УДК 629.7
DOI: 10.26467/2079-0619-2025-28-4-40-49

Mathematical model of threats to an aviation data network under unauthorized access

A.A. Ganichev[1], **V.I. Petrov**[1]
[1]*Moscow State Technical University of Civil Aviation, Moscow, Russia*

Abstract: Due to the increasing integration of onboard and ground-based data networks in aviation and the associated rise in information threats, the development of comprehensive models capable of assessing the security of such systems against unauthorized access is becoming increasingly necessary. One promising direction for enhancing the resilience of aviation networks is the creation of mathematical models that consider not only technical malfunctions and random equipment failures but also deliberate cyberattacks by intruders. This paper proposes a mathematical model of threats to aviation data networks, developed in accordance with ICAO recommendations and the requirements of ARINC standards. The network structure is represented as a directed graph, the nodes and edges of which are characterized by probabilistic indicators of failures and vulnerability to attacks. A distinctive feature of the developed model is the integration of probabilistic characteristics of random equipment failures, intentional attack scenarios, and parameters reflecting the efficiency of systems detecting unauthorized access. Utilizing probabilistic theory approaches, we synthesized an algorithm enabling the calculation of an integral indicator representing the risk of network connectivity loss and performance degradation. A significant aspect of this algorithm is its ability to simultaneously account for various types of threats and quantitatively assess the vulnerability of network elements. Numerical simulations of the proposed model were conducted, and results evaluating the criticality of specific network nodes and data transmission channels are presented. The analysis confirmed that applying the developed mathematical model provides a sound basis for identifying the most vulnerable aviation network components and selecting appropriate protective measures.

Key words: unauthorized interference, aviation data network, network reliability, connectivity, attack detection, risk, threat model.

For citation: Ganichev, A.A., Petrov, V.I. (2025). Mathematical model of threats to an aviation data network under unauthorized access. Civil Aviation High Technologies, vol. 28, no. 4, pp. 40–49. DOI: 10.26467/2079-0619-2025-28-4-40-49

Математическая модель угроз авиационной сети передачи данных в условиях несанкционированного вмешательства

А.А. Ганичев[1], **В.И. Петров**[1]
[1]*Московский государственный технический университет гражданской авиации, г. Москва, Россия*

Аннотация: В связи с возрастающей степенью интеграции бортовых и наземных сетей передачи данных в авиации и ростом количества информационных угроз все более необходимой становится разработка моделей, позволяющих проводить комплексную оценку защищенности таких систем от несанкционированного вмешательства. Одним из перспективных направлений повышения устойчивости авиационных сетей является создание математических моделей, позволяющих учитывать не только технические сбои и случайные отказы оборудования, но и преднамеренные атаки нарушителей. В работе предложена математическая модель угроз авиационной сети передачи данных, выполненная в соответствии с рекомендациями ИКАО и требованиями стандартов ARINC. Представление структуры сети осуществляется в виде ориентированного графа, узлы и ребра которого характеризуются вероятностными показателями отказов и подверженностью атакам. Особенностью разработанной модели является объединение вероятностных характеристик случайных отказов оборудования и сценариев целенаправленных атак, а также параметров эффективности функционирования систем обнаружения несанкционированного вмешательства. На основе подходов теории вероятностей синтезирован алгоритм, позволяющий рассчитывать интегральный показатель риска потери связности сети и деградации ее характеристик. Отличительная особенность алгоритма заключается в том, что он позволяет одновременно учитывать различные типы воздействий и производить количественную оценку уязвимости элементов сети. Выполнено численное моделирование предложенной модели, представлены результаты оценки критичности отдельных узлов сети и каналов передачи данных. Анализ результатов показал, что применение разработанной математической модели позволяет обоснованно определять наиболее уязвимые компоненты авиационной сети и выбирать адекватные меры защиты.

Ключевые слова: несанкционированное вмешательство, авиационная сеть передачи данных, надежность сети, связность, обнаружение атак, риск, модель угроз.

Для цитирования: Ганичев А.А., Петров В.И. Математическая модель угроз авиационной сети передачи данных в условиях несанкционированного вмешательства // Научный вестник МГТУ ГА. 2025. Т. 28, № 4. С. 40–49. DOI: 10.26467/2079-0619-2025-28-4-40-49

Introduction

Ensuring the protection of aviation transport networks from unauthorized interference is of paramount importance in the context of the digitalization of the aviation industry/[1] The transition of aviation communication systems from analog voice communication to the use of IP data transmission networks significantly expand their functionality, however, it is accompanied by a significant increase in the number of cyber threats[2] capable of disrupting the operation of airborne equipment and flight control systems [1–3]. In addition, the introduction of “Internet of Things” technologies and other intelligent technologies into the aviation infrastructure expands the attack coverage and leads to additional vulnerabilities [4, 5]. Interference in aviation activities can manifest itself in distorting the coordinates of the aircraft, transmitting false instructions to the crew, blocking communication channels or creating interference that prevents the exchange of critical data [2, 6]. These risks require the development of additional protective measures aimed at ensuring the reliability of aviation systems and preventing the destabilization of air traffic control [7–9].

In recent years, a number of studies have been conducted on improving protection against unauthorized interference hazards in air transport: their topics cover a wide range of areas, from organizational measures at airports [10] and the creation of integrated on-board security systems [7, 11] to modeling unauthorized impacts on aviation systems [12, 13] and the use of machine learning methods for intrusion detection [14–16]. However, the approaches proposed in these works remain fragmented and do not cover the full range of current threats to aviation data transmission networks [17, 18]. In addition, industry standards and recommendations (for example, ICAO and IATA) often do not keep pace with the rapid development of unauthorized interference methods, and existing approaches to risk assessment and testing show that the available protection tools do not cover all possible attack scenarios [6, 19].

Modern research confirms the existence of a wide range of vulnerabilities in the architecture of aviation data transmission networks. Intruders are capable of distorting route information, intercepting control signals, and disrupting the functioning of interacting subsystems. In unmanned aircraft systems, as shown in [20, 21], stable mechanisms for countering unauthorized interference have not been implemented. Cases of malicious modifications, interception of controls and destructive effects on navigation units have been recorded.

The lack of formalized approaches significantly complicates the assessment of the aviation data transmission networks stability. In [22], a laboratory platform was proposed that focuses on reproducing real-world attack scenarios, including the using SDR (software defined radio) and analysis of intersystem interactions. In [23], typical vulnerabilities of aircraft network do-

[1] Compilation of cyber security regulations, standards, and guidance. (2022). IATA. Available at: https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regs.pdf (accessed: 20.11.2024).

[2] Security and Facilitation Strategic Objective: Aviation Cybersecurity Strategy (2019). ICAO, 8 p.

mains are systematized, errors in the logical isolation of subsystems and the vulnerabilities of standard security tools are demonstrated.

However, until recent, there has been no formalized model that makes it possible to quantify the impact of both accidental equipment failures and deliberate attacks by intruders on the connectivity of the aviation network. The present work is aimed at filling this gap by developing an integrated mathematical threat model.

Methods

When the model was being developed, the recommendations of industry standards on aviation security were applied: the classification of communication channels according to ARINC 811[3] (division into protected and unsecured channels) was used and the methodological provisions of RTCA DO-356A[4] were taken into account when analyzing intervention scenarios. In accordance with this, the data transmission network (DTN) is represented as a graph of nodes and connections, for which a probabilistic reliability analysis is performed. Each node and channel of the model is characterized by uptime and failure probabilities, determined on the grounds of statistical data and the assumption of failure independence. The model introduces threats of unauthorized interference – deliberate impacts on nodes and communication lines – which are considered as additional probabilistic factors for the failure of network elements.

This approach, based on the theory of network reliability and the analysis of minimal vulnerable sets of components, makes it possible to formalize the task of ensuring the stability of the aviation network against unauthorized interference in the form of a set of probabilistic indicators. The developed model is presented below.

Development of a mathematical model

To begin with, we formalize the structure of the aviation DTN. We represent the network as a graph G with many nodes V and edges E:

$$G = (V, E). \tag{1}$$

Here V – set of nodes (vertices) of the graph, and E – multiple connections (edges) between them.

The nodes of the graph are on-board and ground computing devices (aircraft on-board computers, control center servers, repeaters, etc.). The edges of the graph correspond to data transmission channels (radio links, satellite channels, etc.) that provide communication between the nodes. It is assumed that the topology of the graph is fixed during the period under consideration, that is, the composition of nodes and the presence of channels are set initially and do not change over time.

Each element of the network has a certain reliability and, consequently, a non-zero probability of failure. Let's introduce the notation: let p_i be the probability of uptime of node i in the period under review. Then we can express:

$$q_i = 1 - p_i, \tag{2}$$

where q_i is the probability of failure of this node due to technical reasons.

Similarly, for each communication channel (edge) $e \in E$, we denote by p_e the probability of its proper functioning:

$$q_e = 1 - p_e, \tag{3}$$

where q_e is the probability of channel failure.

Let us take the simplifying assumption that failures of individual nodes and channels are statistically independent events (in reality, correlated failures may occur, but independence is allowed to facilitate analysis).

To evaluate the operability of the entire network, we introduce the concept of graph connec-

[3] ARINC Project Paper 658. Internet protocol suite (IPS) for aeronautical safety services roadmap document. (2017). ARINC Project Paper 658, 15 p.Available at: https://www.icao.int/APAC/Meetings/2017%20ACSICG4/IP05_USA%20AI.3%20-%20IPS%20Roadmap.pdf (accessed: 20.11.2024).

[4] RTCA DO-356. Airworthiness security methods and consideration. (2018). GlobalSpec, 370 p. Available at: https://standards.globalspec.com/std/10398650/rtca-do-356 (accessed: 20.11.2024).

tivity. A network is considered connected and functioning if for any pair of important nodes (for example, an on-board control center) there is at least one path connecting them through serviceable nodes and channels. A connectivity disruption event, on the contrary, means that there will be at least one pair of nodes between which there is not a single workable data transmission route left. The probability of maintaining network connectivity can be considered as an indicator of its overall reliability. Calculating this probability is equivalent to the problem of estimating the reliability of a graph with given element reliabilities.

In general, an accurate calculation of the connectivity probability for an arbitrary graph is difficult, since it requires taking into account all possible combinations of element failures. However, analytical expressions can be written for some typical network configurations. For example, if two important nodes are interconnected by a sequential chain of n channels, then the network will remain connected only if each of these channels is operational. In this case, the probability of maintaining communication between nodes is determined by the product of channel reliability:

$$R_{conn} = \prod_{e=1}^{N} p_e. \quad (4)$$

On the contrary, with redundant channels (parallel independent communication lines), the network reliability increases. For the case of two parallel channels between the same nodes, the probability that communication is **completely** lost is equal to the product of the probabilities of failure of each channel. Accordingly, the probability of maintaining communication over at least one of the two channels is written as:

$$R_{conn} = 1 - (1 - p_1)(1 - p_2). \quad (5)$$

These simplified examples illustrate how the network topology affects its reliability: the presence of alternative routes (duplicate nodes or channels) reduces the likelihood of a complete communication failure. In a real aviation network, the structure may be more complex, including many nodes and intersecting routes. For the general model, we introduce a set of minimal cuts of the graph – critical sets of components, the failure of which leads to a violation of connectivity. Let us denote by C the set of all minimal sections:

$$C = \{C_1, C_2, \dots, C_K\}, \quad (6)$$

where each C_i represents the minimum set of nodes and/or edges, at the simultaneous failure of which the graph G splits into disconnected parts. Thus, the elements of C_i are the "critical" nodes and lines that form the vulnerable point of the network.

Aviation DTN is subject not only to accidental failures, but also to targeted unauthorized influences. These include attacks on network nodes (for example, unauthorized entry into the on-board network or disabling the control server), intentional interference in communication channels (jamming the radio signal), the introduction of false commands or data, and other types of malicious actions that can disrupt the normal operation of the system. To quantify such threats, we introduce their probabilistic model. Let us assume that for each element of the network, it is possible to estimate the probability of a successful attack during the period under review. Then, by P_i^{attack} we will denote the probability that the node $i \in V$ will be compromised by an attacker, i.e. it will be attacked, disrupting its functioning. Similarly, for the $e \in E$ channel, we will introduce P_e^{attack} – the probability that a successful attack will be made on the nel e. As a rule, the values of P_i^{attack} are relatively small, but non-zero, which reflects the very possibility of a successful attack under certain conditions.

The unauthorized interference, in fact, leads to the failure of a node or channel in a similar way to a technical failure, although it has a different nature. Therefore, it is natural to consider an attack as an additional reason for component failure. Let us combine two causes of disruption – accidental failure and a successful attack – in a single probabilistic model of a network element. If we consider these reasons to be statistically independent, then the final probability that the component i will fail (either due to a failure or as a result of an attack) is determined by the expression:

$$q_j^{total} = 1 - \left(1 - q_j\right)\left(1 - P_j^{attack}\right). \qquad (7)$$

Here, q_j^{total} is the total probability of the \$i\$ element being inoperable for any of two reasons. Formula (7) shows that the element will fail if at least one of two events occurs: an internal technical failure or a successful external impact. Equivalently, you can write down the probability of fail-safe operation, taking into account attacks:

$$p_j^{total} = (1 - q_j)(1 - P_j^{attack}) \qquad (8)$$

in other words, the component will continue to function only in the absence of a failure and the absence of a successful attack.

Probabilities P_j^{attack} characterize the vulnerability of network elements. An attacker, as a rule, seeks to attack the most critical nodes and communication lines, the failure of which leads to maximum disruption of the network. In terms of the minimal cuts introduced earlier, a targeted attack can be aimed at disabling all components of a certain section C_K, which is guaranteed to disrupt the network connectivity. However, the possibility of implementing such a complex attack depends on the resources of the intruder and is reduced if the cut includes a significant number of elements. Nevertheless, the mathematical model must take into account various attack scenarios: from single attacks on individual nodes or channels to combined attacks targeting several network elements simultaneously. For each scenario, you can set the corresponding probability of threat implementation P_j^{attack} or a group of probabilities for a set of attacked elements.

An important factor reducing the impact of threats is a network-based unauthorized interference detection system. Let us assume that the monitoring and diagnostic tools have been implemented in the aviation data transmission system under consideration, which make it possible to detect anomalies in data transmission. These tools include attack detection systems, network traffic analyzers, message integrity monitoring mechanisms, and other monitoring technologies. Their main task is to timely identify the facts of an attack or abnormal behavior of the network with a high probability with a minimum number of false warnings.

Let us model the process of detecting attacks in a probabilistic setting. Let us introduce two key indicators of the effectiveness of the detection system:

(1) p_d is the probability of correctly detecting an attack (system sensitivity);

(2) p_{fa} is the probability of a false alarm, i.e. the formation of an alarm in the absence of a real threat.

If an attack occurs in the DTN, it is likely that it will be detected by monitoring tools, and it is likely that the attack will remain unnoticed and the probability will be $1 - p_d$. A value of p_d close to 1 means effective detection of almost all attacks, while a decrease in p_d indicates an increased likelihood of threats being missed. The indicator p_{fa} characterizes the selectivity of the system: in the absence of attacks, false positives occur with a probability of p_{fa}. It is desirable that p_{fa} was minimal in order to avoid excessive strain on operators and incident response systems.

Thus, the probability of a successful attack that is not detected by monitoring decreases in proportion to the detection factor p_d. Formally, we introduce the effective probability of a successful attack, taking into account the operation of the detection system:

$$\tilde{P}_j^{attack} = P_j^{attack}(1 - p_d). \qquad (9)$$

Substituting P_j^{attack} with $\tilde{P}_j^{attack}$ in formula (7) for the probability of component failure, you can recalculate the total probability of its failure, taking into account the functioning of the monitoring system. From (7), taking into account (9), we obtain for any node or channel:

$$\tilde{q}_i = 1 - \left(1 - q_j\right)\left(1 - \tilde{P}_j^{attack}\right), \qquad (10)$$

where q_j is the probability of a technical failure of a node or channel j; $\tilde{P}_j^{attack}$ is the probability of a successful undetected attack on the component j.

The values defined above allow us to estimate the total risk for DTN. By risk $P(F)$, we mean the probability of an event F in which the network loses connectivity, that is, data exchange between some nodes becomes impossible. Such an event F occurs if all components of at least one of the minimal sections of the network graph C_K fail. The probability of connectivity disruption is thus determined by a combination of independent failures and undetected attacks affecting network nodes and channels. Assuming the independence of such outcomes for different sections, it is possible to obtain an approximate estimate of the total probability as the sum of the failure probabilities of all critical sets:

$$P(F) = \sum_{k=1}^{K} \prod_{j \in C_K} \tilde{q}_i. \tag{11}$$

Formula (11) takes into account all possible critical sections of the network and, in fact, adds up the risks of loss of connectivity for each of them. This amount slightly overestimates the true value of $P(F)$, since different sections may have common components (their failure events are not independent). For a more accurate calculation, the inclusion-exclusion principle or other methods of network reliability theory would be required. Nevertheless, the resulting expression provides a useful risk assessment and allows you to compare different network configurations and options for protective measures.

If any section of the network has a significantly higher probability of failure compared to the rest, then the overall risk $P(F)$ is determined primarily by this “weak point”. For example, if there is a single critical node in the network through which all data passes, then the probability of a complete network failure is approximately equal to $\tilde{q}_i$ – the effective probability of failure of this node (taking into account attacks). In more balanced networks, where the failure of a single element does not immediately lead to the collapse of the network, several terms in (11) contribute to the risk calculation.

Discussion of the results

The obtained mathematical model makes it possible to quantify the impact of failures and unauthorized impacts on the functioning of the aviation DTN. Based on the model, it is possible to identify the most vulnerable network elements – nodes and channels included in the minimum sections with the highest probability of failure. Obviously, it is the failure of these critical components that determines the main contribution to the risk $P(F)$. The next step after assessing the risk is to develop measures to reduce it. Optimization of the aviation network protection strategy should be aimed at reducing the likelihood of successful attacks and failures of those elements that most significantly affect network connectivity, which will be reflected in future publications.

Conclusion

The paper presents a mathematical model describing the threats to the functioning of the aviation SPD in conditions of unauthorized interference. The proposed approach integrates a probabilistic model of technical failures with a model of deliberate attacks and their detection. Based on the model, analytical expressions are obtained to estimate the probability of network connectivity loss (formulas (7)–(11)) and it is shown how various factors – network topology, node reliability, attack intensity and detection efficiency – affect the overall risk of disruption. The scientific novelty of the result consists in the formal consideration of unauthorized exposure factors and security monitoring in the task of network reliability. The practical value of the work lies in the fact that the model allows you to identify the most vulnerable elements of the network and justify priority protection measures. Improving the reliability of critical nodes and channels, as well as the introduction of effective airborne detection systems, reduces the likelihood of successful attacks and thereby increases flight safety. The developed model can be used in the design of advanced information systems for quantifying the risk of interference and optimal allocation of protection resources.

References

1. **Ukwandu, E., Ben-Farah, M.A., Hindy, H. et al.** (2022). Cyber-security challenges in aviation industry: a review of current and future trends. *Information*, vol. 13, no. 3, ID: 146. DOI: 10.3390/info13030146 (accessed: 20.11.2024).

2. **Ben Mahmoud, M.S., Pirovano, A., Larrieu, N.** (2014). Aeronautical communication transition from analog to digital data: A network security survey. *Computer Science Review*, vol. 11–12, pp. 1–29. DOI: 10.1016/j.cosrev.2014.02.001

3. **Kızılcan, S., Mızrak, K.C.** (2022). Cyber attacks in civil aviation and the concept of cyber security. *International Journal of Disciplines Economics & Administrative Sciences Studies*, vol. 8, no. 47, pp. 742–752. DOI: 10.29228/ideas.65891

4. **Gaurav, D., Gaurav, Ch., Vikas, S., Ilsun, Y., Kim-Kwang, R.Ch.** (2022). Cyber security challenges in aviation communication, navigation, and surveillance. *Computers & Security*, vol. 113. ID: 102516. DOI: 10.1016/j.cose.2021.102516 (accessed: 20.11.2024).

5. **Kagalwalla, N., Churi, P.P.** (2019). Cybersecurity in aviation: An intrinsic review. *In: 2019 5th International Conference On Computing, Communication, Control and Automation (ICCUBEA)*, India, Pune, pp. 1–6. DOI: 10.1109/ICCUBEA47591.2019.9128483 (accessed: 20.11.2024).

6. **Corretjer, P.J.** (2018). A Cybersecurity analysis of today's commercial aircrafts and aviation industry systems: A thesis master of science. USA, NY, Utica College, 22 p.

7. **Kulik, A.A., Bolshakov, A.A.** (2021). Methodological approaches to development of intelligent aviation safety control system. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, no. 3, pp. 41–48. DOI: 10.24143/2072-9502-2021-3-41-48 (in Russian)

8. **Basora, L., Olive, X., Dubot, T.** (2019). Recent advances in anomaly detection methods applied to aviation. *Aerospace*, vol. 6, no. 11, ID: 117. DOI: 10.3390/aerospace6110117 (accessed: 20.11.2024).

9. **Zhang, R., Liu, G., Liu, J., Nees, J.P.** (2018). Analysis of message attacks in aviation data-link communication. *IEEE Access*, vol. 6, pp. 455–463. DOI: 10.1109/ACCESS.2017.2767059 (accessed: 20.11.2024).

10. **Meshankov, D.V., Tikhonov, A.I.** (2021). Implementation of a new safety information system. *Moscow Economic Journal*, no. 10. DOI: 10.24411/2413-046X-2021-10601 (accessed: 20.11.2024). (in Russian)

11. **Koptev, D.S., Mukhin, I.E.** (2020). Concept of integrated airborne systems for providing aircraft operations safety, including systems for monitoring the functional state of the operator. *T-Comm*, vol. 14, no. 12, pp. 58–65. DOI: 10.36724/2072-8735-2020-14-12-58-65

12. **Ganichev, A.A., Pitelinskiy, K.V., Britvina, V.V.** (2024). Statistical analysis of potential threats to information security in the aircraft on-board network. *Information security questions*, no. 1 (144), pp. 11–22. DOI: 10.52190/2073-2600_2024_1_11 (in Russian)

13. **Petrov, V.I.** (2016). Undeclared Capabilities of Aircraft Onboard Computer Software. *In: Grazhdanskaya aviatsiya na sovremennom etape razvitiya nauki, tekhniki i obshchestva: sbornik tezisov dokladov Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii, posvyashchennoy 45-letiyu Universiteta*, p. 160. (in Russian)

14. **Taleqani, A.R., Nygard, K.E., Bridgelall, R., Hough, J.** (2018). Machine learning approach to cyber security in aviation. *In: 2018 IEEE International Conference on Electro/Information Technology (EIT)*, Rochester, MI, USA, pp. 0147–0152. DOI: 10.1109/EIT.2018.8500165

15. **Wrana, M.M., Elsayed, M., Lounis, K., Mansour, Z., Ding, S., Zulkernine, M.** (2022). OD1NF1ST: True skip intrusion detection and avionics network cyber-attack simulation. *ACM Transactions on Cyber-Physical Systems*, vol. 6, no. 4, ID: 33, 27 p. DOI: 10.1145/3551893 (accessed: 20.11.2024).

16. **Mashoshin, A.O.** (2021). Message verification of the automatic dependent surveillance system under unauthorized intervention using the monolateration method. *Scientific Bulletin of the State Scientific Research Institute of Civil*

Aviation (GosNII GA), no. 37, pp. 136–145. (in Russian)

17. Ganichev, A.A., Pitelinskiy, K.V., Kesel, S.A., Pikov, V.A. (2024). Threat model of unauthorized interference in wireless avionics information systems. *Information security questions*, no. 4 (147), pp. 35–43. DOI: 10.52190/2073-2600_2024_4_35 (in Russian)

18. Petrov, V.I. (2017). The technique of analysis of software of on-board computers of air vessel to absence of undeclared capabilities by signature-heuristic way. *Civil Aviation High Technologies*, vol. 20, no. 1, pp. 186–193. (in Russian)

19. Kessler, G.C., Craiger, J.P. (2018). Aviation cybersecurity: An overview. *In: The National Training Aircraft Symposium (NTAS) 2018*. Available at: https://commons.erau.edu/ntas/2018/presentations/37/ (accessed: 20.11.2024).

20. Israfilov, A. (2024). Contemporary challenges in cybersecurity of unmanned aerial systems. *Universum: Technical Sciences*, no. 2 (119). Available at: https://7universum.com/ru/tech/archive/item/16760 (accessed: 20.11.2024). (in Russian)

21. Lyanguzov, D.A., Plyusnin, N.I. (2023). Security and vulnerability of unmanned aerial vehicle networks: a review. *Izvestiya Tulskogo gosudarstvennogo universiteta. Tekhnicheskiye nauki*, issue 7, pp. 528–529. DOI: 10.24412/2071-6168-2023-7-528-529 (in Russian)

22. Costin, A., Turtiainen, H., Khandker, S., Hämäläinen, T. (2023). Towards a unified cybersecurity testing lab for satellite, aerospace, avionics, maritime, drone (SAAMD) technologies and communications. *Cryptography and Security*. DOI: 10.48550/arXiv.2302.08359 (accessed: 20.11.2024).

23. Habler, E., Bitton, R., Shabtai, A. (2022). Evaluating the security of aircraft systems. *Cryptography and Security*, 38 p. DOI: 10.48550/arXiv.2209.04028 (accessed: 20.11.2024).

Список литературы

1. **Ukwandu E., Ben-Farah M.A., Hindy H. и др.** Cyber-security challenges in aviation industry: a review of current and future trends [Электронный ресурс] // Information. 2022. Vol. 13, no. 3. ID: 146. DOI: 10.3390/info13030146 (дата обращения: 20.11.2024).

2. **Ben Mahmoud M.S., Pirovano A., Larrieu N.** Aeronautical communication transition from analog to digital data: A network security survey // Computer Science Review. 2014. Vol. 11–12. Pp. 1–29. DOI: 10.1016/j.cosrev.2014.02.001

3. **Kızılcan S., Mızrak K.C.** Cyber attacks in civil aviation and the concept of cyber security // International Journal of Disciplines Economics & Administrative Sciences Studies. 2022. Vol. 8, no. 47. Pp. 742–752. DOI: 10.29228/ideas.65891

4. **Gaurav D.** Cyber security challenges in aviation communication, navigation, and surveillance / D. Gaurav, Ch. Gaurav, S. Vikas, Y. Ilsun, R.Ch. Kim-Kwang [Электронный ресурс] // Computers & Security. 2022. Vol. 113. ID: 102516. DOI: 10.1016/j.cose.2021.102516 (дата обращения: 20.11.2024).

5. **Kagalwalla N., Churi P.P.** Cybersecurity in aviation: An intrinsic review [Электронный ресурс] // 2019 5th International Conference On Computing, Communication, Control and Automation (ICCUBEA). India, Pune, 2019. Pp. 1–6. DOI: 10.1109/ICCUBEA47591.2019.9128483 (дата обращения: 20.11.2024).

6. **Corretjer P.J.** A Cybersecurity analysis of today’s commercial aircrafts and aviation industry systems: A thesis master of science. USA, NY, Utica College, 2018. 22 p.

7. **Кулик А.А., Большаков А.А.** Методологические подходы к разработке интеллектуальной авиационной системы управления безопасностью полетов // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2021. № 3. С. 41–48. DOI: 10.24143/2072-9502-2021-3-41-48

8. **Basora L., Olive X., Dubot T.** Recent advances in anomaly detection methods applied to aviation [Электронный ресурс] // Aerospace. 2019. Vol. 6, no. 11. ID: 117. DOI: 10.3390/aerospace6110117 (дата обращения: 20.11.2024).

9. **Zhang R.** Analysis of message attacks in aviation data-link communication / R. Zhang, G. Liu, J. Liu, J.P. Nees [Электронный ресурс] // IEEE Access. 2018. Vol. 6. Pp. 455–463. DOI:

10.1109/ACCESS.2017.2767059 (дата обращения: 20.11.2024).

10. **Мешанков Д.М., Тихонов А.И.** Внедрение новой информационной системы обеспечения безопасности полетов [Электронный ресурс] // Московский экономический журнал. 2021. № 10. DOI: 10.24411/2413-046X-2021-10601 (дата обращения: 20.11.2024).

11. **Коптев Д.С., Мухин И.Е.** Концепция разработки комплексных бортовых систем обеспечения безопасности полетов воздушных судов, включая системы контроля функционального состояния оператора // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14, № 12. С. 58–65. DOI: 10.36724/2072-8735-2020-14-12-58-65

12. **Ганичев А.А., Пителинский К.В., Бритвина В.В.** Статистический анализ потенциальных угроз информационной безопасности в бортовой сети воздушного судна // Вопросы защиты информации. 2024. № 1 (144). С. 11–22. DOI 10.52190/2073-2600_2024_1_11

13. **Петров В.И.** Недекларированные возможности программного обеспечения бортовых компьютеров воздушного судна // Гражданская авиация на современном этапе развития науки, техники и общества: сборник тезисов докладов Международной научно-техн. конференции, посвященной 45-летию Университета. Москва, 18–20 мая 2016 года. М.: ИД Академии имени Н.Е. Жуковского, 2016. С. 160.

14. **Taleqani A.R.** Machine learning approach to cyber security in aviation / A.R. Taleqani, K.E. Nygard, R. Bridgelall, J. Hough // 2018 IEEE International Conference on Electro/Information Technology (EIT). USA, MI, Rochester, 2018. Pp. 0147–0152. DOI: 10.1109/EIT.2018.8500165

15. **Wrana M.M.** OD1NF1ST: True skip intrusion detection and avionics network cyberattack simulation / M.M. Wrana, M. Elsayed, K. Lounis, Z. Mansour, S. Ding, M. Zulkernine [Электронный ресурс] // ACM Transactions on Cyber-Physical Systems. 2022. Vol. 6, no. 4. ID: 33. 27 p. DOI: 10.1145/3551893 (дата обращения: 20.11.2024).

16. **Машошин А.О.** Определение истинности сообщений системы автоматического зависимого наблюдения в условиях несанкционированного вмешательства на управление воздушным движением за счет метода монолатерации // Научный вестник ГосНИИ ГА. 2021. № 37. С. 136–145.

17. **Ганичев А.А.** Модель угроз несанкционированного вмешательства в беспроводных информационных системах авионики / А.А. Ганичев, К.В. Пителинский, С.А. Кесель, В.А. Пиков // Вопросы защиты информации. 2024. № 4 (147). С. 35–43. DOI: 10.52190/2073-2600_2024_4_35

18. **Петров В.И.** Методика анализа программного обеспечения бортовых компьютеров воздушного судна на отсутствие недекларированных возможностей сигнатурно-эвристическим способом // Научный вестник МГТУ ГА. 2017. Т. 20, № 1. С. 186–193.

19. **Kessler G.C., Craiger J.P.** Aviation cybersecurity: An overview [Электронный ресурс] // The National Training Aircraft Symposium (NTAS) 2018. URL: https://commons.erau.edu/ntas/2018/presentations/37/ (дата обращения: 20.11.2024).

20. **Исрафилов А.** Современные вызовы в области кибербезопасности беспилотных авиационных систем [Электронный ресурс] // Universum: технические науки. 2024. № 2 (119). URL: https://7universum.com/ru/tech/archive/item/16760 (дата обращения: 20.11.2024).

21. **Лянгузов Д.А., Плюснин Н.И.** Безопасность и уязвимость сетей беспилотных летательных аппаратов: обзор // Известия ТулГУ. Технические науки. 2023. Вып. 7. С. 528–529. DOI: 10.24412/2071-6168-2023-7-528-529

22. **Costin A.** Towards a unified cybersecurity testing lab for satellite, aerospace, avionics, maritime, drone (SAAMD) technologies and communications / A. Costin, H. Turtiainen, S. Khandker, T. Hämäläinen [Электронный ресурс] // Cryptography and Security. 2023. DOI: 10.48550/arXiv.2302.08359 (дата обращения: 20.11.2024).

23. **Habler E., Bitton R., Shabtai A.** Evaluating the security of aircraft systems [Электронный ресурс] // Cryptography and Security. 2022. 38 p. DOI: 10.48550/arXiv.2209.04028 (дата обращения: 20.11.2024).

Information about the authors

Alexandr A. Ganichev, Senior Lecturer, the Chair of Fundamentals of Radio Engineering and Information Security, Moscow State Technical University of Civil Aviation, alexunderlich@gmail.com.

Viktor I. Petrov, Candidate of Technical Sciences, Associate Professor, the Head of the Chair of Fundamentals of Radio Engineering and Information Security, the Dean of the Faculty of Aviation Systems and Complexes, Moscow State Technical University of Civil Aviation, v.petrov@mstuca.ru.

Сведения об авторах

Ганичев Александр Александрович, старший преподаватель кафедры основ радиотехники и защиты информации МГТУ ГА, alexunderlich@gmail.com.

Петров Виктор Иванович, кандидат технических наук, доцент, заведующий кафедрой основ радиотехники и защиты информации, декан факультета авиационных систем и комплексов МГТУ ГА, v.petrov@mstuca.ru.

Поступила в редакцию	24.03.2025	Received	24.03.2025
Одобрена после рецензирования	30.04.2025	Approved after reviewing	30.04.2025
Принята в печать	24.07.2025	Accepted for publication	24.07.2025