ПРОБЛЕМА УЯЗВИМОСТИ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ МЕЖДУ БПЛА И НАЗЕМНЫМ КОМПЛЕКСОМ УПРАВЛЕНИЯ

Кириченко В. В.

Национальный авиационный университет, Киев, Украина.

Современные беспилотные летательные аппараты (БПЛА) находят широкое применение не только в военном деле, но и в гражданском секторе. Их все чаще применяют для решения таких народнохозяйственных задач, как аэрофотосъемка, метеорологические измерения, контроль состояния трубопроводов, линий электропередач и др. Наблюдаемый в мире бум использования беспилотной авиации в последнее время объясняется очевидными преимуществами таких устройств – низкой стоимостью, экономичностью, простотой эксплуатации и безопасностью обслуживающего персонала.

Особую остроту приобретают вопросы информационной безопасности, в частности, закрытие телекоммуникационных каналов связи с БПЛА. Проблема уязвимости каналов передачи данных между БПЛА и наземным комплексом управления, в качестве которого чаще всего используется планшетный компьютер или ноутбук, решается одним из следующих способов [1]:

- применение автономных БПЛА;
- использование спутниковых ретрансляторов;
- применение криптографических средств.

В большинстве применений наиболее приемлемым и экономичным является последний из перечисленных вариантов.

При оценивании требований, предъявляемых к системе защиты канала связи криптографическими методами, можно выделить такие аспекты как: быстродействие, надежность шифрования, массогабаритные показатели бортовой части системы. Данные факторы вступают в противоречие между собой, особенно при повышенных требованиях к пропускной способности канала и небольшой массе БПЛА.

На выбор алгоритма шифрования влияет ряд факторов, как организационных (в частности, вопросы сертификации), так и технических, среди которых важным моментом является реализуемость на имеющейся элементной базе.

Данная работа посвящена разработке программно-моделирующего алгоритма шифра, обеспечивающего скоростное поточное криптографическое преобразование широкополосных сигналов, передаваемых с борта БПЛА. В последнее время формируется новое направление в криптологии, которое связано с использованием динамических систем с хаотическим поведением. Один из основных подходов в данной области, основан на использовании обратных систем управления для построения криптографических алгоритмов [2].

Динамические системы, обладающие хаотичной поведением, в настоящее время интенсивно используются и применяются в различных областях, в частности для криптографической защиты информации. На основе таких систем могут строиться генераторы псевдослучайных последовательностей, которые в дальнейшем используются для кодирования открытого текста. С другой стороны всякая динамическая система, имеющая структуру вход-выход, может использоваться непосредственно для преобразования информации. На основе таких систем создается шифратор. Входом в систему служит оцифрованное сообщение, а выходом является зашифрованный сигнал, направленный в телекоммуникационные сети. Необходимым условием для однозначной дешифровки является существование обратной системы.

Алгоритм шифрования, используемый в данной работе, основанный на использовании дискретного аналога динамической хаотической системы Лоренца [3]. Конечный автомат Лоренца описывается системой уравнений:

$$\begin{cases} x_1(t+1) = x_1(t) + hA_1(x_2(t) - x_1(t)), \\ x_2(t+1) = x_2(t) + h(A_2 x_1(t) - x_2(t) - \\ \qquad - x_1(t)x_3(t) + Au(t)), \\ x_3(t+1) = x_3(t) + h(x_1(t)x_2(t) - A_3 x_3(t)), \end{cases}$$

$$y(t) = x_2(t) + h(A_2 x_1(t) - x_2(t) - x_1(t)x_3(t) + Au(t))$$

Здесь аддитивная составляющая – текущий входной символ исходной информации $u(t)$. $y(t)$ – соответствующий символ зашифрованной информации. Множества входных и выходных символов, компоненты $x_i(t),\ i = 1,2,3$ понимаются как элементы конечного поля $GF(q)$ или кольца $Z(q)$, а операции сложения и умножения есть соответствующие операции в этом поле, или кольце.

В настоящем исследовании проанализированы вопросы закрытия канала связи с беспилотным летательным аппаратом криптографическими средствами. Сформулированы требования, предъявляемые к таким средствам. Разработанный программный комплекс реализует один из возможных алгоритмов криптографически защищенной передачи широкополосных видеосигналов с борта БПЛА на Землю.

ЛИТЕРАТУРА

1. Моисеев В. С. Прикладная теория управления беспилотными летательными аппаратами: монография. – Казань: ГБУ «Республиканский центр мониторинга качества образования» (Серия «Современная прикладная математика и информатика»). – 768 с.

2. Kirichenko V.V. Using inverse control systems for encoding and transmission // The problems of global communication, navigation, surveillance and air traffic management CNS/ATM / Abstracts of Scientific and Technical Conference. (November 17, 2014, Kyiv).– P. 139.

3. Kirichenko V.V. Information security of communication channel with UAV // Electronics and control systems. – 2015. – 45, №3. – P. 23–27.