UDC 004.312; 004.89; 621.391.825 (045)

[1]V. M. Sineglazov,
[2]O. Yu. Tkachenko

INTELLECTUAL TWO-LEVEL SYSTEM OF ELECTRONIC WARFARE WITH UAVs

Aviation Computer-Integrated Complexes Department, National Aviation University, Kyiv, Ukraine
E-mails: [1]svm@nau.edu.ua, [2]ElenaTkachenko@bigmir.net

Abstract*—*This work represents an algorithm of development of broadband interference source for the unmanned aerial vehicles. The configuration of device is implemented by an intellectual unit, which provides remote turn-on of the generators that ensures a pulsed mode of the system.

Index Terms—Unmanned aerial vehicles; electronic warfare; Joint Precision Airdrop Systems; jammer.

I. Introduction

Currently, unmanned aerial vehicles (UAVs) are the efficient means of intelligence, allowing identifying the target and transmitting necessary information to a central control point (informational radio channel). As a rule, all UAVs used for solving these problems have remote control channel (command radio channel) that is, belong to the class of remotely piloted vehicles (RPV). The remote control of UAVs carried out through command radio channel (from manual control unit to the control unit of the autopilot), which consists of a CAN-channel controller, radiomodem and dual mode antenna. Data are transmitted via information radio channel, which includes radiomodem and dipole antenna.

To solve the UAVs navigation problems are actively use GPS channel during its movement.

Thus it is necessary to effectively work of EW suppress three radio channels: command, information and GPS.

Fight with GPS channel is possible by implementing spoofing.

II. Problem Statement

Develop a method of constructing a system of electronic warfare (EW) ensure the impossibility of functioning of command and information radio channel of the UAV. Form interference of given frequency and power at the course of motion of the aircraft.

It is necessary to develop a broadband source of interference for the UAV with further the practical application and the ability to create a working device.

The aim is to develop a system of EW, provides suppression of:

– command radio channel;

– information radio channel;

– GPS channel / implementation of spoofing.

During realization of this goal solves the following tasks:

– detection of UAVs;

– determination of the course of the UAV;

– determination of the frequency operation of command and information radio channels.

III. Review of Existing Solutions

Among the known EW systems should note the following.

In order to combat UAVs used means of electronic warfare, which provide blocking of information channels of intelligence, communication, control and guidance systems armament and military equipment by creating a sufficient level of electromagnetic interference power spectral characteristics of which should be optimized for the specific signals of information channels to be controlled [1].

We know about the development of advanced systems capable of striking modern unmanned aerial vehicles of different classes. According to some reports, overseas is being created of microwave's emitters capable "burn" the electronics of the aircraft. This technique in the future will be able to send to the enemy UAV an electromagnetic pulse, the power of which will incapacitate its electronics. As a result, the UAV remains intact relatively, but is not able to continue execution of its task.

In the context of the destruction or damage of modern UAVs is possible to recollect the old Soviet developments. In the eighties, was being tested a laser-propelled complex "Sanguine" designed to incapacitate optoelectronic systems of enemy equipment. According to available data, the complex "sanguine", built on the basis of self-propelled anti-aircraft "Shilka" could incapacitate optoelectronic system at a distance of 10 km. At distances of 8…10 km ensured the destruction of light-sensitive elements of the target hardware. Thus, the complex "Sanguine" could be used against modern light and medium UAVs, for a while "blinding" or destroying their electro-optical surveillance system [2].

Meanwhile, the American company SRC in October 2012 at the AUSA conference in Washington showed the layout of its products, called Vigilant Falcon. In the company declined to give details on the system, but noted that it is based on existing systems developed by SRC, which are able to detect and track potential threats, to ensure "the visual and electronic identification, and provide opportunities for electronic jamming".

In the company SRC declare that the system offers "several modes of suppression", but not specifying what, simply referring to non-kinetic means of electronic warfare defeat. Presumably, this is some form of communication channels or controls jamming UAVs [3].

To solve the problems of flight control, observation of the underlying surface in real time during flight, a digital photograph of the selected terrain sectors, including hard to reach areas, determining the coordinates examined terrain, as well as for storage of information with its subsequent transmission to the customer (in addition, possible to transmit information in real time) to the onboard equipment of modern UAVs must include the following devices and systems:

– a signal receiver Navigation Satellite System (GLONASS / GPS);

– devices receiving of species information;

– radio line reception and transmission of telemetry data and of species;

– command and navigation radio line with antenna-feeder device;

– the unit of exchange command information;

– the unit of information exchange;

– the storage device (accumulation) imagery.

An important vulnerable link in managing UAVs is the need to maintain a constant exchange of information with ground control. A large amount of transmitted data requires quite active, intensive radio channels for which it is very difficult (almost impossible in the present conditions) to provide the required secretive operation and high reliability. Explored the frequency of the communication channels UAVs with ground control available jammers, it is possible to operate these communication channels to score suppresses noises. Figure 1 shows an example of the construction of such a system

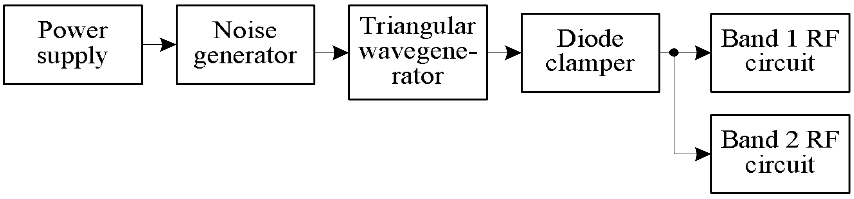

Fig. 1. Block diagram of the system jamming UAVs

The creation of "umbrella" of radio electronic interference to navigation systems, flight control, communication channels, radio lines reception and transmission of information, and others. Above the battlefield (theater of war) can lead to significant reduction in the effectiveness of combat employment or complete neutralization of the UAV [4].

Holding company "Ukrspetstechnika" military-industrial complex of Ukraine has developed a set of jamming GPS and "GLONASS" called "Enclave".

Suppression equipment navigation receivers consumer satellite navigation systems designed to create a sighting frequency interference consumer navigation equipment systems GPS / GLONASS.

The new complex is designed primarily to deal effectively with unmanned aerial vehicles. Its operation is quite simple – the device interferes with navigation equipment that uses signals GPS / GLONASS to determine the current position.

The complex of "Enclave" has the ability to use non-directional and directional (directional pattern – 40×40, the gain – 13 dB) antenna from the kit, which provides a certain effect on the sector. One of the disadvantages of the complex is its selectivity and consequently not it suppresses alarms and their own units and troops. For use of such equipment is being developed special algorithms use.

On the Engineering Technologies 2012 concern "Vega" demonstrated his own initiative development – hardware of radiomonitoring and blocking of control channels remote-controlled aircraft models, code "Rosehip Aero".

The hardware system is tuned to combat unmanned aerial vehicles, in addition to its help it is possible to suppress the broadcast stations, command centers of communication, signals of cellular networks, networks Wi-Fi, WiMax, DECT.

Can use wideband interference and suppress all the signals, it is possible to use narrowband and suppress certain frequency range, you can set information interference, which would distort the information. That in contrast to military EW stations, becoming not interference barrage oriented mistake receiver and an information-oriented error decoder. "Rosehip Aero" can work in motion and stationary, either directly with the hardware, and a remote station. Remote station and hardware can work together so you can take two simultaneous bearing and accurately determine the location of the object on which the work is performed. [5]

The considered system is adaptive, but have several disadvantages: they are expensive and bulky. And if the whole complex is situated in one place, it can be easily neutralize by enemy.

IV. Problem Solution

To solve the problem it is advisable to make a decomposition of the problem, which as follows.

Structural decomposition of posed problem has the following form.

1) Evaluation of the frequency bands work of command and information channels.

2) Determination of the power consumption.

3) Determination of point coordinates of system's elements placement in order to effective cover the predetermined area.

4) The optimal choice of complex of technical means.

To suppress radio channel UAV requires a system that generates high-power interference signal and carries out the task of broadband noise. At the same time its cost should be minimal.

Tasks:

– create a radar with Doppler low-signature;

– radar (centimeter-band radar);

– development of the comb filter provides an estimate of the radio signals emitted by the object of the air;

– implementation of incorporating elements of electronic warfare systems at the rate of motion of the object in the air a certain range of frequencies comb filter.

Functional of system.

1. Determination of geometric placement of elements of the lower level of the system.

2. Detection of UAV.

3. Identification of target coordinates.

4. Determining the frequency subsystem command and information radio UAVs.

5. Calculation of the reference variable (frequency, power, range of elements of the lower level) for the elements of the lower level of intellectual two-tier system of electronic warfare UAV.

6. Suppression of information and command radio signal, GPS.

Figure 2 shows a block diagram of the system of intellectual EW.

The intellectual system of upper level provides definition of a given frequency and interference power for the elements of the lower level (AJ) of EW system.

To create a disturbance choose a digital signal generator with adjustable frequency.

The hardware of the digital generator includes the following blocks:

– synchronization unit;

– a frequency synthesizer;

– control device;

– microprocessor;

– LCD display;

– LED unit.

Figure 3, consider the block diagram of the adaptive jammer (digital signal generator tunable).

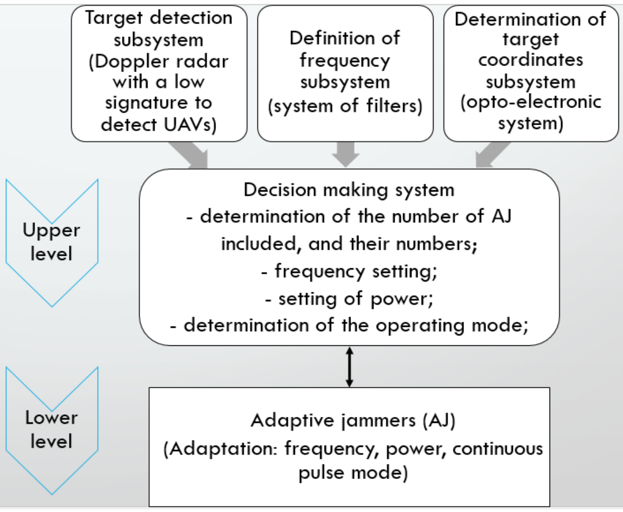
Target detection subsystem (Doppler radar with a low signature to detect UAVs)
Definition of frequency subsystem (system of filters)
Determination of target coordinates subsystem (opto-electronic system)
Upper level
Decision making system
- determination of the number of AJ included, and their numbers;
- frequency setting;
- setting of power;
- determination of the operating mode;
Lower level
Adaptive jammers (AJ)
(Adaptation: frequency, power, continuous pulse mode)

Fig. 2. Block diagram of a two-level system of intellectual EW

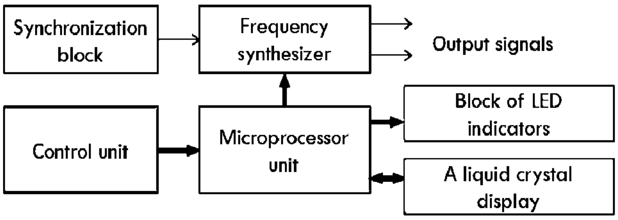

Fig. 3. A block diagram of an adaptive jammer

To detect the UAV using Doppler radar with a low signature (RLS). The functions and the appointment of the radar as follows:

– automatic review of space discovery, recognition of class goals;

– auto en-route tracking 20 targets with the issuance of each of these three coordinates and radial velocity in the CMC BM.

Station system and targeting of VAT shown in Fig. 4.

A Suppression channel GPS UAV

The device has two-way action affects the device uses the GPS signal. These include UAV works with coordination. GPS signal jammers produce noise interference on frequency coordination of the system, making it impossible to broadcast and receive information.

Jamming is blocking communication with the satellites navigation trekkers, so cannot be determined, to fix the coordinates of its location and movement.

B GPS-spoofing

Spoofing attack on GPS is an attack that tries to fool the GPS-receiver, transmitting broadcast signal is a bit more powerful than those obtained from satellites GPS, such as to be similar to the number of normal signals GPS. These mimic the signals changed in such a way to make the UAV is wrong to determine your location, considering it as such, an intelligent system which sends electronic warfare [10].

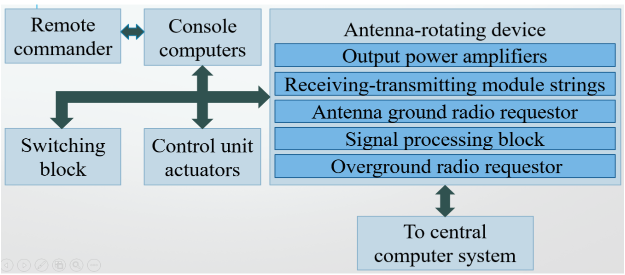

Fig. 4. Structure RLS including VAT

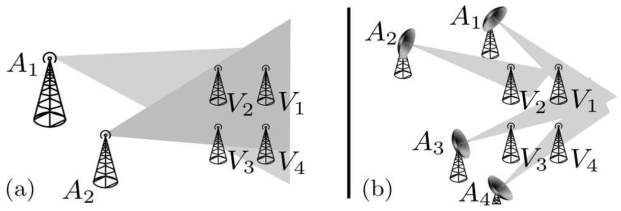

Fig. 5. Models of the attacker's antenna coverage. (a) Attacker's signals reach all victims (used in the analysis of this paper). (b) Attacker's antennas each only reach one victim. This requires the attacker to be in close proximity to the victims if the distances between the receivers are small

V. Method for Determining the Frequency of Narrowband Signal

A method for determining the frequency of the narrowband signal, wherein the signal duration T to obtain N sampled points, calculate the discrete energy spectrum it is determined number k of the spectral component with a maximum amplitude [11].

A method is known for determining the frequency of the narrowband signal, which consists in that sampled S signal duration T is sampled with a period of T/N, thereby obtaining N samples in the time domain signal S_n. Thereafter, the resulting sample signal applied the discrete Fourier transform to obtain discrete values of the Fourier transform of formula F_k

$$F_k = \frac{1}{N}\sum_{n=0}^{N-1}\left[S_n \exp\left(-j\frac{2\pi nk}{N}\right)\right]$$

where j is the designation of the imaginary unit; n is the number of time-domain samples, k is the number of discrete values of the Fourier transform in the frequency domain.

Then, using the obtained values is calculated the discrete energy spectrum of the signal by the equation:

$$P_{Fk} = \left[\operatorname{Re}(F_k)\right]^2 + \left[\operatorname{Im}(F_k)\right]^2,$$

where $\operatorname{Re}(F_k)$ and $\operatorname{Im}(F_k)$ are real and imaginary parts of k-values of the discrete Fourier transform. The resulting energy spectrum is determined by a number k of the spectral component having the maximum value and the calculated value P_{Fk} angular frequency ω for a given maximum spectral component of the formula.

The disadvantage of this method is considered that the accuracy of determining the frequency of the signal depends on the duration of the sample T.

V. Conclusions

A distinctive feature of the developed system is its reliability and functionality. Ultralight and stable construction of the system is fixed and can be easily transferred by quadrocopters. The mobility of system allows performing jamming in inaccessible places. Due to radio control, the operator can controlled and adjusted operation of the system jamming. In addition, the use in developing of the intellectual system can cover a large area, without loss of quality.

References

[1] Means of jamming and anti-jamming of radar station. [Online]. Available: http://www.techniformula.ru/foakom-459.html

[2] How to counteract the drone? (2015, Feb. 17). [Online]. Available: http://topwar.ru/print:page, 1,69167-kak-protivodeystvovat-bespilotniku.html

[3] A. Alexeev, (2013 Dec. 24). The old and new ways of dealing with unmanned vehicles. [Online]. Available: http://topwar.ru/37629-starye-i-novye-sposoby-borby-s-bespilotnymi-apparatami. html

[4] G. V. Yeremin, A. D. Gavrilov, and I. I. Nazarchuk, (2015, May 21). Organization of the system combating small-sized UAVs. *An arsenal of the Fatherland.* [Online]. Available: http://arsenal-techestva.ru/article /389 -antidrone

[5] D. Apolit, (2012, Aug. 24). "Rosehip Aero" – a system of struggle against drones. [Online]. Available: http://politikus.ru/army/2080-shipovnik-aero-sistema-borby-protiv-bespilotnikov.html

[6] Coverage calculation interference. (2014, Nov. 29). [Online]. Available: http://studopedia.org/5-99971.html

[7] An Autonomous Autopilot Control System Design for Small-Scale UAVs. QSS Group, Inc. NASA ResearchCenter, 2005.

[8] Developmentof Unmanned Aerial Vehicle Manual Control System, Engineeringand Technology, 2008.

[9] F. Perunov and L. M. Yudin, Jamming communication channels weapon control systems. Radio Engineering, 2003.

[10] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, On the Requirements for Successful GPS Spoofing Attacks. [Online]. Available: https://www.cs.ox.ac.uk/files/6489/gps.pdf

[11] Method for determining the frequency of narrowband signal, by A. V. Berintsev, A. A. Chertoriysky. *Patent G01R23/16.* [Online]. Available: http://www.findpatent.ru/patent/244/2442178.html

Received August 28, 2015

Sineglazov Viktor. Doctor of Engineering. Professor.
Aviation Computer-Integrated Complexes Department, National Aviation University, Kyiv, Ukraine.
Education: Kiev Polytechnic Institute. Kiev, Ukraine (1973).
Research interests: Air Navigation, Air Traffic Control, Identification of Complex Systems, Wind/solar power plant.
Publications: more than 500 papers.
E-mail: svm@nau.edu.ua

Tkachenko Olena.
Aviation Computer-Integrated Complexes Department, National Aviation University, Kyiv, Ukraine
Research interests: Air Navigation, Air Traffic Control.
E-mail: ElenaTkachenko@bigmir.net

В. М. Синєглазов, О. Ю. Ткаченко. Інтелектуальна дворівнева система радіоелектронної боротьби з БПЛА

Розглянуто алгоритм розробки широкосмугового джерела перешкод для безпілотних літальних апаратів. Конфігурація пристрою здійснюється за допомогою інтелектуального блоку, який забезпечує дистанційне включення генераторів, що забезпечує імпульсний режим роботи системи.

Ключові слова: безпілотні літальні апарати, радіоелектронна боротьба, перешкоди.

Синєглазов Віктор Михайлович. Доктор технічних наук. Професор.
Кафедра авіаційних комп’ютерно-інтегрованих комплексів, Національний авіаційний університет, Київ, Україна.
Освіта: Київський політехнічний інститут. Київ, Україна (1973).
Напрям наукової діяльності: аеронавігація, управління повітряним рухом, ідентифікація складних систем, вітроенергетичні установки.
Кількість публікацій: більше 500 наукових робіт.
E-mail: svm@nau.edu.ua

Ткаченко Олена Юріївна
Кафедра авіаційних комп’ютерно-інтегрованих комплексів, Національний авіаційний університет, Київ, Україна.
Напрямок наукової діяльності: аеронавігація, управління повітряним рухом.
E-mail: ElenaTkachenko@bigmir.net

В. М. Синеглазов, Е. Ю. Ткаченко. Интеллектуальная двухуровневая система радиоэлектронной борьбы с БПЛА

Рассмотрен алгоритм разработки широкополосного источника помех для беспилотных летательных аппаратов. Конфигурация устройства осуществляется с помощью интеллектуального блока, который обеспечивает дистанционное включение генераторов, что обеспечивает импульсный режим работы системы.

Ключевые слова: беспилотные летательные аппараты; радиоэлектронная борьба; постановщик помех.

Синеглазов Виктор Михайлович. Доктор технических наук. Профессор.
Кафедра авиационных компьютерно-интегрированных комплексов, Национальный авиационный университет, Киев, Украина.
Образование: Киевский политехнический институт, Киев, Украина (1973).
Направление научной деятельности: аэронавигация, управление воздушным движением, идентификация сложных систем, ветроэнергетические установки.
Количество публикаций: более 500 научных работ.
E-mail: svm@nau.edu.ua

Ткаченко Елена Юрьевна
Кафедра авиационных компьютерно-интегрированных комплексов, Национальный авиационный университет, Киев, Украина.
Направление научной деятельности: аэронавигация, управление воздушным движением.
E-mail: ElenaTkachenko@bigmir.net