ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2022. No. 4 (22)*

UDC 004.6 DOI: https://doi.org/10.30837/ITSSI.2022.22.014

S. SEMENOV, Z. Z. MINJIAN, S. YENHALYCHEV, L. SMIDOVYCH

GENERALIZED MODEL OF THE ADS-B UNMANNED AERIAL VEHICLE DATA TRANSMISSION PROCESS IN A STEGANOGRAPHIC SYSTEM

The subject of the article is a model of the ADS-B data transmission process of an unmanned aerial vehicle in a steganographic system using direct spectrum expansion technology. **The aim** of the publication is to improve the security of unmanned aerial vehicles with an integrated ADS-B system. Particular scientific **tasks:** analysis of basic methods of ADS-B format data protection; development of the scheme of ADS-B drone data transfer in steganographic system with the use of direct spectrum expansion technology; improvement of the model of ADS-B drone data transfer in steganographic system with the use of direct spectrum expansion technology; determination of qualitative and quantitative characteristics as well as security properties of ADS-B format data. The following research **results** were obtained: as the result of the scientific works analysis the hypothesis about the perspectives of the ADS-B format steganographic data protection usage was put forward; the scheme of an unmanned aerial vehicle ADS-B data transmission in the steganographic system with the usage of the direct spectrum spreading technology was developed; the main safety properties as well as the safety parameters and characteristics of the ADS-B format information signal were formulated; the generalized model of an unmanned aerial vehicle ADS-B data transmission was further developed. This will improve the safety of UAVs. The advantages and disadvantages of the model were **revealed**, which allowed to determine the priority of further research and possible promising ways of solving the assigned tasks.

Keywords: unmanned aerial vehicles; security; ADS-B system; steganography; direct spectrum enhancement technology; data protection.

Introduction

Under the conditions of increased demand for the volume and speed of cargo and passenger delivery, the intensity of air transportation is steadily increasing every year. This, in turn, necessitates an increase in operational flexibility while maintaining or improving safety. The safe organization of increasingly large and complex air traffic requires the use of technologies that are more advanced, tools and means. One such important tool in the air traffic management process is aerial surveillance, in particular automatic dependent surveillance of the broadcast-type ADS-B.

Given the fact of increasing attention to unmanned aerial vehicles (UAVs), the issue of using ADS-B technology in them is also relevant.

However, ADS-B lacks explicit mechanisms to protect confidentiality, integrity and availability of data transmitted between UAVs and controlling personnel (air traffic controllers), which makes such system vulnerable to threats of cyberterrorist nature, which are especially relevant in connection with the modern development of computer technologies and programmable radio (SDR – Software Defined Radio). Therefore, the problem of increasing the security of the ADS-B data transmission process of an unmanned aerial vehicle is urgent.

Literature review

Article [1] provides an overview of the shortcomings of the ADS-B system. In addition, the paper analyzes a number of countermeasures aimed at reducing the risks of cyberattacks. However, the authors of the article do not focus on the highest-priority areas in the issue of improving ADS-B security. It should be emphasized that all the examples under consideration are more related to guided aircraft (aircraft and helicopters) and do not touch the problems of UAV.

Work [2] presents the results of comparative studies of methods to improve cybersecurity of UAVs with embedded ADS-B system. It analyzes the main types of cyber attacks on UAVs with embedded ADS-B system, developed a taxonomy of cyber attacks of modification and forced implementation of ADS-B messages. In addition, a broad review of cryptographic methods to enhance ADS-B data security was performed. The results of the review led to conclusions about their disadvantages in operation in the UAV management system, including the increased burden on the generation of public keys; the threat in case of a private key; increased hardware requirements, etc.

Also, the paper proposed the use of steganographic data methods to improve the security of the ADS-B UAV system.

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 4 (22)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

In [3] an analytical report on promising directions and modern methods of steganographic data protection is presented. The paper notes the promising direction associated with the use of direct spectrum expansion technology in steganographic systems.

The analysis of the communication system with direct spectrum spreading, as well as the feasibility and effectiveness of using this technology are considered in [4]. Unfortunately, this analysis is limited only to the military field of use, which reduces the practical value of this research.

The paper [5] describes the technology of direct spectrum enhancement for data hiding in audio. The article shows the advantage of using this technology for data security.

In [6] the research of the technology of direct spectrum expansion in steganographic system is presented in a practical application to data hiding in images. The analysis of this paper allowed us to conclude about the wide possibilities of this technology in the implementation of different types of data.

The issue of using the technology of direct spectrum expansion in steganographic system is disclosed in [7]. It describes a mathematical model and a structural scheme of a steganographic information protection system using complex discrete signals of direct spectrum expansion technology. The paper modifies the structural scheme of receiving-transmitting information in a noise-protected digital communication system using the technology of direct spectrum spreading. This technology can be the basis for further research in the framework of the problem of increasing the security of UAV using the ADS-B system.

The analysis of these works allowed us to conclude that the problem of security of UAV with built-in ADS-B system is topical, the need to develop new methods and means to improve their security. In addition, the results of the analysis allowed us to put forward a hypothesis about the possibility of using steganographic methods of data protection to improve the security of UAV with built-in ADS-B system. The basis for the developed system can be the technology of direct spectrum expansion.

Main part

By analogy with the steganographic system model considered in [7], let us introduce and justify the basic operators of steganographic transformation of ADS-B UAV data. In the developed model, it is necessary to take into account several factors, which have not found their representation in known models. Firstly, it is necessary to consider the factor that the direct spectrum expansion technology is proposed to be used as the basis for ADS-B steganographic data protection. Secondly, it is important to consider the factor of objective environmental interference and the means of their allocation. Thirdly, it is necessary to consider the peculiarities of format of transmitted digital data from ADS-B UAV devices.

The updated ADS-B UAV data transmission flowchart in the steganographic system using direct spectrum expansion technology is shown in fig. 1.

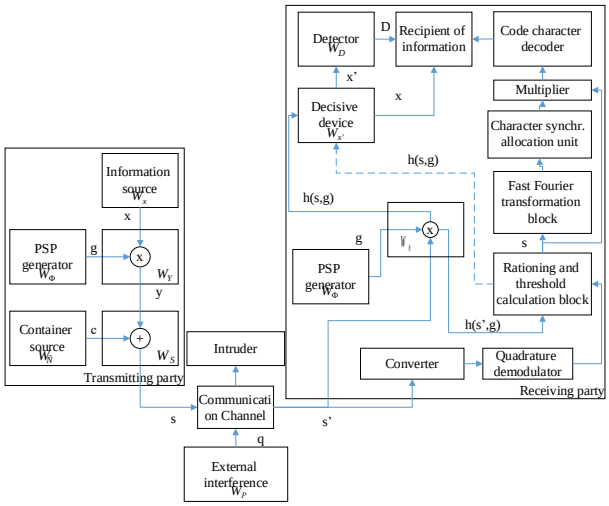

Fig. 1. Structure diagram of ADS-B UAV data transmission in steganographic system with the use of direct spectrum expansion technology

The information signal, which is formed on the basis of the digital identifier and is supposed to be embedded into the container of the ADS-B UAV data format, we denote as $x \in X$, and the operator, which formalizes the process of identifier formation, we denote as W_x. The information signal $x \in X$ in steganographic system is modeled by means of its multiplication by the expanding code signal $g = \Phi_i \in \Phi$ – a noise-like pseudo-random sequence from an ensemble $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$ of weakly correlated discrete signals. Functioning of a pseudo-random sequence generator is formalized by operator W_Φ. The extended signal can be represented in the form of the relation $y = xg \in Y$.

If we take into account the fact that the processes of information signal $x \in X$ formation, pseudo-random sequence $g = \Phi_i \in \Phi$ and extended signal $y = xg \in Y$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 4 (22)

are equivalent to the processes taking place in a broadband communication system with direct spectrum expansion, the modulation process can be formalized in the form of mapping $\phi: X \times \Phi \to Y$.

The process of operation of the ADS-B UAV tool is represented by the operator W_S. Note that the embedding of the digital signal identifier in the ADS-B UAV data container can be described as

$$s = y + c, \quad (1)$$

where the modified ADS-B UAV data s is a mapping

$$\psi: Y \times C \to S \quad (2)$$

of the filled container $s = \psi(y, c)$, realized by the operator W_S of embedding the extended signal y into the container c using a complex discrete signal g. In this case S – is a set of filled containers.

Thus, the empty data container ADS-B UAV c should be interpreted as a noise e in the communication channel, and the process of embedding the information signal in the container can be represented as a process of transmitting an enhanced signal below the noise level in a broadband covert communication system

Taking into account the factor of external interference and impacts requires its representation in the form of a block of interference in the communication channel and formalized by the operator W_P. In this case, the result of interference can be represented as $s' = sq$, where q – external interference.

As in a digital communication system, the receiving side of a steganographic system is tasked with extracting a useful signal from a mixture of noise (an empty container). Thus, the transmission of the filled container $s = y + c$ is actually the transmission of a useful signal below the noise level, i.e. such a covert transmission of information in which the transmission itself is indistinguishable from noise (distortion of the container is not detected). Since the code signal $g = \Phi_i \in \Phi$ by its statistical properties similar to noise, then the resulting filled data container ADS-B UAV (as well as enhanced signal $y = xg$) is slightly distinguishable from an empty container (from the noise in the communication channel), which allows to implement a covert data transmission.

The process of extracting a UAV identifier from an ADS-B format data container at the receiving end of a steganographic system is similar to the operation of the receiving end of a broadband communications system. Filled ADS-B UAV data container s' is processed by the correlation receiver. A multiplication procedure s' is performed to a synchronized copy of the expanding signal g. This calculates the correlation coefficient, the value of which determines the decision making rule:

$$h(s', g) = s'g = xgg + cg =$$
$$= \frac{1}{n}\sum_{z=0}^{n-1} x\left(\Phi_{i_z}\Phi_{i_z}\right) + \frac{1}{n}\sum_{z=0}^{n-1} c\Phi_{i_z} = x + h(c, g),$$

where $h(c, g)$ – correlation coefficient of the initial ADS-B UAV signal c and expanding code signal.

The process of calculating the correlation coefficient and making a decision about the received information signal ADS-B UAV can be formalized in general terms by the operators W_h and $W_{x'}$ respectively.

The result of the operation $W_{x'}$ in the form of an evaluation x' is processed by a detector designed to confirm the authenticity of the identifier x'. This procedure can be formalized by the operator W_D. The formalized evaluation of the authenticity of the identifier x' and the result of the detector operation are then output to the control device.

When describing the receiving part of ADS-B data transmission systems, consider the signal preprocessing process in the signal converter, quadrature demodulator, and normalization and threshold calculation unit.

Signal registration and recording can be performed by Software Defined Radio (SDR) hardware and software [8]. For example, based on the PXI 1062 platform [9], with the NIPXI 5600 frequency reduction module and the NIPXI 5142 ADC [10]. The output signals of this converter are samples of in-phase and quadrature components, the frequency spectrum of which is shifted to the region of zero intermediate frequency.

The quadrature counts of the complex signal go to the quadrature demodulator, where the envelope of the input signal s' is extracted. The normalization block normalizes the demodulated signal in the range from 0 to 1 and calculates the threshold.

In [11] an example is presented when the signal amplitude is subject to random fluctuations as a result of interference. Figure 2 shows a de-modulated signal from the output of the quadrature demodulator of one of the ADS-B packages, illustrating this practical case.

To reduce the probability of error when demodulating such a signal, it is proposed to perform pre-processing in the block of normalization and calculation of the threshold. This will increase the accuracy of the extraction of symbolic synchronization signals from the received message.

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 4 (22)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

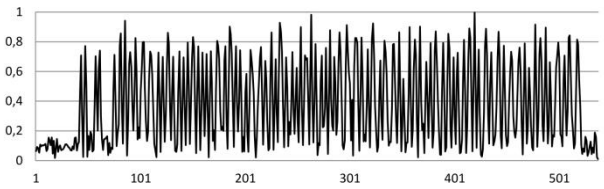

Fig. 2. Example of quadrature demodulator output signal

The analysis of the presented generalized model and the scheme of steganographic ADS-B identifier transmission system has shown that during the element-by-element addition of the modulated message with the ADS-B information signal a signal with new properties is formed. This process can be associated with the superposition of errors on the useful signal. In this case, only knowledge about the properties of the signal g makes it possible to extract the identifier, and taking into account the most important characteristics in the setup and configuration of the steganographic system will increase the level of security of the identifier.

The qualitative characteristic of the system to a large extent depends on such indicators as its noise immunity, stealth, resistance to unauthorized extraction, destruction and modification. These indicators have a great influence on the security of steganographic communication channel. Therefore, when organizing information exchange with ADS-B format data, it is necessary to take these properties into account.

It can also be noted that in a number of scientific studies [12 – 15] among the properties that characterize the security of signals, the following are noted: correlation, ensemble and structure properties.

In addition, the conducted research showed that the safety of the ADS-B UAV identifier transmission process is affected by the following characteristics: communication channel bandwidth, time of signal transmission and processing, etc.

Based on the above it can be concluded that the proposed model of ADS-B UAV data transfer in steganography system using direct spectrum enhancement technology can be used to assess the safety level of the aircraft based on the composite index

$$F_{\text{sec}} = f(PR_{sign}, \text{CH}_{link}, \text{CH}_{steg}),$$

where PR_{sign} – signal properties;

CH_{link} – link characteristics;

CH_{steg} – steganographic system characteristics.

Direct estimation of the specified characteristics and properties within the framework of the generalized model is not possible. Therefore, the study of the characteristics and properties of the complex safety indicator is possible through the implementation of mathematical models of different configuration. Such models will be the object of further research.

Conclusion

The analysis of methods to improve the cybersecurity of unmanned aerial vehicles with built-in ADS-B system, as well as promising directions in the development of formalized data protection systems was carried out. Conclusions are made about the promising direction of steganographic protection of ADS-B UAV format data.

An analysis of steganographic data protection methods has been made. A promising direction of direct spectrum enhancement technology has been singled out.

A scheme of ADS-B UAV data transmission in steganographic system with the use of direct spectrum enhancement technology has been developed.

On the basis of the developed scheme the generalized ADS-B UAV data transmission model was further developed. The model differs from the known ones by inclusion of steganographic data protection system into the existing information exchange process using the direct spread spectrum technology. This will improve the cybersecurity of the UAV with the built-in ADS-B system.

References

1. Manesh, Mohsen Riahi & Kaabouch, Naima (2017), "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system", *International Journal of Critical Infrastructure Protection*, Vol. 19 (C), P. 16–31. DOI: https://doi.org/10.1016/j.ijcip.2017.10.002
2. Semenov, S., & Zhang, M. J. (2022), "Comparative studies of methods for improving the cyber security of unmanned aerial vehicles with the built-in ADS-B system", *Advanced Information Systems*, 6 (4), P. 69–73. DOI: https://doi.org/10.20998/2522-9052.2022.4.10
3. Kuznetsov, A., Serhiienko, R., Kovtun, V., Botnov, A. (2010), "Use of Complex Discrete Signals for Steganographic Information Security", *Statistical Methods of Signal and Data Processing (SMSDP2010)*, P. 143 – 146.
4. Yihong, Gao (2022), "The analysis on the direct sequence spread spectrum communication system", *Proc. SPIE 12175, International Conference on Network Communication and Information Security (ICNCIS 2021)*, Vol. 12175. DOI: https://doi.org/10.1117/12.2628421

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2022. No. 4 (22)*

5. Kuznetsov, A, Onikiychuk, A, Peshkova, O, Gancarczyk, T, Warwas, K, Ziubina, R. (2022), "Direct Spread Spectrum Technology for Data Hiding in Audio*", Sensors (Basel)*, Vol. 22 (9), P. 3115–3138. DOI: https://doi.org/10.3390/s22093115
6. Kuznetsov, A., O. Smirnov, A. Arischenko, I. Chepurko, A., Onikiychuk, and Kuznetsova, T. (2019), "Pseudorandom Sequences for Spread Spectrum Image Steganography" *In Proceedings of the International Workshop on Cyber Hygiene (CybHyg-2019) Co-Located with 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks*, Vol. 2654.
7. Smirnov, O. A. (2012), "Method steganography hiding and withdrawal given in spatial area of the scenes with use the direct expansion of the spectrum", *Information Processing Systems*, Vol. 3 (101), P. 56–61.
8. Natarajan, Thangadurai & Kh, Chetna. (2017), "A Review on Recent Trends in Software Defined Radio Design and Applications", *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)*, 6, P. 1021–1025.
9. Iranian, M. E., Mohseni, M., Aghili, S., Parizad, A., Baghaee, H. R. and Guerrero, J. M. (2022), "Real-Time FPGA-Based HIL Emulator of Power Electronics Controllers Using NI PXI for DFIG Studies", in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, Vol. 10, No. 2, P. 2005–2019. DOI: https://doi.org/10.1109/JESTPE.2020.3023100
10. Gaurav, Jajoo, Yogesh, Kumar, Sandeep, Kumar Yadav, Bibhas, Adhikari, Ashok, Kumar, "Blind signal modulation recognition through clustering analysis of constellation signature", *Expert Systems with Applications*, Vol. 90, 2017, P. 13–22. DOI: https://doi.org/10.1016/j.eswa.2017.07.053
11. Soulat, H., Stephen, E.P., Beck, A.M. et al. (2022), "State space methods for phase amplitude coupling analysis". *Scientific Reports* 12, No. 15940. DOI: https://doi.org/10.1038/s41598-022-18475-3
12. Kuznetsov, A., Smirnov, A., Gorbacheva, L., Babenko, V. (2020), "Hiding Data in Cover Images Using a Pseudo-Random Sequences", *In Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020)*, Vol. 2608, P. 646–660.
13. Kostenko, P. YU., Simonenko, C. N., Semenov, S. G., Vasyuta, K. S. (2009), "Povysheniye skrytnosti khaoticheskikh signalov pri peredache binarnykh soobshcheniy", *Radioelektronika*, Vol. 52, No. 8, P. 13–25.
14. Knyazev, V., Lazurenko, B., Serkov, A. (2022), "Methods and tools for assessing the level of noise immunity of wireless communication channels", *Innovative Technologies and Scientific Solutions for Industries*, No. 1 (19), P. 92–98. DOI: https://doi.org/10.30837/ITSSI.2022.19.092
15. Ruban, I., Kuchuk, H., Kovalenko, A. (2017), "Redistribution of base stations load in mobile communication networks", *Innovative technologies and scientific solutions for industries*. Kharkiv., No. 1 (1), P. 75–81.

Received 21.12.2022

Відомості про авторів / Сведения об авторах / About the Authors

Семенов Сергій – доктор технічних наук, професор, Харківський національний економічний університет ім. С. Кузнеця, професор кафедри кібербезпеки та інформаційних технологій, Харків, Україна; e-mail: s_semenov@ukr.net; ORCID: http://orcid.org/0000-0003-4472-9234

Семенов Сергей – доктор технических наук, профессор, Харьковский национальный экономический университет им. С. Кузнеца, профессор кафедры кибербезопасности и информационных технологий, Харьков, Украина.

Semenov Serhii – doctor of technical sciences, professor, Simon Kuznets Kharkiv National University of Economics, professor department cyber security and information of technologies, Kharkiv, Ukraine.

Міньянг Чанг Чжэцзян – Nova intelligent technology co. Ltd, Чжецзян, Китай e-mail: minjianzhang.s@gmail.com; ORCID: https://orcid.org/0000-0002-4143-1689

Миньянг Чанг Чжецзян – Nova intelligent technology co. Ltd, Чжецзян, Китай.

Minjian Zhang Zhejiang – Nova Intelligent Technology Co. Ltd, Zhejiang, China.

Енгаличев Сергій – аспірант, Харківський національний економічний університет ім. С. Кузнеця, кафедра кібербезпеки та інформаційних технологій, Харків, Україна; e-mail: Ser.engalichev@gmail.com; ORCID: https://orcid.org/0000-0001-5298-2251

Енгалычев Сергей – аспирант, Харьковский национальный экономический университет им. С. Кузнеца, кафедра кибербезопасности и информационных технологий, Харьков, Украина.

Yenhalychev Serhii – graduate student, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine.

Смідович Леонід – кандидат технічних наук, доцент, Національний аерокосмічний університет ім. М. Є. Жуковського "ХАІ", доцент кафедри комп'ютерних наук та інформаційних технологій, Харків, Україна; e-mail: lsonlinels@gmail.com; ORCID: https://orcid.org/0000-0001-6156-9506

Смидович Леонид – кандидат технических наук, доцент, Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", доцент кафедры компьютерных наук и информационных технологий; Харьков, Украина.

Smidovych Leonid – PhD (Engineering Sciences), Associate Professor, National Aerospace University named after N. E. Zhukovsky "Kharkiv Aviation Institute", Associate Professor at the Department of Computer Science and Information Technologies; Kharkiv, Ukraine.

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 4 (22)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

УЗАГАЛЬНЕНА МОДЕЛЬ ПРОЦЕСУ ПЕРЕДАЧІ ДАНИХ ADS-B БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА В СТЕГАНОГРАФІЧНІЙ СИСТЕМІ

Предметом вивчення статті є модель процесу передачі даних ADS-B безпілотного літального апарата в стеганографічній системі з використанням технології прямого розширення спектра. **Мета** публікації – підвищення безпеки безпілотних літальних апаратів із вбудованою системою ADS-B. Конкретні наукові **завдання:** аналіз основних методів захисту даних формату ADS-B; розроблення схеми передачі даних ADS-B безпілотних літальних апаратів у стеганографічній системі з використанням технології прямого розширення спектра; удосконалення моделі процесу передачі даних ADS-B безпілотного літального апарата в стеганографічній системі з використанням технології прямого розширення спектра; визначення якісних і кількісних характеристик, а також властивостей безпеки даних формату ADS-B. Отримано такі **результати** досліджень: унаслідок аналізу наукових робіт висунуто гіпотезу про перспективність використання стеганографічного захисту даних формату ADS-B; розроблена схема передачі даних ADS-B безпілотного літального апарата в стеганографічній системі з використанням технології прямого розширення спектра; сформульовано основні властивості безпеки, а також показники та характеристики безпеки інформаційного сигналу формату ADS-B; отримала подальший розвиток узагальнена модель передачі даних ADS-B безпілотного літального апарата, що відрізняється від відомих залученням у процес інформаційного обміну, стеганографічної системи захисту даних із використанням технології прямого розширення спектра. Це дозволить підвищити безпеку БПЛ. **Виявлено** переваги й недоліки моделі, що дало змогу визначити пріоритетність подальших досліджень і можливі перспективні шляхи вирішення поставлених завдань.

Ключові слова: безпілотні літальні апарати; безпека; система ADS-B; стеганографія; технологія прямого розширення спектра; захист даних.

ОБОБЩЕННАЯ МОДЕЛЬ ПРОЦЕССА ПЕРЕДАЧИ ДАННЫХ ADS-B БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА В СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЕ

Предметом изучения в статье является модель процесса передачи данных ADS-B беспилотного летательного аппарата в стеганографической системе с использованием технологии прямого расширения спектра. **Цель** публикации – повышение безопасности беспилотных летательных аппаратов со встроенной системой ADS-B. Частные научные **задачи:** анализ основных методов защиты данных формата ADS-B; разработка схемы передачи данных ADS-B беспилотных летательных аппаратов в стеганографической системе с использованием технологии прямого расширения спектра; усовершенствование модели процесса передачи данных ADS-B беспилотного летательного аппарата в стеганографической системе с использованием технологии прямого расширения спектра; определение качественных и количественных характеристик, а также свойств безопасности данных формата ADS-B. Получены следующие **результаты** исследований: вследствие анализа научных работ выдвинута гипотеза о перспективности использования стеганографической защиты данных формата ADS-B; разработана схема передачи данных ADS-B беспилотного летательного аппарата в стеганографической системе с использованием технологии прямого расширения спектра; сформулированы основные свойства безопасности, а также показатели и характеристики безопасности информационного сигнала формата ADS-B; получила дальнейшее развитие обобщенная модель передачи данных ADS-B беспилотного летательного аппарата, которая отличается от известных включением в существующий процесс информационного обмена, стеганографической системы защиты данных с использованием технологии прямого расширения спектра. Это позволит повысить безопасность БПЛ. **Выявлены** достоинства и недостатки модели, что позволило определить приоритетность дальнейших исследований и возможные перспективные пути решения поставленных задач.

Ключевые слова: беспилотные летательные аппараты; безопасность; система ADS-B; стеганография; технология прямого расширения спектра; защита данных.

Бібліографічні описи / Bibliographic descriptions

Семенов С., Міньянг Ч. Ч., Енгаличев С., Смідович Л. Узагальнена модель процесу передачі даних ADS-B безпілотного літального апарата в стеганографічній системі. *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 4 (22). С. 14–19. DOI: https://doi.org/10.30837/ITSSI.2022.22.014

Semenov, S., Minjian, Z. Z., Yenhalychev, S., Smidovych, L. (2022), "Generalized model of the ADS-B unmanned aerial vehicle data transmission process in a steganographic system", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (22), P. 14–19. DOI: https://doi.org/10.30837/ITSSI.2022.22.014