6. Брескін В.О., Розенвассер Д.М. Система прийому дискретних парціально кодованих сигналів з амплітудною модуляцією. – Патент на корисну модель № 89073 від 10.04.2014.

7. Брескін В.О., Розенвассер Д.М. Система прийому дискретних парціально кодованих сигналів з квадратурною амплітудною модуляцією. – Патент на корисну модель № 90004 від 12.05.2014.

8. Хэмминг Р.В. Теория кодирования и теория информации / Хэмминг Р.В.: Пер. с англ. – М.: Радио и связь, 1983. – 176 с.

Венідіктов О.В., Шмельова Т.Р.
ОНАЗ ім. О.С. Попова

EFFICIENCY ANALYSIS OF UAV AND COMMUNICATION DEVICES

Abstract. In this paper Unmanned Aerial Vehicle were classified. Main application goals of UAV were defined. The technical problems of the UAV were investigated. Closings of a communication channel with the UAV cryptographic means were analyzed. According to this problem efficiency solutions were find out.

An unmanned aerial vehicle (UAV) [1], commonly known as a drone, as an unmanned aircraft system (UAS), or by several other names, is an aircraft without a human pilot aboard. The flight of UAVs may operate with various degrees of autonomy: either under remote control by a human operator, or fully or intermittently autonomously, by onboard computers.

When it comes about quadcopters, most of us imagines the device with enough modest characteristics – it is rather a toy on radio control, than something, worthy names "unmanned aerial vehicle". The modern professional UAVs with four rotors very strongly differ from amateur toys. They are capable to fly under a pouring rain, in a frost and a heat, they can hold on in air about an hour, and will be able to control them even child. These, and also other properties of this technique can't remain unnoticed among military experts. Top Consumer Drone Manufacturers are: DJI Innovations, Parrot, 3D Robotics, Hubsan, Blade.

Experts select the main existing and perspective objectives for the UAV [2], classification by mission is presented in table 1.

Table 1 – Classification UAV by mission

Prospecting tasks	Fire (shock) tasks	The providing tasks
– investigation of the terrestrial purposes; – investigation of air targets and, as variety, investigation of the ballistic purposes (warheads of ballistic missiles), in case of application as a part of systems of missile defense; – investigation of the sea purposes; – terrain investigation (as variety – investigation of mines and minefields); – radiation, chemical and biological survey; – investigation of weather (weather reconnaissance); – radio and radio engineering investigation.	– striking blows on the terrestrial purposes; – striking blows on the sea purposes; – defeat of elements of air – defense systems (first of all radar stations); – fight against air targets; – destruction of warheads of ballistic missiles in case of application as a part of systems of missile defense.	– setting of noises of radio - and to radio engineering means of the opponent, execution of other tasks of radio-electronic fight; – fire control and target indication to terrestrial, air and sea fire weapons; – assessment of results of the blows struck to the opponent; – relaying of messages and data; – transport tasks.

Technical problems. Now there is a row the technical problems constraining development of the UAV. Biggest problem of ensuring transfer information on channels is essential communications between "UAV" and ground station of management in demanded volume, with the set speed and without distortion. This problem is solved by increase in capacity and a noise stability of channels information transfers.

Problem of vulnerability of transmission channels between the UAV and terrestrial complex of control, as most of which often the tablet computer or notebook is used, is solved one of following methods:

- use of independent UAVs;
- use of satellite repeaters;
- closing of the communication line with cryptographic means.

In the majority of applications and economic the last from the listed options is the most acceptable. From the classification given above it is visible that the circle of the tasks solved by the UAV is quite wide. Requirements imposed to communication channels in general including means of closing of information, also vary over a wide range.

At estimation of requirements imposed to system of protection of a communication channel by cryptographic methods it is possible to mark out such aspects as: speed, reliability of enciphering, mass-dimensional indicators onboard part. These factors conflict among themselves especially at increased requirements to the capacity of the channel and small mass of the UAV.

Application of the most resistant encryption algorithms accepted as state standards for closing of communication links which are based preferentially on a sequential method of data transfer (bits on bit) encounters on the basic restriction connected to the fact that the mentioned ciphers belong to the class of algorithms of so-called block symmetric encryption. Below this problem is considered on the example of closing with an algorithm of one most widespread communication RS-232 interfaces.

Encoding of the RS-232 interface GOST 28147-89 algorithm. The communication packet transferred according to the RS-232 [5] protocol depending on settings can have length from 9 to 11 bits. From them 8 bits (in the majority of applications) are information, that is bearing payload capacity, remaining – official .

According to an algorithm [3] information which is subject to closing are grouped on 8 bytes (64 bits). The same size has the ciphered block at the exit. Therefore, the bits accepted on the consecutive channel need to be kept in the buffer memory device, and after processing by a cryptoalgorithm to transform to a consecutive form again. As a result, to the highway of transfer information the scheme of enciphering brings the delay depending on the set algorithm, speed of the ciphering device and the chosen speed transfers of the communication channel. Let's estimate the size.

The complete time delay resulting from execution of the procedure of closing of information in case of data transfer in one side including operations of enciphering and deciphering, in case of use of arbitrary algorithm is determined by a formula:

$$T_{f=}T_{E+}T_{d}\,, \tag{1}$$

where T_E and T_d – according to the delay of enciphering and deciphering equal:

$$T_{E=}T_{d=}(2T_{tr}+T_{c}), \tag{2}$$

where T_{tr} – time of transformation of the block of data from consecutive in a parallel code or back; T_c – enciphering/deciphering time.

Time of transformation is defined as:

$$T_{tr}=N_b*(N_u+N_{cb})*T_c\,, \tag{3}$$

where N_b – the number of bytes in the block for the set algorithm;

N_u – the number of useful (information) bits in a communication package;

N_{cb} – the number of control bits in a communication package (starting. stop. parity bit);

T_{cr} – the period of clock rate inversely proportional the selected transmission rate.

Making all substitutions, we receive:

$$T_{\downarrow}f = 2(2(N_{\downarrow}b\ (N_{\downarrow}u + N_{\downarrow}cb\ )\ T_{\downarrow}cr\ ) + T_{\downarrow}c\ ). \quad (4)$$

According to a tabl. 2 we can find a value of a complete time delay.

Table 2 – Value of a complete time delay

Speed [Baud]	Max. Length [meters]
19 200	15
9 600	150
4 800	300
2 400	900

The Baud is a unit of measure of symbolical speed, the number of changes of information parameter of the bearing periodic signal in a second. Emile Baudot, the inventor of a code Baudot of the coding of symbols for teletypes is called by name. Translation of unit baud: 1 baud = 0.8 bits/sec.
In case of use in the RS-232 protocol of eight information bits, one start, one stop, without monitoring of parity, transmission rate of 7680 bits/sec. and the encryption algorithm state standard specification [3] (the unit size – 8 bytes), value of a complete time delay in case of information transfer in one side it is equal:

$$T_f = 2\left(2\left(8 * 10 * \frac{1}{7680}\right) + T_c\right) = 2(0{,}0208+T_c). \quad (5)$$

Therefore, even if time of enciphering will be negligible, the ineradicable delay in the communication channel for the set speed and the chosen algorithm will make not less than 33 ms. It is necessary to notice that application of an algorithm will lead to twice bigger ineradicable delay as block length in this case will make 16 bytes (128 bits).

The proposed solution:

1. On the basis of the above we will formulate requirements imposed to system of protection of a communication channel.

2. The hardware shall consist, at least, of two parts – terrestrial and onboard.

3. For decrease in a delay the greatest possible speed of realization of a cryptoalgorithm has to be provided.

4. Onboard part has to have the minimum weight and dimensions, to consume an energy minimum.

5. Land part has to be joined conveniently to land complex of management, provide functions of a configuration and control.

6. In general the system has to differ in the low cost of development, production and operation.

Conclusion. The main application of UAV are: industrial, ecology, aviation, military and so on. The main technical problem is ensuring transfer information on channels is essential communications between "UAV" and communication device. The solutions of problems defined by technical and communication channel means. In the research analyzed closings of a communication channel with the UAV cryptographic means. The problem connected to origin in the channel of sequential data transfer of a temporal time delay which value can't be made less value in case of application of the most known and the algorithms of block checked by time is revealed the symmetric encoding.

References

1. Marco Lukovic, The Future of Military UAS in Europe A Market Perspective. Proceedings Unmanned Air Systems'09

2.http://aviapanorama.narod.ru/journal/2005_4/bpla.htm

3.Книга: Шнайер Б.: Прикладна криптографія | частина = 14.1 Алгоритм ГОСТ 28147-89 | сторінки = 373–377

4.UAS: The Global Perspective. Yearbook 2008/2009

5."RS232 Tutorial on Data Interface and cables". ARC Electronics. 2010. Retrieved 28 July 2011.

Главацкий С.П.
ОНАС им. А.С. Попова

ИССЛЕДОВАНИЕ ВНЕДРЕНИЯ IPV6

Аннотация. Основной проблемой развития сети Интернет, является проблема исчерпания адресного пространства IPv4. Существуют решения продлевающие время использования IPv4, однако дальнейшее развитие узлов сети Интернет возможно только при переходе на IPv6. В настоящий момент не существует централизованного механизма перехода сети Интернет на адресное пространство IPv6. Каждый оператор доступа и администрации сайтов самостоятельно решают вопросы внедрения IPv6.

Для взаимодействия сетевых узлов в сети Интернет широко используется протокол IPv4. Стремительный рост Интернет привел к проблеме исчерпания адресов IPv4 [1,2]. За время использования протокола IPv4 в нем так же были выявлены и другие недостатки связанные со слабой расширяемостью протокола, проблемами безопасности, отсутствие механизмов качества обслуживания и относительно высокие накладные расходы обработки пакетов маршрутизатором. Для решения этих недостатков был разработан протокол IPv6.

С момента создания IPv6 прошло уже 20 лет, однако степень внедрения и использования IPv6 в сети Интернет в Украине и мире пока незначительна. Брокеры IPv6 [3] позволяют пользователям получить адрес IPv6 через точки присутствия и являются лидерами по внедрению IPv6.

Для проведения исследования о степени внедрения IPv6 в украинском и мировом сегменте сети Интернет были использованы статистические данные специализированных ресурсов по внедрению IPv6 фирм CISCO [4] и Google [5]. Данные ресурсы собирают статистические данные пользователей, посетивших их ресурсы и заслуживают доверия. Так согласно данным фирмы Google, количество пользователей сети Интернет, обладающих IPv6-адресами в мире составляет, на момент написания статьи, около 11-13%, в Украине же – 0.23%. Динамика темпов роста использования пользователями IPv6 в мире показана на рис. 1.

Ресурс фирмы CISCO для анализа степени внедрения и использования IPv6-адресов использует более расширенные параметры, такие как:

– Prefixes – Количество анонсированих и доступных по всему миру префиксов IPv6;
– Transit AS – Количество транзитных сетей поддерживающих IPv6;
– Content – Среднее количество посещаемых сайтов, адаптированных к IPv6;
– Top500 – Количество сайтов с поддержкой IPv6 из рейтинга Alexa top 500;
– Users – Количество пользователей IPv6;
– Relative Index – Усредненная оценка внедрения IPv6, от 0 до 10.