Date of publication SEP-30, 2022, date of current version SEP-05, 2022.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.21.3.2695

Unmanned Aerial Vehicles as a Source of Information Security Threats of Wireless Network

SERHII VOITENKO[1], VOLODYMYR DRUZHYNIN[2], HANNA MARTYNIUK[3], TETIANA MELESHKO[4]

[1]Information Security Department, National Aviation University, Kyyiv, Ukraine, (e-mail: voytenko.s.d@gmail.com)
[2]Department of Scientific Research, National Aviation University, (e-mail: volodymyr.druzhynin@npp.nau.edu.ua)
[3]Department of System Analysis and Information Technology, Mariupol State University, Mariupol, Ukraine, (e-mail: ganna.martyniuk@gmail.com)
[4]Information Security Department, National Aviation University, Kyyiv, Ukraine, (e-mail: zzi.meleshko@nau.edu.ua)

Corresponding author: Hanna Martyniuk (e-mail: ganna.martyniuk@gmail.com).

ABSTRACT This work deals with the identification of threats to wireless networks when considering an attacker from unmanned aerial vehicles. An analysis of heterogeneous networks built on 4 G technology, as objects of UAV attack, is performed. It is determined that the main problem of protecting wireless systems is the lack of protection of radio communication channels and the vulnerability of the base and subscriber station equipment. A model of the UAV as an intruder in the information security of wireless networks is built. The classification of various types of UAVs by targets and weapons of attack, methods of use and the ability to violate the criteria of protection of the information and telecommunication system is presented. A threat model that assesses the level of risks and losses in different types of attacks performed by different types of UAVs is built. It is expedient to use the received models as the basic ones when building a model of threats to a certain corporate network of the organization, developing ways and security means, estimating and controlling 4 G network protection against UAV.

KEYWORDS unmanned aerial vehicles; violator model; threat model; 4G network; WiMAX and LTE; HetNet; confidentiality; availability; integrity; observability; UAV scouts; shock UAV; UAV-EW.

I. INTRODUCTION

AREAS of use of unmanned aerial vehicles (UAVs) are constantly expanding. Today UAVs are employed for monitor, search, recognition and rescue operations in different applications: for military purposes, in agriculture, mining, geodesy, topography [1-4] (Fig.1), critical infrastructures [31], cybersecurity [32].

For example, today unmanned aerial vehicles being often a source of primary information about various forces of fire are widely used to adjust the means of fire, allow the exchange of information and management of UAV using an automated control system [5, 6].

Unfortunately, technical progress in the field of unmanned aerial vehicles has a downside – there is a possibility of using UAV for unauthorized receipt, distortion and destruction of confidential information.

In addition, low visibility and the ability to penetrate into the controlled area allow UAV "bypass" traditional protection systems and create conditions for information leakage through optical, radio and acoustic channels. In fact, with the advent of UAV new technical channels of information leakage have emerged, which in turn requires the development of new methods of information protection and the creation of specialized technical means. This issue is especially relevant for telecommunications networks based on 4G wireless technologies.

II. RELEVANT WORK AND PROBLEM STATEMENT

For today there is a significant amount of works, in which unmanned aerial vehicles are treated as the source of information security threats when intruding into the area of the object. For example, works [7, 8] were devoted to the development of methods and means of detection and destruction of UAVs, and in [9, 10] examples of interception were given.

Short messages are available for the use of UAVs for inspection, testing and adjustment of telecommunication equipment of cellular towers of subscriber stations of mobile operators [7]. There are sources for application of UAVs as subscriber stations for the construction of an extensive 4G network [8, 9].

Figure 1. Multicopter with hotspot on board. Source [3]

From sources [11, 12] it is known that there is already a specially developed system of "Wi-Fi hacking", where UAVs are used.

According to sources [13-15] from April 2016 the Russian military in Donbass uses a complex of electronic warfare (EW) RB-341V “Layer-3” which consists of three UAVs with equipment designed to suppress wireless communication and replace base stations of 3G and 4G networks.

Figure 2. UAV Orlan-10 from the Leer complex. Source [5]

Conducted by the authors, the analysis of open sources shows the lack of work that determines the nature of threats to information security of wireless networks when used by UAV attackers. Therefore, to develop effective methods and means to protect wireless networks from UAV it is necessary to identify potential threats and assess the risk of their occurrence. This work is devoted to the development of basic models of the violator and threats during the attack on 4G wireless internet networks by UAV.

III. ANALYSIS OF 4G NETWORKS AS THE UAV ATTACK OBJECT

As it is already known, the International Telecommunication Union (ITU) at the WRS-10 seminar in Geneva (World Radio communication Seminar 2010) decided that the term 4G could apply to technology LTE i WiMAX [16, 17].

LTE-Advanced (LTE-A) – is a standard for cellular operators based on network technologies GSM/EDGE and UMTS/HSPA, which is used to build heterogeneous computer networks (HetNet) [18].

WiMAX (Worldwide Interoperability for Microwave Access) – telecommunications technology designed to provide universal long-distance wireless communication for a wide range of devices (from workstations and laptops to mobile phones), based on the standard IEEE 802.16, which is also called Wireless MAN [16].

4G networks include several subscriber stations (SS), one or more base stations (BS), united by wireless highways (Fig. 3). The network may include relay stations (RS), providing an increase in range and allows to bypass the big closing obstacles of BS from individual ones of SS [18, 19].

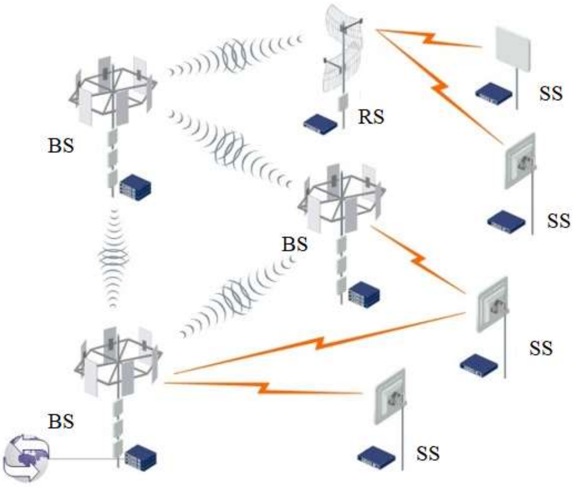

Figure 3. 4G network topology. Source [33]

BS is mounted on towers or roofs of subject houses to the condition of direct visibility between stations. Each BS contains from one to six sectors of antennas. In this case, at least one base station is connected to the provider’s network using classic wired connections [19].

According to the principles of networking, both technologies WiMAX and LTE are similar and have fairly similar standards. They both use coding technology OFDM and a data transmission system MIMO. Both standards apply Frequency Division Duplex (FDD) and Time Division Duplex (TDD) at channel bandwidth up to 20 MHz. Both systems use IP communication protocols [18].

Based on this, according to the authors, the nature of the threats of both networks during the attack of UAV will be similar. And the existing differences will mainly consist in the peculiarities of the implementation of attacks and involved EW equipment. These differences can hardly be considered in the context of a single article.

The main problem with the protection of 4G networks is the lack of control over the radio communication channels of the BS and SS (LTE modems). This allows the UAV to be located in close proximity of the network’s antenna-feeder devices, to carry out a range of attacks that would be impossible for a wired network. In these conditions, for today, there are no reliable methods and means to prevent breaches of confidentiality, integrity, reliability of transmitted information and operability of the network as a whole or its individual nodes [4].

In practice, the protection of transceivers of networks is carried out by restricting the access of potential intruders to the controlled area on the towers and roofs. But in case the use of drones by the violator mentioned measures are not effective. Given that several types of UAVs with different equipment can be used for attacks, it is advisable to develop a model of UAV as a violator of information security for threat analysis.

IV. MODEL OF UAV THREATS

In the general case, the threat model is a formalized description of methods and means of making threats to information. According to [20], there are four main criteria for assessing the security of information and telecommunications systems (ITC):

– confidentiality criterion (C) – unauthorized access to information;

– accessibility criterion (A) – violation of the possibility of using ITS or processed information (denial of customer service);

– integrity criterion (I) – unauthorized modification (distortion, falsification, distortion of information);

– observation criterion (O) – refusal to identify, authenticate and register dangerous actions [6].

The authors consider it appropriate to use the military classification of UAVs by purpose to build a model of the violator. According to this classification, three types can be used for attacks UAV: UAV-scouts, UAV-electronic warfare (UAV-EW) and shock UAVs. However, it is unlikely that attackers will use military specialized models of UAV, it is more likely to use available, commercial models, re-equipped in accordance with the purpose of the attack (Table 1).

Simple, accessible the UAV vertical takeoff and landing (multicopters, helicopters) with standard video surveillance means (IP camera, thermal imager) can be used as scouts. The basis of the listening equipment will be a simple range receiver used by the operator, such as a modem located on board.

Intelligence listening equipment is used to obtain unprotected data and collect network data for future attacks. The hijacking data (identification codes, passwords, etc.) allows to access network resources – create access points for third-party consumers.

Table 1. Distribution of threats by UAV type

Type of UAV / Type of threats	C	A	I	O
UAV-scouts	+			
UAV-EW		+	+	+
shock UAV		+		

Most likely that the method of using the UAV-scout will include:

– flight and recording of information under the control of operators, which must be located at a distance of up to 500 m from the UAV in a parked car or building;

– the location (landing) of the UAV in the area of the pattern of the SS antenna, not necessarily near the antenna devices;

– recording information on on-board media, or use for online data transmission of the regular channel of IP cameras (5.8 GHz);

– processing and decoding of the intercepted information in stationary conditions on office equipment of conspirators.

UAVs-EW are capable of affecting the performance of telecommunication systems by interfering and creating false SS or BS (RS).

Identification codes for SS (BS) substitutions are obtained either by a shock-UAV or by an EW complex consisting of two UAVs: a fault setter and a faulty access point.

Transmitter power supply and active interference setting require significant energy consumption of onboard power supplies, therefore, a platform for UAV-EW can be heavy multicopters with a hybrid power plant or an aircraft with an internal combustion engine. A range of application and duration of work of UAV-EW depends on the chosen type of lethal device and can reach 120 km and 10 hours. If necessary to suppress the SS or BS (RS) a second UAV can be used with an on-board but resettable interference maker [15].

Substitution of a subscriber station is the most difficult from the attack, more likely the SS substitution technique will include:

– usage of a router as specialized on-board equipment, which performs the functions of a transponder and ensures the admission of an attacker through any available wireless network;

– recording on the router pre-intercepted data for authorization in the network: certificates X. 509 station and its manufacturer, authorization keys and encryption;

– the interference detector, being near the receiving antenna SS, fills with interference the whole range of operating parts of the cellular operator, blocking the passage of signals between stations;

– after communication failure and re-identification of UAV-EW being near the receiving antenna, BS is authorized instead of the real SS.

Shock UAVs are carriers of means of damage and can disable critical for the functioning of the telecommunications system equipment, probable antenna-feeder devices and elements of power supply networks [4, 30].

Both SS and BS can be attacked by UAVs, and cheap multicopters or even radio-controlled aircraft models can be the means of destruction. Commercial aerosol cans can be inserted as means of damage Drone Graffeti with not transparent to radio waves coating, metal wires and grids for the failure of antenna-feeder devices and their power lines (Fig. 4).

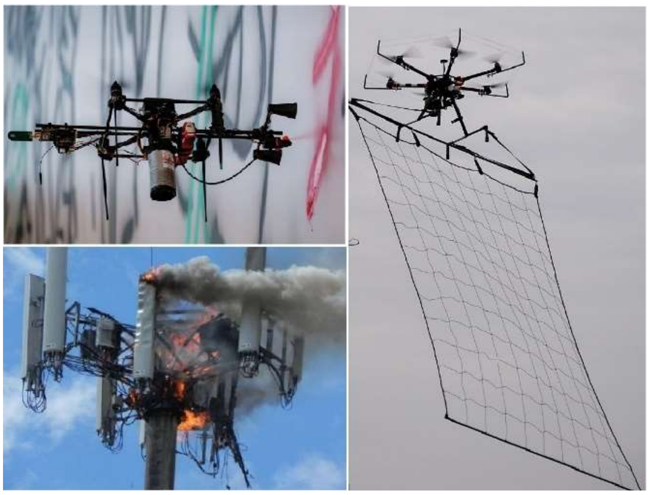

Figure 5. Impact weapon and attack object UAV. Source [34]

It is more likely that attackers will predict:

– attack at night to maintain secrecy;

– finding the control operator in the immediate vicinity of the object of attack (up to 500m), preferably in line of sight;

– applying opaque coatings on the antenna of the device, which prevents or impairs user access to network resources;

– the use of varnishes and oils in order to complicate the search for the cause of failure and determine the fact of the attack;

– discharge of metal wires or nets in order to neutralize the antenna-feeder devices due to a short circuit and fire.

V. THREAT ASSESSMENT

During the day, scouts are able to deliver embedded devices to the facilities for sniffing and hijacking transmitted information.

The purpose of the UAV-EW attack is to suppress the communication channel (Denial-of-Service, DoS) or to replace the SS (Spoofing) with subsequent modification of information and loss of network observation.

Damage to the shock UAV elements of the information system causes denial of user access to network resources.

According to the model of the violator and threats, we assess the risks and losses (1 point-low, 2 points-medium, 3 points-high) when attacking on 4G networks by different types of UAV (Table 2).

Using the results of Table 2 as a basis, the authors came to the following conclusions.

A. SCOUTS

Sniffing – receiving unprotected data or loss of privacy alone will not lead to distortion of information and violation of the functional properties of the network and will usually lead to minor losses (1 point). Given the cheapness of intelligence, ease of use, secrecy (eavesdropping), the probability of using intelligence is high (3 points).

Hijacking is usually a prerequisite for hacking a threat with the wrong access point (such as UAV-EW). Considering the inability of the scout to perform spoofing-attacks independently, the limitations of the functionality of its onboard equipment, relative complexity of organizing such an attack, the authors believe that the levels of damage and risk will be moderate (2 points).

2. UAV-EW

DoS-attack – suppression of BS (SS). Given that powerful radiation immediately unmasks the fact of the attack, the installation of an active obstacle is energy consuming and cannot be long, there is no access to information for attackers, the risk of application and damage will be low (1 point). This method can only be effectively used by the EW complex to block a real access point (e.g., SS) for authorization in the UAV-EW network and to carry out a spoofing attack.

Table 2. Calculation of threat assessment

UAV type	Types of attacks / threats	Level		Threat assessment
		risks	losses	
UAV scouts	Sniffing Confidentiality	high 3	low 1	4
	Hijacking Confidentiality	average 2	average 2	4
UAV-EW	Denial-of-Service Accessibility	low 1	low 1	2
	Spoofing Integrity	high 3	high 3	6
	Spoofing Observation	low 1	low 1	2
Shock-UAV	Denial-of-Service Accessibility	low 1	high 3	4

Spoofing-attack in order to violate the integrity. Given that falsification and distortion of information is the most desirable goal of espionage, the probability of such an attack is high (3 points), and violation of the integrity of information will lead to significant losses (3 points).

Spoofing-attack in order to disrupt observation. According to the authors, modern HetNet networks have a sufficient level of protection to ensure controllability when attacking the SS (BS). Only partial loss of control over user actions is possible (1 point). At the same time, violators must know the structure, functions and mechanisms of information security in ITS, in which case there are simpler options for attack, so the probability of choosing to implement a threat by attacking UAV SS (BS) is small (1 point).

3. Shock-UAV

Physical damage to SS or BS equipment will be resulted in significant property damage and loss of access to a large number of users to network resources (3 points). At the same time, the implementation of such attacks certainly belongs to the plane of criminal responsibility and cannot be mass in commercial espionage (1 point).

VI. CONCLUSION

The developed models contain uniform initial data on security threats in case of interception, blocking and unauthorized access of UAV to 4G networks. These models can be used by organizations and institutions as basic models for methodological support for solving the following problems:

– development of security threat models of specific HetNet networks taking into account their purpose, topology and conditions and features of operation;

– analysis and control of protection against UAV 4G networks;

– development of 4G network protection systems that provide neutralization of possible threats using UAV;

– measures aimed at preventing unauthorized access to information in the 4G network via UAV;

– prevention of the impact of UAV on the technical means of the 4G network, as a result of which its functioning may be disrupted.

References

[1] J.C.O. Koh, M. Hayden, H. Daetwyler, et al., “Estimation of crop plant density at early mixed growth stages using UAV imagery,” *Plant Methods*, vol. 15, article 64, 2019. https://doi.org/10.1186/s13007-019-0449-1.

[2] A. Gurnik, S. Valuiskyi, “The use of intelligent sensor technology for monitoring and search and rescue,” *East European Journal of Advanced Technology. Management Information Systems*, no. 3/9 (63), pp. 27-32, 2013.

[3] M. Półka, S. Ptak, Ł. Kuziora, “The use of UAV's for search and rescue operations,” *Procedia Engineering*, vol. 192, pp. 748-752, 2017. https://doi.org/10.1016/j.proeng.2017.06.129.

[4] S. W. Cho, H. J. Park, H. Lee, D. H. Shim, S.-Y. Kim, “Coverage path planning for multiple unmanned aerial vehicles in maritime search and rescue operations,” *Computers & Industrial Engineering*, vol. 161, article 107612, 2021. https://doi.org/10.1016/j.cie.2021.107612.

[5] O. Vodchyts, S. Voitenko, “The Orlan-10 complex as an element of the automated command and control system,” Weapons and military equipment, no. 2, pp. 33-38, 2015. (in Ukrainian)

[6] S. Borg, “Below the radar. Examining a small state’s usage of tactical unmanned aerial vehicles,” *Defence Studies*, vol. 20, pp. 185-201, 2020. https://doi.org/10.1080/14702436.2020.1787159.

[7] M. Silvagni, *et al*., “Multipurpose UAV for search and rescue operations in mountain avalanche events,” *Geomatics, Natural Hazards and Risk*, vol. 8, issue 1, pp. 18-33, 2017. https://doi.org/10.1080/19475705.2016.1238852.

[8] K. Hartmann and K. Giles, “UAV exploitation: A new domain for cyber power,” Proceedings of the 2016 8th IEEE International Conference on Cyber Conflict (CyCon), 2016, pp. 205-221. https://doi.org/10.1109/CYCON.2016.7529436.

[9] “5 ways drones could come to your rescue,” Popular Mechanics. November 14, 2017. [Online]. Available at: https://www.popularmechanics.com/military/g1437/5-ways-dronescould-come-toyour-rescue/.

[10] C. Yu, B. Zhu and Z. Zuo, “Three-dimensional optimal guidance with lyapunov redesign for UAV interception,” *Guidance, Navigation and Control*, vol. 01, no. 04, 2140004-1–2140004-19, 2021. https://doi.org/10.1142/S2737480721400045.

[11] D. Rudinskas, Z. Goraj, J. Stankūnas, “Security analysis of UAV radio communication system,” *Aviation*, vol. 13, issue 4, pp. 116-121, 2009. https://doi.org/10.3846/1648-7788.2009.13.116-121.

[12] F. Al-Turjman, R. Salama, “Chapter 3 - Cyber security in mobile social networks,” *Security in IoT Social Networks, Intelligent Data-Centric Systems*, 2021, pp. 55-81. https://doi.org/10.1016/B978-0-12-821599-9.00003-0.

[13] M. Yeo, “Electronic warfare in the land domain - The threats continue to increase,” *Asia-Pacific Defence Reporter*, vol. 45, issue 7, pp. 20–22, 2019. https://doi.org/10.5604/01.3001.0012.7224.

[14] P. Smith, “Russian electronic warfare: A growing threat to U.S.”, *Battlefield Supremacy. American Security Project*, 2020.

[15] R. Vasicek, A. Oulehlova, “Cyber and electromagnetic activities and their relevance in modern military operations,” *Proceedings of the 31th European Safety and Reliability Conference*, 2021, pp. 512-519. https://doi.org/10.3850/978-981-18-2016-8_231-cd.

[16] N. Neji, T. Mostfa and Y. B. Sebbane, “Technology assessment for radio communication between UAV and ground: Qualitative study and applications,” *Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 2019, pp. 1-6, https://doi.org/10.1109/VTCSpring.2019.8746306.

[17] A. Sharma, P. Vanjani, N. Paliwal, C. M. W. Basnayaka, D. N. K. Jayakody, H.-C. Wang, P. Muthuchidambaranthane, “Communication and networking technologies for UAVs: A survey,” *Journal of Network and Computer Applications*, volume 168, 102739, 2020. https://doi.org/10.1016/j.jnca.2020.102739.

[18] G. Yang, X. Lin, Y. Li, H. Cui, M. Xu, D. Wu, H. Rydén, S. B. Redhwan, “A telecom perspective on the internet of drones: From LTE-advanced to 5G,” Computer Science, Networking and Internet Architecture, arXiv:1803.11048, 2018.

[19] R. Miura, M. Maruyama, M. Suzuki, H. Tsuji, M. Oodo and Y. Nishi, “Experiment of telecom/broadcasting mission using a high-altitude solar-powered aerial vehicle Pathfinder Plus,” *Proceedings of the 5th International Symposium on Wireless Personal Multimedia Communications*, 2002, vol. 2, pp. 469-473. https://doi.org/10.1109/WPMC.2002.1088218.

[20] S. K. Khan, “Mathematical framework for 5G-UAV relay,” *Trans Emerging Tel Tech*, 32:e4194, 2021. https://doi.org/10.1002/ett.4194.

[21] V. L. Thing, & J. Wu, “Autonomous vehicle security: A taxonomy of attacks and defences,” Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016, pp. 164-170. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.

[22] A. Fotouhi et al., “Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3417-3442, 2019. https://doi.org/10.1109/COMST.2019.2906228.

[23] T. Gu, and Y. Chen, “Design of effectiveness evaluation system for shipborne unmanned reconnaissance aircraft,” *Journal of Coastal Research*, vol. 83, pp. 565-570, 2018. https://doi.org/10.2112/SI83-093.1.

[24] H.-J. Schmidt, “A fresh start of conventional arms control in Europe will face many structural problems,” vol. 151, DEU, 2017.

[25] J. Kjellèn, *Drone-based jamming (REB-N). Russian Electronic Warfare. The role of Electronic Warfare in the Russian Armed*, Swedish Defence Research Agency, 2018, p. 105.

[26] M. Rumney. IMT-Advanced: 4G Wireless Takes Shape in an Olympic Year, Agilent Measurement Journal, 2000, 10 p.

[27] M. Abdulla, *On the Fundamentals of Stochastic Spatial Modeling and Analysis of Wireless Networks and its Impact to Channel Losses*, Ph.D. Thesis, 2012, 126 p.

[28] X. Ji, and Y. Zhao, “Architecture design for unmanned aerial vehicle mission planning system,” *Proceedings of the 2019 International Conference on Modeling, Simulation and Big Data Analysis (MSBDA 2019)*, Atlantis Press, 2019, pp. 419-424. https://doi.org/10.2991/msbda-19.2019.66.

[29] H. A. Kayani, Q. Gueuning, N. Goreux, D. Vanhoenacker-Janvier, C. Oestges and C. Craeye, “Reconfigurable cellular base station antenna consisting of parasitic radiators,” *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 7083-7093, 2020, https://doi.org/10.1109/TIE.2019.2935991.

[30] ND TZI 2.5-004-99 Criteria for assessing the security of information in computer systems from unauthorized access, 1999. (in Ukrainian)

[31] I. M. Kliushnikov, H. V. Fesenko, V. S. Kharchenko, “Scheduling UAV fleets for the persistent operation of uav-enabled wireless networks during NPP monitoring,” *Radioelectronic and Computer Systems*, no. 1, 2020. https://doi.org/10.32620/reks.2020.1.03.

[32] Z. Hu, R. Odarchenko, S. Gnatyuk, M. Zaliskyi, A. Chaplits, S. Bondar, V. Borovik, “Statistical techniques for detecting cyberattacks on computer networks based on an analysis of abnormal traffic behavior,” *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 12, no.6, pp. 1-13, 2020. https://doi.org/10.5815/ijcnis.2020.06.01.

[33] V. Vishnevskii, C. Portnoi, I. Shakhovich, WiMax Encyclopedia. Way to 4G, Tekhnosfera, Moscow, 2009, 472 p.

[34] http://www.ukraviaforum.com/index.php

SERHII VOITENKO, *PhD, a Senior Research Fellow. Graduated Kyiv Institute of Air Force in 1997. Now works as Associate Professor of the Information Security Department. Scientific interests: technical means of information security; unmanned aircraft systems; protection against unauthorized entry of UAVs*

VOLODYMYR DRUZHYNIN, Doctor of Technical Sciences, a Professor. Graduated Kiev State University of Telecommunications, 2017. Now works as manager department of scientific research NAU. Scientific interests: unmanned aircraft systems, multi-position radar systems, pattern recognition systems.

HANNA MARTYNIUK, *PhD. Graduated National Aviation University in 2011. Now works as an Associate Professor of the Department of System Analysis and Information Technology. Scientific interests: information assurance of noise measurement; statistical models of information signals; statistical methods for measuring the characteristics of random processes and fields; methods of signal simulation and measurement data.*

TETIANA MELESHKO, *graduated Kyiv International University of Civil Aviation in 2000. Now works as a Senior Lecturer of the Information Security Department. Scientific interests: acoustic information protection system*