ЗАХИСТ ІНФОРМАЦІЙНОГО КАНАЛУ БПЛА ВІД ЗОВНІШНІХ ПРОГРАМНО-АПАРАТНИХ ВПЛИВІВ

Кириченко В.В., Лесіна Є.В.,
Національний авіаційний університет,
Красноармійський індустріальний інститут ДВНЗ "ДонНТУ"

Анотація. Сучасні безпілотні літальні апарати (БПЛА) знаходять широке застосування не тільки у військовій справі, а й у цивільному секторі. Їх все частіше застосовують для вирішення таких народногосподарських завдань, як аерофотозйомка, метеорологічні вимірювання, контроль стану трубопроводів, ліній електропередач і т.д. Разом з тим стає актуальним ряд проблем, пов'язаних з інтенсивним розвитком даного напрямку, зокрема, закриття телекомунікаційних каналів зв'язку з БПЛА для їх захисту від зовнішніх програмно апаратних впливів. У цьому дослідженні проаналізовано питання закриття каналу зв'язку з безпілотним літальним апаратом криптографічними засобами. Сформульовано вимоги, що пред'являються до таких засобів. Розроблений програмний комплекс, який реалізує один з можливих алгоритмів криптографічного захисту передачі сигналів з борта БПЛА на пульт дистанційного керування. В алгоритмі застосовуються зворотні динамічні системи управління зі складною поведінкою траєкторій.

Ключові слова: інформаційний канал БПЛА, зворотні динамічні системи, кінцевовимірне кільце цілих чисел, генератори псевдовипадкових послідовностей.

PROTECTION OF THE UAV INFORMATION CHANNEL FROM EXTERNAL SOFTWARE AND HARDWARE EFFECTS

Kirichenko V., Lesina Ye.
National Aviation University,
Krasnoarmeysk industrial institute of DonNTU

Abstract. The present study has analyzed the issues of closing the communication channel with unmanned aerial vehicles by cryptographic means. The requirements applicable to such means have been defined. The developed software package realizes one of the possible algorithms of cryptographically secured transmission of broadband video signals from the UAV board to the Ground. The idea of using inverse control systems with complex behavior of trajectories is at the heart of the objective to synthesize new efficient algorithms of information protection, primarily from the unauthorized access. This work analyses the issues of closing the communication channel with an unmanned aerial vehicle by using cryptographic means. Requirements applicable to such means are formulated. The method of information encryption envisaging use of direct and reverse dynamical systems is considered. There has been carried out a series of experiments on information conversion with the encryption-decryption system that showed some algorithm features based on the above mentioned systems.

Key words: Information UAV channels, inverse dynamic system, finite-dimensional ring of integers, generators of pseudo-random sequences.

Вступ. На сьогоднішній день більшість існуючих безпілотних літальних апаратів пілотуються вручну, за допомогою пультів дистанційного керування, що працюють на радіоканалах. При ручному управлінні БПЛА виникають труднощі, пов'язані з підготовкою пілотів, недостатньою робочою дальністю, обмеженнями, які викликані погодними умовами. Особливої гостроти набувають питання інформаційної безпеки, зокрема, закриття телекомунікаційних каналів зв'язку з літальним апаратом. Атаки можуть бути спрямовані на перехоплення управління, виведення з ладу БПЛА, отримання розвідувальної інформації або для подальшої атаки на пілота-оператора і взаємодіючі з ним системи.

Мета роботи – проаналізовано питання закриття каналу зв'язку з безпілотним літальним апаратом криптографічними засобами, з використанням зворотних динамічних систем. Сформулювати вимоги, що пред'являються до таких засобів.

Постановка задачі. Динамічні системи, що володіють хаотичним поведінкою, в даний час інтенсивно використовуються і застосовуються в різних областях, зокрема, для криптографічного захисту інформації. На основі таких систем можуть бути побудовані генератори псевдовипадкових послідовностей, які в подальшому використовуються для кодування відкритих сигналів.

Як спосіб шифрування інформації виберемо спосіб її безпосереднього перетворення за допомогою динамічної хаотичної системи, що використовує пряму і зворотну системи Чуа.

Пряма:

$$\begin{cases} \dot{x}_1 = A_1(A_2(x_2 - x_1) - (x_1 + 1)), \\ \dot{x}_2 = A_3(A_2(x_1 - x_2) - x_3 + Av_{in}), \\ \dot{x}_3 = A_4(x_2 - A_5 x_3). \end{cases}$$

Зворотна:

$$\begin{cases} \dot{x}'_1 = A_1(A_2(x'_2 - x'_1) - (x'_1 + 1), \\ v_{out} = \frac{1}{A}(\frac{1}{A_3}\dot{x}_2 - A_2(x'_1 - x'_2) + x'_3, \\ \dot{x}'_3 = A_4(x'_2 - A_5 x'_3). \end{cases} \quad (1)$$

Тут v_{in} та v_{out} – вхідні сигнали прямої та зворотної систем відповідно. Компоненти $x_i(t)$, $i = 1,2,3$, множини вхідних та вихідних символів, розуміються як елементи кінцевого поля $GF(q)$ або кільця $Z(q)$, а операції додавання і множення є відповідні операції в цьому полі або кільці. Для цифрової обробки інформації застосовуються, як правило, поля або кільця характеристики 2, тобто $q = 2^n, n \in N$. З огляду на особливості подання інформації в пам'яті комп'ютера, в програмі використовуються поля $GF(2^{8k})$, або кільця $Z(2^{8k})$, k = 1,2,3,4.

Вирішення задачі. Для дослідження отриманої псевдовипадкової послідовності чисел є дві групи тестів – графічні та оціночні. На малюнку 1 показані результати шифрування періодичного сигналу з використанням автомата Чуа (1) в кінцевому кільці $Z(2^8)$.

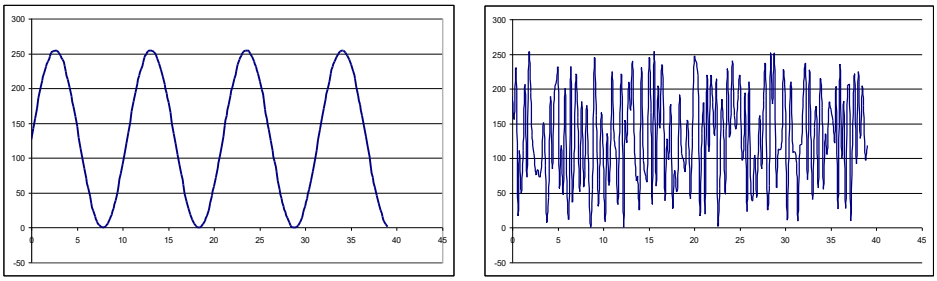

Рис. 1. Вхідний періодичний та зашифрований за допомогою системи Чуа сигнал

Висновок. Будь-яку керовану динамічну систему, що має структуру вхід-вихід, можна використовувати безпосередньо для перетворення інформації. Ідея застосування зворотних систем управління зі складною поведінкою траєкторій лежить в основі завдання синтезу нових ефективних алгоритмів захисту інформації, в першу чергу, від несанкціонованого доступу. Проведені дослідження і їх оцінка дозволяють стверджувати, що отримані нові результати, що розширюють теоретичну базу сучасної криптології і є перспективними для створення ефективних криптографічних алгоритмів.

Список використаних джерел

1. Kirichenko V. V. Information security of communication channel with UAV // Electronics and control systems. – N 3(45), 2015. – P. 23-27.

2. Обобщенная обратимость динамических систем в задачах шифрования / Ковалев А.М., Козловский В. А., Щербак В. Ф. – ПДМ, 2009, приложение № 1. – С. 20–21.

3. Sobhy M. J. and Shehata A. Secure computer communication using haotic algorithms. Int. J. of Bifurcation and Chaos. vol. 10, no. 12, 2000, pp. 2831–2839.