UDC 004.056.5:629.7.014-519 (045)

PROBLEMS OF UNAUTHORIZED INTERFERENCE TO THE WORK OF UAV AND METHODS OF ITS SOLVING

I. O. Kozliuk, Doctor of Engineering, Professor; ***D. I. Bakhtiiarov***,

O. Y. Lavrynenko, ***I. V. Tretiak***
National Aviation University
e-mail: bakhtiyaroff@nau.edu.ua

This article is sanctified to the actual subject -research of unmanned aerial vehicles(UAV). The flow diagram of UAV is shown in this scientific work, the information about advantages, prospects and methods of UAV application in the different spheres of life is brought up. The basic methods of unauthorized access to management and software are analysed. The examples of unauthorized interference to the work of UAV control system are shown and the possible solutions of UAV defence are offered. Anapparatus, which gives an opportunity to find out the place of UAV stay on certain territory and report about it, is analysed.The list of developing safe methods of counteraction to the UAV is given to consideration. The questions of home soldiery unmanned aerial vehicles, that become more important with every day, are considered. The types of possible attacks are analyzed. It is educed that basic defense is still the cryptosystem of UAV control system defense. This article allows you to delve into the issues and benefits caused by new unmanned aerial techniques, understand the seriousness of the problems and prospects, the ability to research and development in this direction.

Keywords: UAV — Unmanned aerial vehicle; immunity encoding; spoofing encryption.

Стаття присвячена актуальній тематиці — дослідженню безпілотних літальних апаратів (БПЛА). У цій науковій праці показано структурну схему БПЛА, наведено інформацію про переваги, перспективи та способи застосування БПЛА у різних сферах життя. Проаналізовано основні способи несанкціонованого доступу до програмного забезпечення і керування. Продемонстровано приклади несанкціонованого втручання в роботу системи керування БПЛА і запропоновано можливі рішення захисту БПЛА. Проаналізовано апаратуру, що дає можливість виявляти перебування БПЛА на певній території і повідомляти про це. Подається до розгляду перелік розроблюваних безпечних способів протидії безпілотним літальним апаратам. Розглянуто питання вітчизняних військових безпілотних літальних апаратів, які стають важливішими кожного дня. Проаналізовано типи можливих атак і виявлено, що основним захистом залишається криптографічна система захисту каналу керування БПЛА. Дана стаття дозволяє заглибитися в проблеми і переваги викликані новою безпілотною літальною технікою, зрозуміти серйозність проблем і перспектив, можливість розвитку і досліджень в цьому напрямку.

Ключові слова: БПЛА — безпілотний літальний апарат; завадостійке кодування; спуфінг; шифрування.

Introduction

Unmanned aircraft systems take up more space both in the military and civilian sectors each year. The activity of developers of unmanned aerial vehicles (UAVs) in Ukraine is more commercial in nature. Developers offer UAV for the needs of the civilian consumer services as well as for structures dealing with national security state. But today the services that may be provided by unmanned aviation systems are immature; the standards under which they have to be created are unapproved.

Ukraine is also a representative of unmanned aircraft systems manufacturers and has sufficient experience of its creation. But UAVs that are in service in the Armed Forces (AF) of Ukraine, were developed in the 70s of the last century, the comparing of their combat capabilities with the UAV of leading countries indicates their non-compliance with modern requirements. Therefore, national research of unmanned aerial vehicles (UAVs) capabilities is a very topical issue for our country.

Failures in the operation are becoming less and less due to the improvement of security and anticipation of contingencies. Problems arise when the cause of failure are offenders who try to damage the unmanned aerial vehicle or remove the information by unauthorized way, doing it for certain purposes, which reflect negatively on society.

To date, more than 70 countries produce unmanned aerial vehicles for the army, police, emergency, etc. On eBay sale from March 2014 127.000

drones were sold. There are about 20.000 UAVs on the military arming [1].

Setting objectives

Conceptual directions of development of unmanned vehicles in the interests of solving problems of national security and other areas are determined, on the one hand, by the relations between importance and volume of tasks that need to be and can be effectively addressed through aerial platforms without humans on board, the other hand — by the cost of development, production of its operation of unmanned vehicles, and most importantly — by the efficiency of their use. All this depends largely on the level of science, engineering and technology.

The purpose of the article is the investigation of the security, capabilities of disabling, unauthorized access and interaction of unmanned aerial vehicles with other developments. For the work implementation a number of works of national and foreign authors, who investigated these issues, have been analyzed.

Navrotskyi D. O. with his work «Cryptographic system of protection UAVs communication channels against illegal intrusion; Cornell University, who, along with Psaki, developed a spoofer and a way to protect against spoofing attacks; Roger Johnst, who offered an effective algorithm of antispoofing and Raul Race, who reported on his work on the use of spoofing attacks by an ordinary citizen.

Based on the analysis of UAVs using trends and ways of their further development, it may be concluded that the urgent task for today is the improving of existing and creating new UAV, the introduction of their classification and identification of typical structure of unmanned aircraft systems.

Main part

There are three main ways of unauthorized interference in the UAV. The first is a mechanical action, which is a direct output down of UAV by anti-aircraft defense capabilities.

The second method is the use of "jamming" devices that inhibit any radio channels, which are related with the work of UAV, by generating very powerful inhibiting signal at specified frequencies.

The third way is to intercept and substitute UAV data packets in the uplink channel of management [2].

Fast data transfer speeds and accuracy are one of the major tasks, posed during the development of UAVs, because in the case of failure of these points the device will harm to perform certain tasks, which will lead to large-scale problems. If the information comes to the "pilot" even with a relatively small delay, he cannot navigate and make the right decision, especially in an emergency situation, as the inability to obtain the information in time will be one of the destabilizing factors. The proceeding of false data to the device is very harmful, as in this case it detects a command incorrectly.

At the interception of UAV control by an attacker, UAV can harm civilians by using it as a weapon, namely, having steered to the selected target, which may be the building with many people. The target can be a municipal, strategically important object.

Representatives of the International Committee for the control of military robots (International Committee for Robot Arms Control) explained that the UAV can get unprotected "civil» GPS-signal, and a potential attacker can easily carry out an attack, using equipment that is not hard to be bought and construct at the home conditions (GPS-spoofer), which signal is stronger than the signal from the GPS satellite. It applies to the less protected devices, as the attitude to the protection of military UAVs is quite serious. Block diagram of the major functional parts of UAV is presented in Fig. 1.

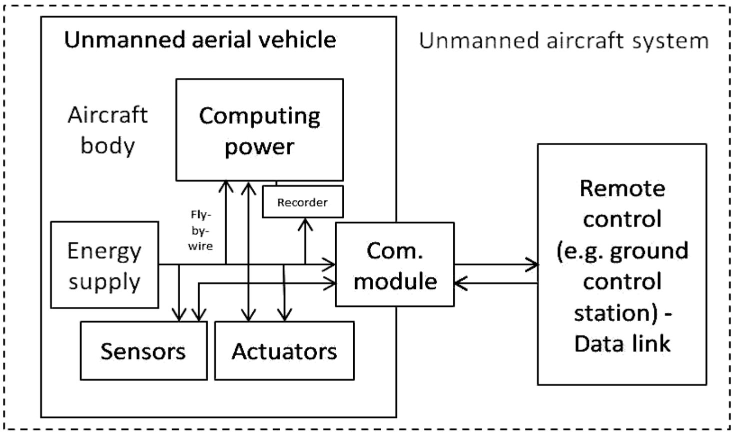


Fig. 1. Block diagram of the major functional parts of UAV

Analysis of the threats of the use of GPS-spoofing

The term Spoofing refers to the attack on GPS — attack that tries to impose GPS-receiver its coordinates, transmitting more powerful signal than the one obtained from GPS satellites, the ones to be like a number of normal signals GPS.

These signals are altered in such a way to make the UAV avionics follow the wrong trajectory of flight.

Since GPS systems work by measuring the time it takes for the signal to come from the satellite to the GPS receiver, GPS spoofing success requires the attacker to do the simulation of real GPS signal with changed coordinates and delays of the passage of signals which do not differ from the real GPS signal [3].

The world-famous example was the case with Iran and the United States. Iran presented a press-release to the media, stating the successful intercept of American unmanned aerial vehicle type RQ-170 Sentinel. Among other versions of the interception of the device one figured, which concerned the use of special electronics to suppress the signal of GPS satellites and its further substitution to their own. As a result of these actions UAV automatically, focusing on global navigation system, began to return home. As a true satellite signal was muffled with false one, the RQ-170 sat on the Iranian airfield, taking him for his final point [4].

Existing methods of dealing with GPS-spoofing

For the investigation of this matter Cornell University (Ithaca, NY) started to expand research activities in 2008. The results of this activity was the Receiver Autonomous Integrity Monitoring — a remarkable step for overcoming GPS spoofing as well as the spoofer, developed by them, which models various spoofing attacks and actively used to develop protection systems [5].

Data Bit Latency Defense Vestigial Signal Defense have been developed and demonstrated. These methods, proposed by Roger Johnston, allow blocking the imposition of a false GPS signal without the use of cryptography:

1. The level of the signal. The signal of GPS satellites on Earth's surface is rather weak, his level is about 163 dB * W. The signal emitted by the simulator is much stronger. Unusually high GPS signal may indicate an attack.

2. The same level of signal from different satellites. Usually GPS-signals of different satellites are very different in terms. Standard emulator allows you to simulate up to 24 satellites, but at this case the level of signal of each satellite is the same.

3. Noise. Emulated GPS signal has a very low noise level. If the GPS-receiver gets a clear signal it, likely, indicates that it is a false signal.

4. Numbers of satellites. On each of the earth's surface we can receive the signal only from certain satellites. Emulators often do not take it into account because if the GPS-receiver receives the signal from the satellite with the wrong number, it is a false signal [6].

Threats from the IP-spoofing

IP-spoofing attacks are often the starting point for other attacks. Typically, IP-spoofing is limited to inserting false information or malicious commands in the normal flow of data, transmitted over the communication channel between the peering devices. For bilateral communication the attacker must change all routing tables and direct traffic to a false IP-address. If he can change the routing table and send traffic to a false IP-address, he receives all packets and can respond to them as if he is sanctioned user [7].

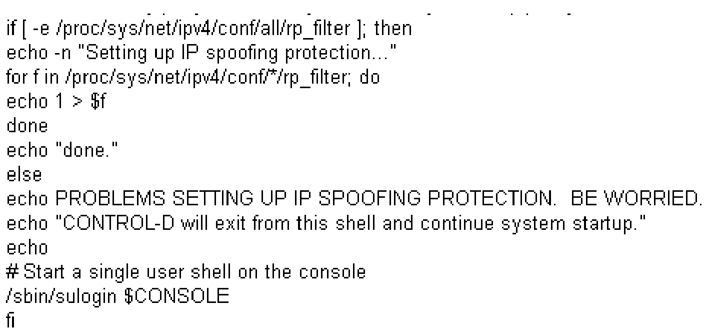
Reverse-engineering for ARDrone program.elf showed that "combined" attack using Maldrone and Skyjack will allow the interception of multiple targets and thereby create a squadron of intercepted UAV. Due to the growing interest in civil UAV from the corporations such DHL and Amazon, the case is a truly sinister. Moreover, using Maldrone, the attacker has the ability to not only steal drones, but to spy through built-in cameras by intercepting video signal from the attacked devices.

Maldron virus is able to control this program and move the UAV in any direction, almost stealing it from the owner. Maldrone disadvantage is that it takes some time to switch management, which is responsible for the navigation device. During this "interception" the drone is disconnected from the control, and it falls straight down, so it can lead to its physical injury [8].

Protection from IP-spoofing

One of the effective ways of disposal of IP spoofing is Source Address Verification, executable by routing programs instead of packet filtering.

The implementation of this algorithm is that initially you should check the file /proc/sys/net/ipv4/conf/all/rp_filter and enable verification of address. To do this, you should insert the commands of initialization scripts performing to configuration settings for network interfaces [9]. The text of this algorithm is shown in Fig. 2. Having analyzed IP-packet, and in particular — the adress of the sender, one can determine the IP-address of data source. IP-spoofing hides IP-address by creating packages that contain false addresses to hide data when connecting and sending information.



```
if [ -e /proc/sys/net/ipv4/conf/all/rp_filter ]; then
echo -n "Setting up IP spoofing protection..."
for f in /proc/sys/net/ipv4/conf/*/rp_filter; do
echo 1 > $f
done
echo "done."
else
echo PROBLEMS SETTING UP IP SPOOFING PROTECTION.  BE WORRIED.
echo "CONTROL-D will exit from this shell and continue system startup."
echo
# Start a single user shell on the console
/sbin/sulogin $CONSOLE
fi
```

Fig. 2. Implementation of initialization script commands

IP-spoofing is a generally recognized method used by hackers to hide their real IP- address. One can define IP-spoofing this way: check the IP-address which was found in the data and respond to it, check the value of TTL (Time to Live) original package before shipping [10].

Review of UAVs in service with the Ukrainian Army

As we know, a number of UAV is already used for repayment of armed conflicts in the area of conflict escalation of ATO and it is planned to be widely used by the Ukrainian army. During the exhibition "Arms and Security-2015" several options for domestic military UAV were presented. Fig. 4 shows the domestic unmanned aerial reconnaissance complex "Fury."

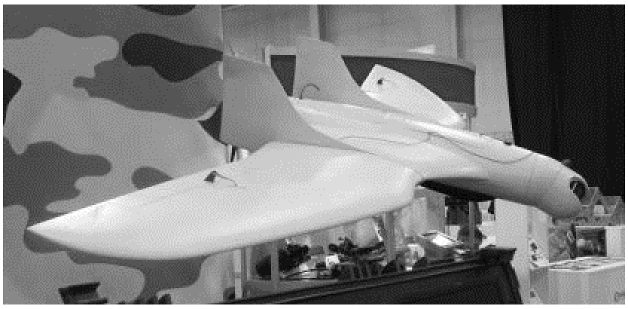


Fig. 4. Unmanned Aerial Reconnaissance Complex "Furies"

This complex has a thermographic device that is able to detect ground targets at a height up to 400 meters, passing intelligence information to the operator in real time.

In view of the technical capabilities of management equipment to take control over unmanned complex it is found that the range of use of "Furies" is 45 km.

This complex has recently been used by experts from the battalion "Dnepr-1" for holding the intelligence operations. The cost of the complex is 270 thousands UAH. It consists of three UAVs, surveillance equipment and ground control complex.

At Fig. 5 the unmanned aerial reconnaissance complex M-49 "Gaydamak" is shown. The complex was developed by the National Aviation University.

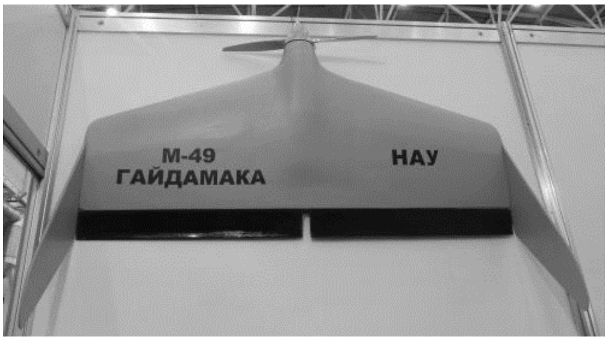


Fig. 5. Unmanned aerial reconnaissance complex M-49 "Gaydamak"

This system was developed in 2014 by experts of scientific-production center of unmanned aircraft "Virage" at the National Aviation University. Its maximum takeoff weight is just 4 kg, length — less than two feet and a wingspan — 0.82 m. According to the immediate purpose this complex is designed for use in surveillance and air reconnaissance purposes and for sabotage operations with the change of board equipment.

In addition to shock-reconnaissance UAVs specialists of "Virage" produce really large unmanned machines, such as aircraft "Heavenly patrol": M-7V5 and M-7D, requiring additional equipment for their transportation to the launch place [7]. These aircrafts increase the efficiency, quality and ease of military operations implementation and allow not endangering military warehouse unnecessarily.

The most effective way to protect military UAV is cryptographic system, which is under cryptanalytic attack. Today several basic types of cryptanalytic attacks are known:

The attack with knowledge of the encryption text. At the disposal of cryptanalyst there are several messages that were encrypted using the same encryption algorithm. The task is to find in the cryptanalyst`s plaintext the greatest number of intercepted messages. He may also try to find keys that were used to encrypt these messages.

Attack with the chosen plaintext. Cryptanalyst not only knows encrypted and plaintext messages, but he can determine the content of these messages.

This kind of cryptanalytic attack is more powerful compared to the attack with knowledge of the plaintext as in this case cryptanalyst can choose the plaintext to be encrypted, and thus receive more information about the keys used.

Attack with the selected key. During the attack, the cryptanalyst has some knowledge of rules by which sender and receiver of messages choose the encryption keys.

With the development of military technology the criminals` knowledge increases, this is why the protection of these systems is quite responsible matter, which requires special vigilance and attention. Achieving effective protection is possible only by examining the problems of unauthorized access and maximum classifying information from intruders.

Ways to fight UAV

Most modern UAVs use electric brushless motors that consume currents up to 100A. Switching the motor windings by a network switch creates specific electromagnetic fields detectable at distances up to 100 m.

Among developing safe ways of countering one can identify the following: setting interference, including blinding cameras with infrared lights, creating invisible air vortex screens along some private estates, including "smart screens" that are turned on suddenly following the signals from the sensors and create directional vortex with the purpose to bring the UAV systems onboard down [5].

In May, a consortium of three British companies announced the development of systems for preventing UAVs — Anti-UAV Defense System (AUDS), which is able to detect, monitor and prevent the use of UAVs within a radius of 8 km. Public authorities are interested in the system of protection of UAVs. They would prefer to prevent unauthorized use of UAVs in the presence of VIP-persons or during large public events [11].

Conclusions

Unmanned aerial vehicles have a significant number of impressive advantages and prospects, their use in the future cannot be questioned. The main problem arises is the unauthorized capture of information and control apparatus.

Being got by an attacker once, unmanned machine becomes a tool for the offense. Having sufficient theoretical knowledge, each ordinary citizen can make a UAV, or perform a type of attack on technique, so the direction to develop systems of detection and disposal of aircraft, which illegally stay on the territory, becomes relevant.

The leading countries are involved into the development of UAVs defense and bring a significant contribution to world science and spheres of human life. Due to the large-scale dissemination of such technology and general public awareness of its danger and importance, most countries impose certain rules and standards for the use of UAVs, the violation of which entails responsibility under the law.

Review article allows to deeper into the problems and benefits due to the newest unmanned aerial equipment. To understand the seriousness of the problems and prospects enable the development of research in this direction.

REFERENCES

1. *Dylevskyy, A. S.* Vzlom dronov [Hacking Drones]. Хакспейс Neuron. 2015. Retrieved from https://habra-habr.ru/company/neuronspace/blog/254685/.

2. *Dylevskyy, A. S.* Fyl-tratsyya paketov, firewall y maskaradynh v Linux [Packet filtering, firewall and masquerading under Linux]. Unixoid. 2014. Retrieved from http://www.fima.net/masquerade_page5.html.

3. *Navrotskyi D.* Cryptographic system of protection UAVs communication channels against illegal intrusion. Ukrainian Scientific Journal of Information Security, 2014. Vol. 20, issue 3, p. 248–252. Retrieved from http://jrnl.nau-.edu.ua/index.php/ Infosecurity/article/viewFile/7551/8607.

4. *Ju Anne.* 'Spoofed' GPS signals can be countered, researchers show. Cornell Chronicle Cornell Univercity. Retrieved_from http://news.cornell.edu/stories/ 2012/07/ resear-chers-counter-gps-spoof-attacks.

5. *Bakhtiiarov, D. I.* GPS spoofing yak zasib perekhoplennya keruvannya Bezpilotnym lital□nym aparatom [GPS spoofing as a way of intercepting UAV`s management]. POLIT. Tezy dopovidey VI mizhnarodnoyi naukovo-praktychnoyi konferentsiyi molodykh uchenykh i studentiv:Suchasni problemy nauky. Aeronavihatsiyni systemy. Elektronika ta aerokosmichni systemy upravlinnya [Abstracts of the VI International Scientific Conference of young scientists and students: Modern problems of science. Air navigation system. Electronics and aerospace control systems]. Kyiv: NAU, April 2014. — P. 125.

6. *Savelenko, O. K.* Sposoby poslablennya IP-spufinh ataky [Ways of weakening IP-spoofing]. Informatsiyni tekhnolohiyi ta kompyuterna inzheneriya: zbirnyk tez dopovidey naukovo-praktychnoyi konferentsiyi [Information Technology and Computer Engineering: a collection of abstracts of scientific conference]. Kirovohrad. December, 2014. — P. 173–174.

7. Kak ukrainskiye voyennyye ispol'zuyut bespilotniki: S pomoshch'yu "Furii" unichtozhili ZRK "Strela-10[How Ukrainian military use drones: With the help of "Furies" SAM "Strela-10 was destroyed]. Segodnya.UA. Retrieved from http://www. segodnya.ua/ ukraine/kak-ukrainskie-voe-nnye-ispolzuyut-bespilotniki-s-pomoshchyu-furii-unichto-zhili-zrk-strela-10-653312.html.

8. *Alferov, A.P., Zubov, A.U., Kuzmin, A.S., Cheremushkin, A.V.* Osnovy kriptografii: Uchebnoye posobiye [Basics of cryptography: Textbook]. 2001. Moscow: Helious. — P. 479.

9. *Sushko S. O., Kuznetsov H. V., Fomychova L. Y., Korablov A. V.* Matematychni osnovy kryptoanalizu [Mathematical fundamentals of cryptanalysis]. Textbook. Dnipropetrovsk: National Mining University, 2010.

10. *Bakhtiiarov D. I., Kozliuk, I. O.* Analiz efektyvnosti kompleksnoho zastosuvannya zakhodiv zavadoza-khyshchenosti dlya pidvyshchennya stiykosti funktsi-onuvannya zasobiv keruvannya BPLA [Analysis of effectiveness of complex application of noise protection measures to improve the sustainability of UAV control functioning]. Tezy dopovidey naukovo-tekhnichnoyi konferentsiyi:Problemy rozvytku hlobalnoyi systemy zv'yazku, navihatsiyi, sposterezhennya ta orhanizatsiyi povit-ryanoho rukhu CNS/ATM [Abstracts of scientific conference:Problems of the global system of communication leads, navigation, and surveillance of air traffic CNS / ATM]. Kyiv: NAU, November 2014. — P. 50.

11. *Bakhtiiarov D. I.* Doslidzhennya metodiv pobudovy zakhyshchenykh kanaliv upravlinnya BPLA [The investigation of methods to build the secured channels of UAV management]. Materialy XII mizhnarodnoyi naukovo-tekhnichnoyi konferentsiyi „AVIA-2015” [Materials of XII International Scientific Conference "AVIA 2015"]. Kyiv: NAU, 2015. — P. 151.

ЛІТЕРАТУРА

1. *Дилевский А. С.* Взлом дронов [Електронний ресурс] / А. С. Дилевский. — 2015. — Режим доступу: https://habrahabr.ru/company/neuronspace/blog-/254685/.

2. *Дилевский А. С.* Фильтрация пакетов, firewall и маскарадинг в Linux [Електронний ресурс] / А. С. Дилевский // Unixoid. — 2014. — Режим доступу: http://www.fima.net/masquerade_page5.html.

3. *Navrotskyi D.* Cryptographic system of protection UAVs communication channels against illegal intrusion Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3. — P. 248–252. — [Електронний ресурс]. — Режим доступу http://jrnl.nau.edu.ua/index.php/Infosecurity/article/viewFile/7551/8607.

4. *Anne Ju* 'Spoofed' GPS signals can be countered, researchers show Cornell Chronicle [Електронний ресурс] // Офіційний сайт Cornell Univercity. — Режим доступу: http://news.cornell.edu/stories/2012/07/researchers-counter-gps-spoof-attacks.

5. *Бахтіяров Д. І.* GPS spoofing як засіб перехоплення керування Безпілотним літальним апаратом / Д. І. Бахтіяров // ПОЛІТ. Сучасні проблеми науки. Аеронавігаційні системи. Електроніка та аерокосмічні системи управління: тези доповідей XIV міжнародної науково-практичної конференції молодих учених і студентів, м. Київ, 2–3 квітня 2014 р. — К. : НАУ, 2014. — С. 125.

6. *Савеленко О. К.* Способи ослаблення IP-спуфінг атаки / О. К. Савеленко. // Інформаційні технології та комп'ютерна інженерія: збірник тез доповідей науково-практичної конференції, Кіровоград, 4 грудня 2014 р. — 2014. — С. 173–174.

7. *Как украинские* военные используют беспилотники: С помощью «Фурии» уничтожили ЗРК «Стрела». — [Електронний ресурс] // Офіційний сайт Сегодня.UA. — 2015. — Режим доступу: http://www.seg-odnya.ua/ukraine/kak-ukrainskie-voennye-ispolzuyut-bes-pilotniki-s-pomoshchyu-furii-unichtozhili-zrk-strela-10-653312.html.

8. *Основы* криптографии: учеб. пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. — М. : Гелиос, 2001. — 479 с.

9. *Математичні* основи криптоаналізу: навч. посібник / С. О. Сушко, Г. В. Кузнецов, Л. Я. Фомичова, А. В. Корабльов. — Д. : Національний гірничий університет, 2010. — 465 с.

10. *Бахтіяров Д. І.* Аналіз ефективності комплексного застосування заходів завадозахищеності для підвищення стійкості функціонування засобів керування БПЛА / Д. І. Бахтіяров, І. О. Козлюк // Проблеми розвитку глобальної системи зв'язку, навігації, спостереження та організації повітряного руху CNS/ATM: тези доповідей науково-технічної конференції; м. Київ, 17–19 листопада. — К. : НАУ, 2014. — С. 50.

11. *Бахтіяров Д. І.* Дослідження методів побудови захищених каналів управління БПЛА / Д. І. Бахтіяров // Матеріали XII міжнародної науково-технічної конференції «АВІА-2015». — К. : НАУ, 2015. — С. 151.

Стаття надійшла до редакції 01.04.2016