrow{N_{n+1}} = \begin{cases} -\dfrac{x_{n+1}}{|x_{n+1}|}, \text{ якщо } |x_{n+1}| = a \\ -\dfrac{y_{n+1}}{|y_{n+1}|}, \text{ якщо } |y_{n+1}| = a \\ -\dfrac{x_{n+1}\vec{i} + y_{n+1}\vec{j}}{\sqrt{x_{n+1}^2 + y_{n+1}^2}}, \text{ інакше} \end{cases}. \tag{4}$$

Вважаємо $A_{n+1}(x_{n+1}, y_{n+1})$ точкою $(n+1)$ зіткнення, тому A_{n+1} належить до перетину траєкторій точок з більярдною межею Γ. Визначимо f, функцію переходу від $\left(A_n, \theta_n\right)$ до $\left(A_{n+1}, \theta_{n+1}\right)$, таких як:

$$\left(x_{n+1}, y_{n+1}, \theta_{n+1}\right) = f\left(x_n, y_n, \theta_n\right).$$

Генератор заснований на системі хаотичного більярду, тому створюються послідовності, які успадковують хаос і непередбачуваність більярду.

Чутливість до невеликої зміни початкових параметрів є однією з основних властивостей даного генератора псевдовипадкових чисел. Ця властивість робить генератор високо захищеним від статистичних та диференціальних атак.

За математичною моделлю генерації ключів шифрування на основі більярду Сіная розроблено алгоритм. Реалізація математичної моделі виконана мовою Pyton в середовищі Visual Studio Communnity з математичною бібліотекою Matplotlib. На рис. 4 зображено візуалізацію руху математичної точки в більярді Сіная при двох ітераціях.

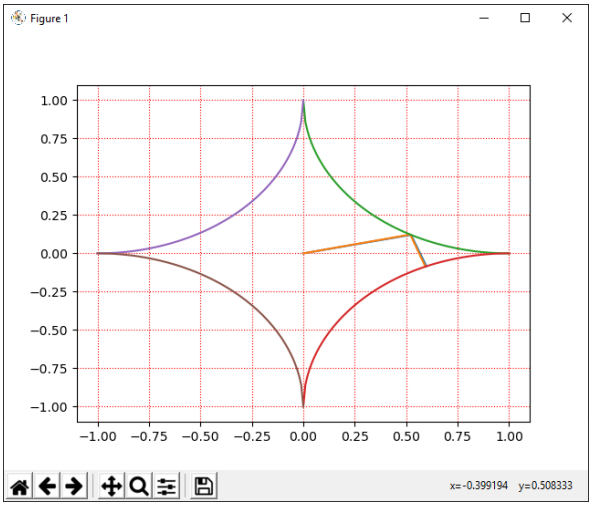

Рисунок 4 – Візуалізація руху математичної точки в більярді Сіная при 2-х ітераціях під час генерації ключа шифрування

Джерело: розроблено автором

З рис. 4 видно, що математичні частинки починають свій рух від центру поля в бік початкового кута, який задається на початку розрахунків. Далі частинка в точці перетину відбивається по закону кутів та рухається до іншої точки перетину. Саме в цих точках перетину ї є число, яке генерується як випадкове. Для кращого розуміння розглянемо рис. 5, зображено візуалізацію руху математичної точки в більярді Сіная при 12-ти ітераціях.

На рис. 5 видно, що на полі рухаються дві математичні частинки. Це зроблено для порівняння розбіжності їх траєкторій при невеликій різниці початкового кута. Початковий кут частинок відрізняється всього лише на 0,3 градуси. При цьому видно, що така незначна різниця дає дуже велику розбіжність. Це пояснюється високою хаотичністю даного математичного більярду. Тому генератор ключів шифрування на основі такого математичного більярду буде мати високу надійність.

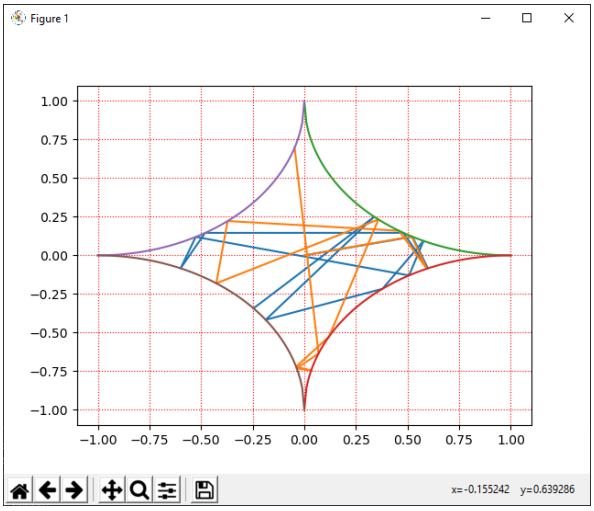

Рисунок 5 – Візуалізація руху математичної точки в більярді Сіная при 12-х ітераціях під час генерації ключа шифрування

Джерело: розроблено автором

На рис. 6 зображено візуалізацію руху математичної точки в більярді Сіная при 200-та ітераціях.

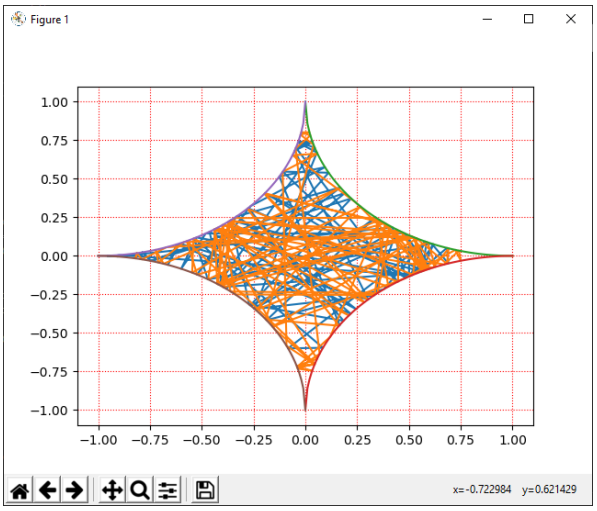

Рисунок 6 – Візуалізація руху математичної точки в більярді Сіная при 200-х ітераціях під час генерації ключа шифрування

Джерело: розроблено автором

При використанні запропонованого методу шифрування через канал зв'язку не передається ніякої інформації про ключі. Початкові параметри ключа записуються на квадрокоптер перед стартом, а ключі генеруються на кожному із пристроїв самостійно на основі початкових параметрів.

Всі програми для мікроконтролерів починаються з ініціалізації. Спочатку треба ініціалізувати тактовий генератор мікроконтролера з вказаними джерелами тактового сигналу, множенням тактового сигналу для ядра та діленням для периферії та системних шин. Після цього ініціалізується потрібна для роботи периферія мікроконтролера. А саме: GPIO – порти вводу виводу, UART – послідовний асинхронний порт та USB – універсальна системна шина.

Зазвичай першими ініціалізують порти вводу виводу (GPIO) [14]. GPIO - general-purpose input output pin або ж порт вводу виводу. Порт вводу виводу – це контакт загального призначення. Може працювати як на вхід так і на вихід. Тобто має можливість або читати логічний стан контакта або навпаки задавати логічний рівень (рівень напруги). Також деякі групи контактів мають можливість працювати в аналоговому режимі при вимірах аналого-цифрового перетворювача (АЦП). Потім треба послідовну шину UART.

UART – це універсальна асинхронна послідовна шина [15]. Шина UART дуже гнучка та дозволяє підключати багато різних пристроїв (мікросхем модулів). Сама шина є повністю дуплексною. Тобто дозволяд передавати данні в обидві сторони як від ведучого пристрою так і від веденого пристрою.

Ініціалізація UART починається з тактування. Після ініціалізації тактування UART необхідно налаштувати контролер NVIC який відповідає за події та вектори переривання.

NVIC (Nested vectored interrupt controller) – модуль контролю переривань [16]. Він виконує наступні функції:

- Дозволяє або забороняє переривання.
- Назначає пріоритет переривань (від 0 до 15. 0 - максимальній пріоритет, 15 - мінімальний пріоритет).
- Автоматично зберігає дані при виконанні одиноких чи вкладених переривань.

При використанні промислового зразка розробленої системи потрібно мати комп'ютерний пристрій, який може передавати цифровий сигнал.

Пристрій повинен бути оснащений засобами Bluetooth, Wi-Fi або радіомодулем. Апаратно програмний модуль як група, що складається з двох об'єктів які пов'язаних між собою або загальним пін кодом або вписаними у програмний код однаковими початковими даними:

– Початкова точка відліку координати по x, y.

– Напрямок куту напрямку руху.

Пристрій повинен бути оснащений модулем RTC, який здійснює синхронізацію прийому та передачі пакетів.

Для захисту прошивки від зчитування хакерами при завантаженні керуючої програми необхідно встановити біт захисту від зчитування. В разі спроби читання програми мікроконтролер очистить всю пам'ять програм.

Перевірка здійснення шифрування та дешефрування виконується за допомогою зовнішнього персонального комп'ютера, через який послідовно за таймером передаються повідомлення однакового змісту від пристрою до пристрою. Після чого повідомлення перевіряються на помилки.

Впровадження у виробництво можливе у декількох варіантах:

- Продаж запрограмованого мікроконтролера з встановленим бітом захисту від

зчитування керуючої програми.

- У вигляді невеликого модуля, який виступає UART – UART мостом.
- У вигляді модуля, який має в собі радіомодуль з підключенням до схеми користувача по UART або USB інтерфейсу.
- У вигляді модуля з аналоговим входом та аналоговим виходом.

Розглянемо функціональну схему варіанта використання у вигляді запрограмованого мікроконтролера з захищеною пам'яттю програми. На рис. 7 зображено функціональну схему МК, який виступає мостом між різними інтерфейсами.

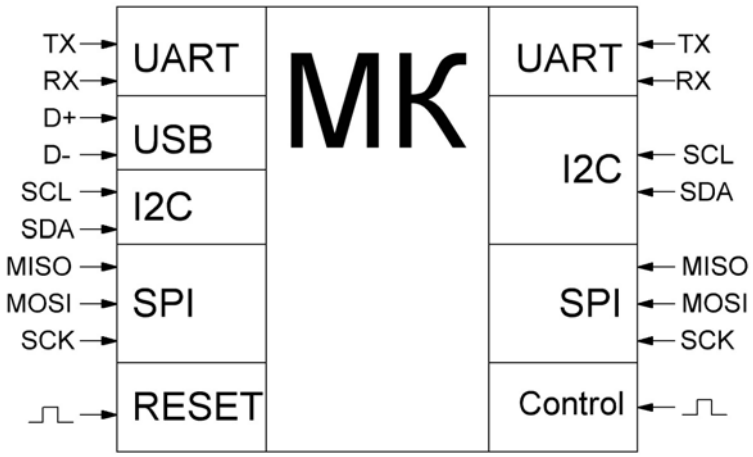

Рисунок 7 – Функціональна схема моста на основі МК

Джерело: розроблено автором

Такий міст повинен шифрувати та розшифровувати трафік даних, який проходить через нього. З рис. 7 видно, що мікроконтролер має декілька вхідних та декілька вихідних інтерфейсів передачі даних. Це дозволяє з легкістю адаптувати мікроконтролер з алгоритмом шифрування у будь-яку систему передачі даних. Також на схемі вказано сигнал контроля, за допомогою якого користувач матиме змогу вибирати потрібні йому інтерфейси. Отже такий варіант виступає у вигляді моста між декількома інтерфейсами. Але якщо користувач потребує одразу здійснити передачу даних через радіоканал, то необхідно використати варіант модуля з МК радіомодуля. Такий варіант одразу передбачає передачу даних між двома пристроями через радіоканал, що на сьогоднішній день є дуже актуальним. Функціональна схема модуля МК з радіомодулем зображена на рис. 8.

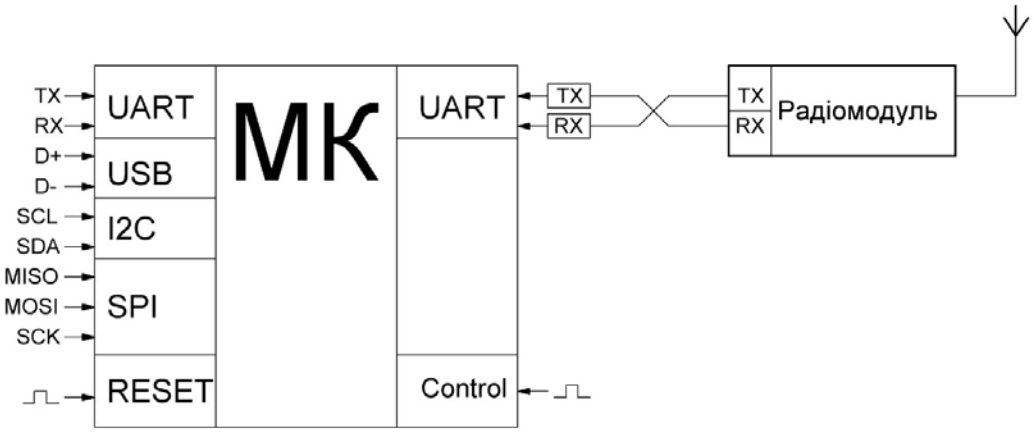

Рисунок 8 – Функціональна схема модуля на основі МК та радіомодуля

Джерело: розроблено автором

Але якщо потрібна шифрована передача даних на основі старих аналогових комунікацій можливий варіант передачі даних через модуль чкий сприймає аналоговий сигнал відцифровує його через аналогово-цифровий перетворювач (АЦП) шифрує та перетворює в аналовий сигнал через цифро-аналоговий перетворювач (ЦАП). Функціональна схема модуля з аналоговим вводом та виводом зображена на рис. 9.

Рисунок 9 – Функціональна схема модуля з аналоговим вводом та виводом
Джерело: розроблено автором

Проведено тестування працездатності розробленого програмного та апаратного забезпечення, що підтвердило можливість його використання у квадрокоптках під час моніторингу сільськогосподарських наземних об'єктів. Було успішно здійснено обмін шифрованими даними між двома пристроями по радіоканалу. Після шифрування на одному пристрої, дані були успішно дешифровані на іншому пристрої.

Висновки. У даній роботі було запропоновано метод шифрування трафіку квадрокоптерів через аналоговий тракт під час моніторингу сільськогосподарських наземних об'єктів.

Розроблене програмне та апаратне забезпечення системи шифрування трафіку квадрокоптера, що дозволяє шифрувати дані, якими квадрокоптер обмінюється з комп'ютером оператора.

Для шифрування даних було використано шифр Вернама. А у якості ключа шифрування псевдовипадкову послідовність, що генерувалася за допомогою математичного більярду Сіная. Було запропоновано покращену математичну модель генерації ключів шифрування на основі більярду Сіная. На основі запропонованої математичної моделі було розроблено програмне забезпечення та створені робочі макети пристроїв для проведення експериментів. Для створення макету обрано модуль на основі мікроконтролера STM32F103C8T6, дані між пристроями передавалися через радіомодуль. Проведено тестування працездатності розробленого програмного та апаратного забезпечення, що підтвердило можливість його використання у квадрокоптках.

Список літератури

1. Agarwal A., Shukla V., Singh R., Gehlot A., Garg V. (2018), "Design and Development of Air and Water Pollution Quality Monitoring Using IoT and Quadcopter", In: Singh R., Choudhury S., Gehlot A. (eds) Intelligent Communication, Control and Devices, Advances in Intelligent Systems and Computing, Vol. 624, Springer, Singapore, DOI: https://doi.org/10.1007/978-981-10-5903-2_49
2. "Unmanned aerial vehicles in agriculture" (2019), Website of the Company "GEOMIR", Modern technologies for agribusiness, URL: https://www.geomir.ru/publikatsii/bespilotniki-v-selskom-khozyaystve/ (in Russian)
3. Duggal V., Sukhwani M., Bipin K., Reddy G.S., Krishna K.M. (2016) "Plantation monitoring and yield estimation using autonomous quadcopter for precision agriculture", IEEE International Conference on Robotics and Automation (ICRA), pp. 5121-5127, doi: 10.1109/ICRA.2016.7487716, URL:https://ieeexplore.ieee.org/abstract/document/7487716
4. Zubarev Ju.N., Fomin D.S., Chashhin A.N., Zabolotnova M.V. (2019), "The use of unmanned aerial vehicles in agriculture", Bulletin of the Perm Federal Research Center, №2. URL:

https://cyberleninka.ru/article/n/ispolzovanie-bespilotnyh-letatelnyh-apparatov-v-selskom-hozyai-stve (in Russian)
5. Главное о безопасности дронов. *Веб-сайт фирмы «Лаборатория Касперского»*. URL: https://www.kaspersky.ru/resource-center/threats/can-drones-be-hacked (дата обращения: 27.10.2021)
6. Eastlake, D.E., Schiller, J.I., & Crocker, S. (2005). Randomness Requirements for Security. RFC, 4086, 1-48.
7. Barker, E. and Kelsey, J. (2015), Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-90Ar1 (Accessed November 29, 2021)
8. Sinai Y.G. Dynamical systems with elastic reflections . *Russian Mathematical Surveys*.1970. Vol. 25, no. 2. Pp. 137-189.
9. Ганапольский Е.М. О природе квантового хаоса в рассеивающей бильярдной К-системе . *Доповіді Національної академії наук України*. 2012. № 3. С. 85-91.
10. Собінов О.Г. Простий генератор псевдовипадкової послідовності . *Інформаційні технології та комп'ютерна інженерія*: зб. тез доп. наук.-практ. конф., м. Кіровоград, 4 груд. 2014 р. Кіровоград: КНТУ, 2014. С. 184.
11. STM32CubeIDE. URL: https://www.st.com/en/development-tools/stm32cubeide.html.
12. STM32F103C8 . URL: https://www.st.com/en/microcontrollers-microprocessors/stm32f103c8.html.
13. JDY-40 2.4G wireless serial port transmission transceiver and remote communication module . URL: https://sunhokey.cn/collections/wifi-module/products/jdy-40-2-4g-wireless-serial-port-transmission-transceiver-and-remote-communication-module.
14. GPIO internal peripheral . URL: https://wiki.st.com/stm32mpu/wiki/GPIO_internal_peripheral.
15. AN2582 Application note. URL: http://read.pudn.com/downloads106/sourcecode/embed/437624/stm32/STM32F Documents/Application Note/STM32F10xxx USART application examples.pdf.
16. Nested Vectored Interrupt Controller (NVIC) . URL: http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.dai0179b/ar01s01s01.html

Referencis

1. Agarwal A., Shukla V., Singh R., Gehlot A., Garg V. (2018). "Design and Development of Air and Water Pollution Quality Monitoring Using IoT and Quadcopter", In: Singh R., Choudhury S., Gehlot A. (eds) Intelligent Communication, Control and Devices, Advances in Intelligent Systems and Computing, Vol. 624, Springer, Singapore, DOI: https://doi.org/10.1007/978-981-10-5903-2_49 [in English].
2. "Unmanned aerial vehicles in agriculture" (2019), Website of the Company "GEOMIR", Modern technologies for agribusiness. *www.geomir.ru*. Retrieved from https://www.geomir.ru/publikatsii/bespilotniki-v-selskom-khozyaystve/ [in Russian]
3. Duggal V., Sukhwani M., Bipin K., Reddy G.S., Krishna K.M. (2016). "Plantation monitoring and yield estimation using autonomous quadcopter for precision agriculture", IEEE International Conference on Robotics and Automation (ICRA), pp. 5121-5127, doi: 10.1109/ICRA.2016.7487716. *ieeexplore.ieee.org*. Retrieved from https://ieeexplore.ieee.org/abstract/document/7487716 [in English].
4. Zubarev Ju.N., Fomin D.S., Chashhin A.N., Zabolotnova M.V. (2019). "The use of unmanned aerial vehicles in agriculture", Bulletin of the Perm Federal Research Center, №2. *cyberleninka.ru.* Retrieved from https://cyberleninka.ru/article/n/ispolzovanie-bespilotnyh-letatelnyh-apparatov-v-selskom-hozyai-stve [in Russian].
5. Glavnoe o bezopasnosti dronov. Veb-sajt firmy «Laboratorija Kasperskogo» [The main thing about the safety of drones. Website of Kaspersky Lab]. *www.kaspersky.ru.* Retrieved from https://www.kaspersky.ru/resource-center/threats/can-drones-be-hacked
6. Eastlake, D.E., Schiller, J.I., & Crocker, S. (2005). Randomness Requirements for Security. RFC, 4086, 1-48 [in English].
7. Barker, E. and Kelsey, J. (2015). Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-90Ar1 (Accessed November 29, 2021) [in English].
8. Sinai, Y.G. (1970). Dynamical systems with elastic reflections . *Russian Mathematical Surveys, Vol. 25*, *2,* 137-189. [in English].
9. Ganapol'skij, E.M. (2012). O prirode kvantovogo haosa v rasseivajushhej bil'jardnoj K-sisteme [On the nature of quantum chaos in a scattering billiard K-system]. *Dopovidi Nacional'noï akademiï nauk Ukraïni – Reports of the National Academy of Sciences of Ukraine.].* 2012. № 3. S. 85-91.

10. Sobinov, O.H. (2014). Prostyj henerator psevdovypadkovoi poslidovnosti [A simple pseudo-random sequence generator*]. Information technology and computer engineering: naukovo-praktychna konferensia. (4 hrud. 2014 r.) – Scintific and Practical Conference*. (pp. 184). Kirovohrad: KNTU [in Ukrainian].
11. STM32CubeIDE . *www.st.com.* Retrieved from https://www.st.com/en/development-tools/stm32cubeide.html. [in English].
12. STM32F103C8 . *www.st.com*. Retrieved from https://www.st.com/en/microcontrollers-microprocessors /stm32f103c8.html [in English].
13. JDY-40 2.4G wireless serial port transmission transceiver and remote communication module . *sunhokey.cn.* Retrieved from https://sunhokey.cn/collections/wifi-module/products/jdy-40-2-4g-wireless-serial-port-transmission-transceiver-and-remote-communication-module [in English].
14. GPIO internal peripheral . *wiki.st.com.* Retrieved from https://wiki.st.com/stm32mpu/wiki /GPIO_internal_peripheral [in English].
15. AN2582 Application note . *read.pudn.com.* Retrieved from http://read.pudn.com/downloads106/sourcecode /embed/437624/stm32/STM32F Documents/Application Note/STM32F10xxx USART application examples.pdf [in English].
16. Nested Vectored Interrupt Controller (NVIC) . *infocenter.arm.com.* Retrieved from http://infocenter.arm.com/help /index.jsp?topic=/com.arm.doc.dai0179b/ar01s01s01.html [in English].

Yelyzaveta Meleshko, Prof., DSc., **Oleksandr Maidanyk,** Master student, **Oleksandr Sobinov,** lecturer, **Roman Mynailenko,** Assoc. Prof., PhD tech. sci.
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

A Method of Encrypting the Traffic of Quadrocopters Through an Analog Path During Monitoring of Agricultural Ground Objects

The purpose of this work to developed a method for encrypting the traffic of quadcopters through an analog path throughout the monitoring of agricultural ground objects.

The use of unmanned aerial vehicles of a quadrocopter type for monitoring ground objects in agriculture is becoming more and more common practice and allows you to effectively solve a wide range of tasks. Technologically equipped drones in agriculture are capable of performing various monitoring operations, in particular: aerial photography, video filming, thermal filming, laser scanning, etc. Such monitoring makes it possible to assess the quality of crops and identify the fact of damage or death of crops, identify crop defects and problem areas, analyze the effectiveness of plant protection measures, check compliance with crop rotation plans, identify deviations and violations in the process of agrotechnical work, analyze the relief and create maps, conduct audit and inventory of land, carry out security measures and collect information for the security service, etc.

At the same time, drones are vulnerable to information attacks, which can be carried out for different purposes, in particular, to steal a drone, use it in a network of bots to attack other devices, or to intercept information that it collects for a device operator. All this necessitates the development of effective methods of information protection of drones from cyberattacks.

In this work, the Vernam cipher was used to encrypt the data, and a pseudo-random sequence generated using the Sinai mathematical billiard was used as the encryption key. Thus, an improved mathematical model for generating encryption keys based on the Sinai billiards has been proposed. On the basis of the proposed mathematical model, software was developed and working models of devices for conducting experiments were created. To create a layout, a module based on the STM32F103C8T6 microcontroller was selected, data between devices was transmitted via a radio module.

encryption, key generation, traffic, quadcopter, analog path, monitoring, agricultural ground objects

Одержано (Received) 30.10.2021 *Прорецензовано (Reviewed) 16.11.2021*
Прийнято до друку (Approved) 29.11.2021