Section 1

USING ZERO TRUST TECHNOLOGIES TO PROTECT UAVs IN THE MODERN CYBERSPACE ENVIRONMENT

Ruslan Demura
National Aerospace University «Kharkiv Aviation Institute»
Research adviser: Vyacheslav Kharchenko
Language adviser: Iryna Shulga

The relevance of ensuring cybersecurity of unmanned aerial vehicles (UAVs) is rapidly increasing. Their growing popularity in military commercial and research applications is becoming critical [1]. In this context, the Zero Trust approach, which focuses on verifying every interaction in the network, offers a reliable way to protect UAV communication channels, control and operating systems. In today's cyberspace, it is of vital importance to prevent unauthorised access, data interception and drone hacking by providing protection through authentication, segmentation and monitoring.

The purpose of this paper is to substantiate the need for and propose the use of Zero Trust technology to protect information assets of UAVs operating in the modern aggressive cyberspace.

Main points. Zero Trust is a cybersecurity model that provides for the verification of every user and device without trust by default, regardless of their location [2].

Key arguments that determine the need to use Zero Trust to protect UAV cyber assets:

- vulnerabilities in UAV communication channels and control systems can lead to data loss, technology theft, or disruption of operations [3];
- Zero Trust implies the absence of «trust» between network elements meaning that every interaction in the system must be verified and protected;
- Zero Trust requires multi-level authentication and reliable data encryption to provide protection even if a part of the network is compromised [4];
- for secure Zero Trust operations, artificial intelligence and machine learning algorithms are used to analyze network behavior, which helps to detect suspicious activities and respond to them before they cause harm;
- the network segmentation limits each device access only to the resources it needs [5];
- with the development of swarm technologies, Zero Trust approaches can scale to protect hundreds of UAVs in swarms that interact with each other and with the base station;

– as cyber threats and cyberattack tools become more sophisticated, the importance of Zero Trust for UAVs is increasing. Modern research and technology is aimed at creating adaptive solutions that will protect UAVs, even in conditions of unstable communication and dynamic combat situations.

Conclusions. The research identifies specific challenges that arise when adapting Zero Trust for unmanned aerial vehicles due to limited computing resources and unstable connectivity. The research found that multi-level authentication, continuous anomaly monitoring, and dynamic network segmentation can significantly reduce UAV security risks, even in the event a compromise of individual system elements.

List of references

1. Syed N., Shah S., Shaghaghi A., Anwar A., Baig Z., Doss R. Zero trust architecture (ZTA): A comprehensive survey. IEEE Access 2024, 11. 57143–57179. DOI: 10.1109/access.2022.3174679.
2. V. Stafford, «Zero trust architecture», NIST special publication, Volume 800, Page 207, 2020.
3. Dhar S., Bose I., «Securing IoT Devices Using Zero Trust and Blockchain», Journal of Organizational Computing and Electronic. 2021. Volume 31(1). Page 18-34.
4. Phiayura P., Teerakanok S. A Comprehensive Framework for Migrating to Zero Trust Architecture. IEEE Access. 2023. Page 1. DOI: https://doi.org/10.1109/access.2023.3248622.
5. Li S., Iqbal M., Saxena N. Future Industry Internet of Things with Zero-trust Security. Information Systems Frontiers 2022.

Information about the authors

Ruslan Demura, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», r.i.demura@csn.khai.edu

Vyacheslav Kharchenko, Doctor of Science, Professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», v.kharchenko@csn.khai.edu

Iryna Shulga, PhD of Pedagogic Sciences, associate professor, Head of the Department of Foreign Languages, National Aerospace University «Kharkiv Aviation Institute», i.shulga@khai.edu