Evgeny OCHIN

THE VULNERABILITY OF UNMANNED VEHICLES TO TERRORIST ATTACKS SUCH AS GNSS-SPOOFING AND/OR JAMMING BY SCREENING OF ANTENNA

Streszczenie

Spoofing, anti-spoofing, jamming and anti-jamming technologies have become an important research topic within the GNSS discipline. While many GNSS receivers leave large space for signal dynamics, enough power space is left for the GNSS signals to be spoofed. The goal of spoofing is to provide the receiver with a misleading signal, fooling the receiver to use fake signals in the space for positioning calculations. The receiver will generate a misleading position of the navigator. Practical spoofing that provides misleading navigation results of the receiver is difficult to conduct due to the signal infrastructure and by applying trivial anti-spoofing algorithms in GPS receivers, spoofing attacks can be easily detected. The article discusses a new approach to anti-spoofing based on shielding of antennas from the signal spoofer.

INTRODUCTION

Navigating with a compass and map is an essential skill for many incident positions. Even with new technology, such as Global Navigation Satellite System (GNSS) receivers, map and compass skills are still needed. Confidence with navigation skills comes with practice and proficiency. This confidence level often impacts how a person performs during a crisis – which can result in life or death decisions. Equipment of Unmanned Vehicles (UV) today takes the character of a sustainable trend. The need for such equipment poses a lot of problems, the main of which are shown in Fig. 1.

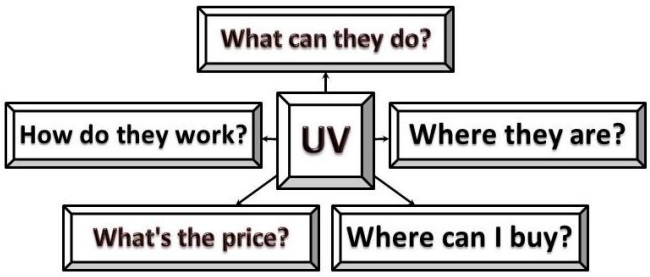


Fig. 1. *Equipment of Unmanned Vehicles (UV) and related issues*

To understand the problems of UV should be classify UV on methods of control (Fig. 2) and on the environment (Fig. 3).

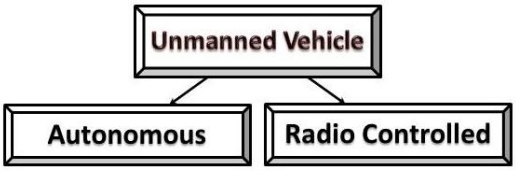


Fig. 2. *Classification of UV on methods of control*

The term "unmanned" implies the absence of a pilot on board the UV, but admits the presence of a remote human operator (remote control). If there is no pilot and no remote human operator, such UV referred to as "autonomous".

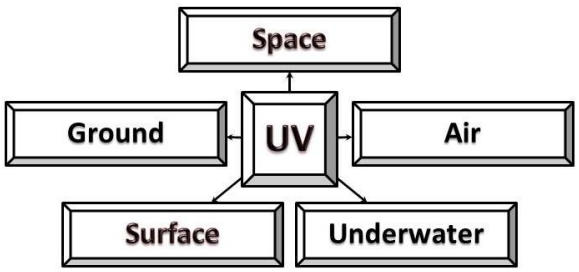


Fig. 3. *Classification of UV on the environment*

The development of modern and advanced technologies allows UV to successfully perform these functions, which in the past were not available to them or perform other forces and means. In particular, UV shown to be highly effective in carrying out the tasks of monitoring of roads, pipelines, farmland, forest fires, rivers, lakes, seas, and coastal oceans, searching of fish and others. An unmanned vehicle prevails in those industries that are as remote from humans. This is primarily warehouse logistics, mining and others. UV allow you to track and monitor the development of the situation in a given area or for a given route in real time.

It should be noted that the driving force of UV development are special-purpose technology and above all the military (Dual-Use System). And it is not only the traditional system of military intelligence, but also rapidly developing electronic warfare systems, including mobile systems noise suppression radar and radio navigation systems (jamming) [3] and mobile jamming and/or spoofing of GNSS signals [4].

1. INTERFERENCE FOR UNMANNED VEHICLES

For positioning UV used GNSS and INS. The accuracy of positioning using INS is not sufficient. GNSS corrected the work of INS. Creation a field of radio interference for GNSS is neutralizing UV. The monitoring information is not accurate snap to the area has no significant value. Furthermore themselves UV, without knowing its coordinates with a high probability cannot return to the base, and will be lost. In areas where there are woods or forest, you cannot see under the trees a objects of interest, such as human or animal, even in the winter when there are no leaves on the trees. Not by

chance all advertising UV is applied to the treeless terrain with a smooth relief, i.e. in relation to the deserts and water surfaces.

It should be emphasized the importance of UV as a means of electronic warfare, i.e., media jammers and/or spoofers of GNSS. In this case, the radar will observe hundreds of decoys and the GNSS-receiver will switched from real signals of GNSS to false signals.

2. GENERATION OF RADIO NOISE TO SUPPRESS GNSS SIGNALS (GNSS-JAMMING)

The availability and usage of low-cost GNSS jamming devices has resulted in the increased threat of intentional and unintentional disruption to commercial and industrial systems that rely on precise GNSS data. The basic scheme of jamming shows on Fig. 4.

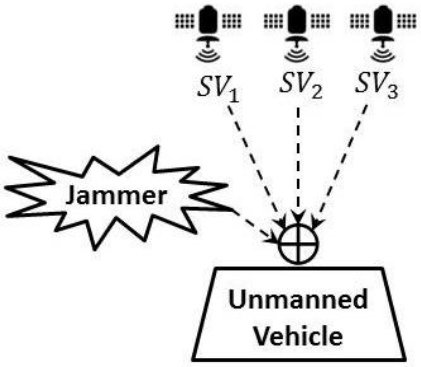


Fig. 4. *Suppression GNSS signals via radio noise generator (GNSS jamming)*

3. FALSIFICATION OF GNSS SIGNALS (GNSS-SPOOFING)

GNSS-spoofing attack is a attack, that trying to deceive GNSS receiver, broadcast transmitting slightly more powerful signal, received from the GNSS satellites and so distorted, that positioning system UV incorrectly determined its position in space and time. That is the purpose of spoofing is a real distortion of the GNSS signal to a receiver instead of the real UV coordinates of space and time $(\mathrm{x_v}, \mathrm{y_v}, \mathrm{z_v}, t_\mathrm{v})$ expected to false coordinates $(\mathrm{x_v} + \Delta x, \mathrm{y_v} + \Delta \mathrm{y}, \mathrm{z_v} + \Delta z, t_\mathrm{v} + \Delta t)$, where $\Delta x, \Delta y, \Delta z, \Delta \mathrm{t}$ – coordinate errors of vehicle UV in space and time, by repeater R. One version of the capture drone Lockheed RQ 170 in Iran in 2011 is the result of such an attack1. In 2012, it proved the feasibility of hacking and interception UV control by GNSS-spoofing2, and already in 2013 it was able to prove it in practice3. In 2014, it was forced to an emergency landing UAV MQ-5B4. All researchers note that a successful GNSS-spoofing can be performed only for positioning systems that use a standard positioning service (unencrypted civil C/A code) GNSS5. Our research has shown that the use of simple spoofer of special purpose based on GNSS signal repeater provides losing of UV control, using Y-coding, which is an encrypted version of the P-code in anti-spoofing mode [21].

4. THE MAIN SCENARIO OF GNSS SPOOFING

The main scenario of GNSS spoofing is shown in Fig. 11. Vehicle UV during normal operation carries traffic using GNSS. Terrorist, located at a distance from UV, takes GNSS signals, making them some distortions and broadcasts to the vehicle UV high power signal, sufficient to switch navigation equipment UV from the normal mode of GNSS into mode GNSS-spoofing.

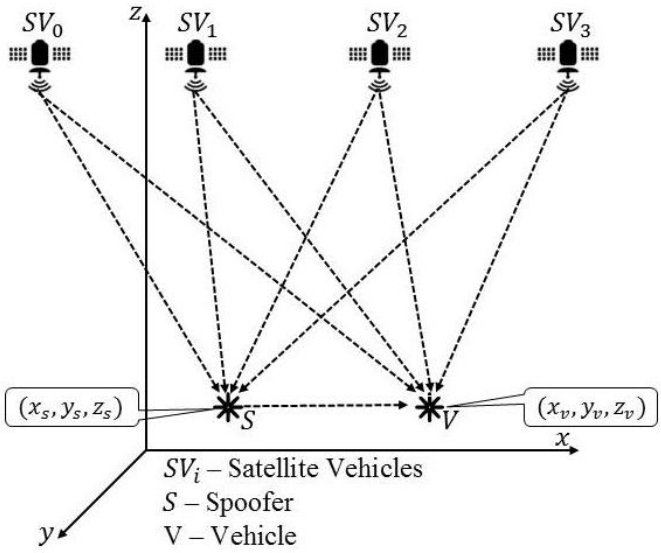


Fig. 5. *The main scenario GNSS spoofing (designate)*

5. THE SHIELDING OF UV ANTENNA FOR EASING OF GNSS-SPOOFING AND/OR JAMMING

Assume that the transmitting antenna of SV and the receiving antenna of V are at the same height, i.e. $\mathrm{z_s} = \mathrm{z}_v$. In this case V may protect against spoofing and/or jamming by a metal ring screen (Fig. 6).

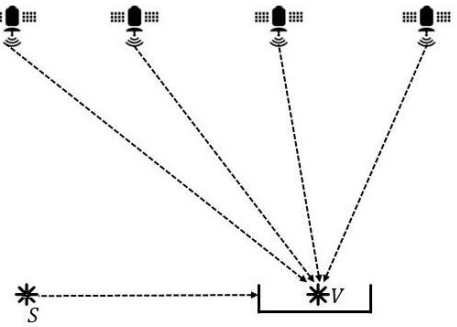


Fig. 6. *UV protection from spoofing using a metal ring screen*

Assume that the distance from S to the metallic screen is sufficiently large, to consider an electromagnetic wave, falling on the screen, is a flat wave (Fig. 7)

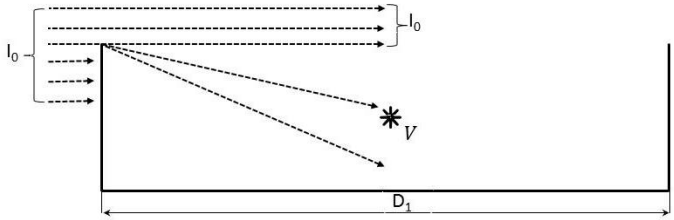


Fig. 7. *Diffraction of electromagnetic waves from a spoofer on the edge of the ring*

The reception antenna is located in the shadow of the incident wave, however, due to diffraction at half-plane, a part of the signal

[1] http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video
[2] http://www.bbc.com/russian/science/2012/06/120629_drone_spoof_hack.shtml
[3] http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea
[4] http://rbase.new-factoria.ru/news/kompleks-avtobaza-zasek-i-posadil-amerikanskiy-bpla-mq-5b-v-krymu
[5] http://rt.com/usa/texas-1000-us-government-906/

energy from the spoofer reaches the receiving antenna. A rigorous solution of diffraction problems can in principle be found on the basis of the wave equation and the boundary conditions. However, a rigorous formulation solution, due to the complexity, can be obtained in just a few simple cases.

6. THE FRESNEL DIFFRACTION AT THE EDGE OF SHIELDING RING

The distribution of wave amplitude for the half-plane metal screen in general is a complex mathematical problem. When the screen is at a short distance from the receiving antenna the intensity distribution of the diffracted wave in the near field is described by the Fresnel integral. A rigorous solution of the Fresnel diffraction at the edge of the half-plane shows that near the area of the geometrical shadow picture is a series of alternating light and dark bands, which are parallel to the edge of the half-plane and located in the illuminated region (Fig. 16).

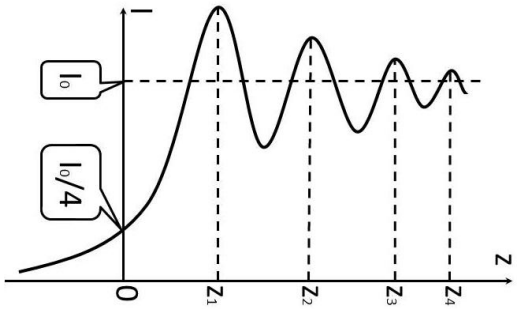


Fig. 8. *Diffraction of electromagnetic waves on the edge of the ring*

In the shadow the intensity decreases monotonically to zero, and at the boundary of geometric shadow intensity 4 times lower than the intensity of the incident wave.

7. THE REDUCTION OF DIFFRACTION AT THE EDGE OF SHIELDING RING

To reduce diffraction can be installed the second ring which have the same height H (Fig. 17).

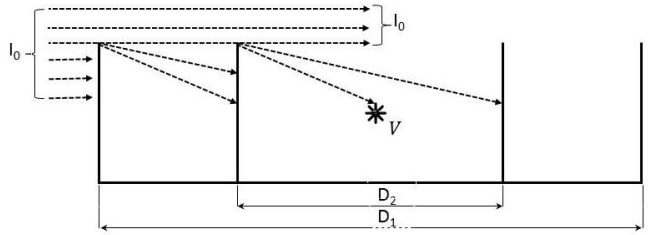


Fig. 9. *The reduction of diffraction by the second ring*

To further reduce the effects of diffraction can install the third, fourth, etc.rings. Thus, for example, Fig. 18 shows a system of screening, which consists of four concentric rings of height H.

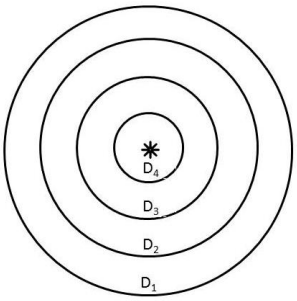


Fig. 10. *The shielding of antenna with four concentric rings*

8. THE TASK OF SHIELDED ANTENNAS DESIGNING

The task of shielded antennas designing for a given amount of shielding rings N reduces to finding the diameters D and heights H of shielding rings

$$\{D_1;\ D_2;\ \dots;\ D_N;\ H_1;\ H_2;\ \dots;\ H_N\} \quad (1)$$

In the particular case if $H_1 = H_2 = \dots = H_N$ then the task of designing is reduced to finding the diameter D of the shielding rings

$$\{D_1;\ D_2;\ \dots;\ D_N\} \quad (2)$$

If it can be assumed that

$$\{(D_1 - D_2) = (D_2 - D_3) = \cdots = (D_{N-1} - D_N) = \Delta D\}, \quad (3)$$

then the task of GNSS antennas screening is reduced to defining the diameter of the outer ring and the determination of such values ΔD, where the energy E diffracted wave, incident on the receiving antenna of UV would be minimal.

$$E(\Delta D) = E_{min} \quad (4)$$

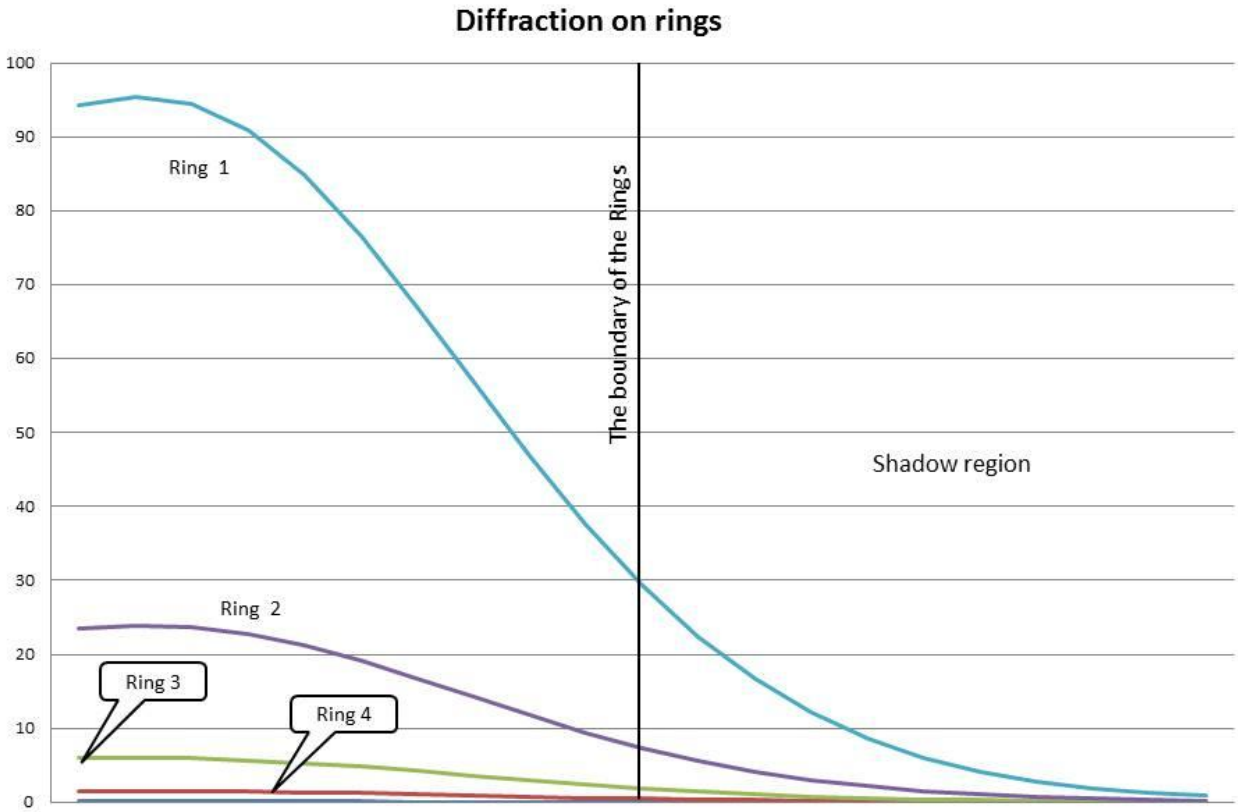
Because in the shadow the intensity of the diffracted wave decreases monotonically to zero and on the border of geometric shadow intensity 4 times less than the intensity of the incident wave, we can assume that screening system through N rings reduces the energy E of diffracted wave, incident on the receiving antenna of UV at K time:

$$K = 4^N \quad (5)$$

For example, for N=4 (Fig. 10) you can expect a decrease of the diffracted wave energy at 4^4=256 time.

9. SIMULATION OF UV SHIELDING ANTENNA

In accordance with the principle of Huygens-Fresnel we can calculate the energy of the diffracted wave by the first ring, reaches the second ring as a screen. It is known that the distribution of the operating frequency of GNSS as NAVSTAR GPS and GLONASS is in the range of 1559÷1610 MHz, which corresponds to wavelengths in the centimeter range 18.6÷19,2 cm.



Z=	0,10	0,09	0,08	0,07	0,06	0,05	0,04	0,03	0,02	0,01	0,00	-0,01	-0,02	-0,03	-0,04	-0,05	-0,06	-0,07	-0,08	-0,09	-0,10
Ring 4	1,47	1,49	1,48	1,42	1,33	1,20	1,05	0,89	0,73	0,59	0,46	0,35	0,26	0,19	0,13	0,09	0,06	0,04	0,03	0,02	0,01
Ring 3	5,89	5,96	5,91	5,68	5,30	4,79	4,19	3,55	2,93	2,35	1,84	1,40	1,04	0,76	0,54	0,37	0,25	0,17	0,11	0,08	0,05
Ring 2	23,55	23,85	23,62	22,74	21,21	19,15	16,75	14,22	11,72	9,40	7,35	5,60	4,17	3,04	2,16	1,50	1,02	0,68	0,45	0,30	0,22
Ring 1	94,20	95,40	94,49	90,95	84,82	76,60	67,01	56,86	46,87	37,60	29,39	22,41	16,69	12,14	8,63	5,99	4,06	2,71	1,79	1,21	0,88

Fig. 11. *Modeling of waves diffraction from spoofer at four rings shielding antenna in Matlab 6*

For approximate calculations we can assume that the length of the main work wave of GNSS is λ =18 cm. For $\{-10 \leq z \leq 10\}$ cm in steps of 1 cm calculated the intensity of the diffracted wave

$$I(z) = \sum_{k=0}^{99} \exp\left(i\frac{2\pi}{\lambda} * abs(z - 0{,}01k + \text{i}\Delta D, -10 \leq z \leq 10 \text{ sm}\right) \quad (6)$$

where = $\sqrt{-1}$, λ =18 cm, ΔD = 15 cm.

Diffracted wave is diffracted a second time on the ring 2 etc. on rings 3 and 4. As a result, the energy of the diffracted wave, reaching GNSS antenna, reduced at hundreds of times.

10. THE SPOOFING DETECTION USING UV SHIELDING ANTENNA

Assume that the antennas S and V are at the same height, i.e. $z_s = z_v$. In this case V can be used to detect spoofing by two metal discs, fixed on the dielectric ring (Fig. 12). Electromagnetic waves from the GNSS satellites is largely shielded by the upper metal disc, and the electromagnetic waves reflected from the surface of the ground or other objects are screened by lower metal disc. Signals from spoofer without weakening reach the antenna V.

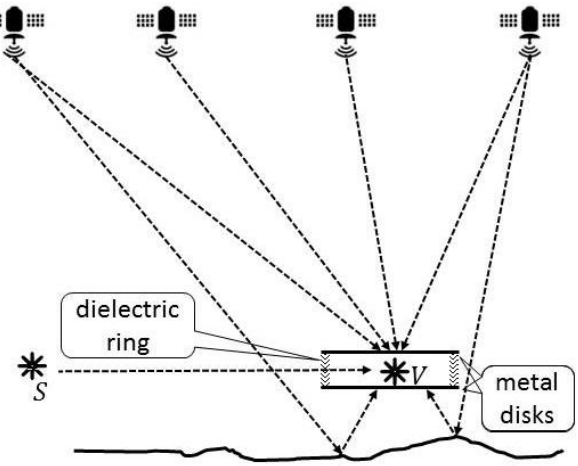


Fig. 12. *The shielding of antenna for GNSS-spoofing detecting*

CONCLUSION

It is now known a variety of approaches to the problem of detecting spoofing. For example, we have developed several methods for detecting spoofing [16-24]. In this paper, we are present a new approach to GNSS spoofing and/or jamming detection and anti-spoofing and/or anti-jamming on shielding of antennas.

Considered the case when antennas S and V are at the same height, ie, $z_s = z_v$. If the transmitting antenna of spoofer is below the receiving antenna of UV, ie $z_s < z_v$, then the energy of the diffracted wave incident on a receiving antenna is reduced. If the

transmitting antenna of spoofer is above the receiving antenna of UV, i.e. $z_s > z_v$, then the energy of the diffracted wave incident on a receiving antenna increases. If the transmitting antenna of spoofer and receiving antenna of UV are at a relatively small distance, in this case, is considered as a spherical wave and the calculation of the energy of the diffracted wave is somewhat more complicated.

In conclusion it should be emphasized that the simplifications due to the fact that the heights of the shielding rings and the same and the difference in diameter of the rings is constant are not significant. Removal of these restrictions leads to a certain complication of engineering calculations of diffraction.

BIBLIOGRAFIA

1. Association for Unmanned Vehicles Systems International (AUVSI). http://www.auvsi.org
2. Basic Land Navigation, Global Positioning System, page 5.1, National Interagency Incident Management System,2007. http://www.nwcg.gov/pms/pubs/475/PMS475_chap5.pdf
3. Sam Pullen, Grace Gao. GNSS Jamming in the Name of Privacy. INSIDE GNSS: applications of the Global Navigation Satellite Systems: GPS, Galileo, GLONASS, BeiDou, and related technologies, U.S.A. 2012. http://www.insidegnss.com/auto/marapr12-Pullen.pdf
4. Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle. GPS Vulnerability to Spoofing Threats and a Review of Anti-spoofing Techniques. International Journal of Navigation and Observation, Volume 2012 (2012), Article ID 127072, http://dx.doi.org/10.1155/2012/127072
5. Ochin Evgeny. Prezent USA do Iranu, część 1, 19.12.2011. http://youtu.be/Mj9Dafc4jqg?list=PL0C885EF8A83CA824
6. Ochin Evgeny. Prezent USA do Iranu, część 2, 19.12.2011. http://youtu.be/gTgk_eciyFQ?list=PL0C885EF8A83CA824
7. Ochin Evgeny. Anty-spoofingowa architektura GPS do systemów nawigacji bezzałogowej, 28.03.2012. https://youtu.be/TLUD26xfEfQ?list=PL0C885EF8A83CA824
8. Ochin Evgeny, Dobryakova Larisa, Lemieszewski Łukasz. Antiterrorism – design and analysis of GNSS anti-spoofing algorithm, Scientific Journals of the Maritime University of Szczecin, 2012. http://repository.scientific-journals.eu/handle/123456789/358
9. Ochin Evgeny. Antyterroryzm – projektowanie i analiza algorytmów antyspoofingu dla GNSS, 16.05.2012. https://youtu.be/mQpY9R-pIPo
10. Ochin Evgeny. Anty-spoofingowa architektura GPS do systemów nawigacji bezzałogowej, 28.03.2012. https://youtu.be/TLUD26xfEfQ
11. Ochin Evgeny, Dobryakova Larisa, Lemieszewski Łukasz. The analysis of the detecting algorithms of GNSS-spoofing, Scientific Journals of the Maritime University of Szczecin, 2013. http://repository.scientific-journals.eu/handle/123456789/561
12. Dobryakova Larisa, Lemieszewski Łukasz, Ochin Evgeny. GNSS: повышение точности позиционирования с использованием модели WCS-84, Opublikowane w Моделювання та информаційні технології/ Збірник наукових праць, випуск 68, Київ – 2013, UKD 621.396+681.511, 2013
13. Ochin Evgeny, Dobryakova Larisa, Lemieszewski Łukasz, Lusznikov Eugeniusz. The study of the spoofer's some properties with help of GNSS signal repeater, Scientific Journals of the Maritime University of Szczecin, 2013. http://repository.scientific-journals.eu/handle/123456789/581
14. Ochin Evgeny. Design and Analysis of Spoofing Detection Algorithms for GNSS Signals, 16.03.2013. https://youtu.be/qPEVa58xrz4
15. Ochin Evgeny. Репитер ГНСС сигналов в качестве спуфера, 04.02.2014. https://youtu.be/_Qwr202IF3o
16. Ochin Evgeny. Spoofing detection and anti-spoofing for GNSS controlled drones, bombs and artillery shells (in English and Russian languages), 10.07.2014. https://youtu.be/0PlQoAynlQo
17. Ochin Evgeny, Dobryakova Larisa, Lemieszewski Łukasz, Lusznikov Eugeniusz, The application of satellite compass for GNSS-spoofing detecting, Scientific Journals of the Maritime University of Szczecin, 2014. http://repository.scientific-journals.eu/handle/123456789/616
18. Dobryakova Larisa, Lemieszewski Łukasz, Ochin Evgeny, Design and analysis of spoofing detection algorithms for GNSS signals, Scientific Journals of the Maritime University of Szczecin, 2014. http://repository.scientific-journals.eu/handle/123456789/668#
19. Dobryakova Larisa, Ochin Evgeny, On the application of GNSS signal repeater as a spoofer, Scientific Journals of the Maritime University of Szczecin, 2014. http://repository.scientific-journals.eu/handle/123456789/669#
20. Ochin Evgeny. Detekcja GNSS spoofingu i bezpieczeństwo transportu, część I / Akademickie Aktualności Morskie, ISSN 1508-7786, nr 2(82)/ 2014, str. 8-10. http://am.szczecin.pl/userfiles/File/aam/AAM%202_82_2014.pdf
21. Ochin Evgeny. Detekcja GNSS spoofingu i bezpieczeństwo transportu, część II / Akademickie Aktualności Morskie, ISSN 1508-7786, nr 3(82)/ 2014, str. 12-13. http://am.szczecin.pl/userfiles/File/aam/AAM%203_83_2014.pdf
22. Larisa Dobryakova, Łukasz Lemieszewski, Evgeny Ochin. "Design and Analysis of Spoofing Detection Algorithms for GNSS Signals"/ Mechanika – Nawigacja – Transport Akademia Morska w Szczecinie, październik/listopad 2014.
23. Larisa Dobryakova, Łukasz Lemieszewski, Evgeny Ochin. " Transport safety: the GNSS spoofing detecting using two navigators" /Logistyka 3/2014, str. 1328-1331
24. Larisa Dobryakova, Łukasz Lemieszewski, Evgeny Ochin. " The main scenarios of GNSS spoofing and corresponding spoofing detection algorithms" /Logistyka 4/2014, str. 2751-2761