REFERENCES

1. Build Facility. SpaceX – Mission. [Electronic resource]. – Access mode: https://www.spacex.com/mission/
2. Falcon 9 Launch Vehicle. Payload User's Guide. 2021. [Electronic resource]. – Access mode: https://www.spacex.com/media/falcon-users-guide-2021-09.pdf
3. SpaceX Falcon Data Sheet: Space Launch Report. 2007. [Electronic resource]. – Access mode: https://web.archive.org/web/20071207012921 http://www.geocities.com/launchreport/falcon.html#config

B. Cherniavskyi, D. Chernetchenko, O. Hurko

COMMUNICATION USING MULTI-FACTOR ENCRYPTION WITH SECOND FACTOR VARIATIONS

The growing number of web service and radio receiver integrations necessitates the encryption of confidential data at all levels. Standard security methods, such as Basic Authentication and Digest Access Authentication, do not cover the advanced content encoding methods of transmitted messages that require a secure communication channel. Using a second factor in such systems will eliminate third-party interference with the channel and nullify the chances of obtaining the original content of requests [2, p.5-6].

Known 2FA application protection methods [1, p. 8-12]:

1. One Time Password (OTP) – a password that is engengered once, randomly, and can be sent via SMS or generated using a dedicated application.
2. Biometric Authentication – uses the user's physical characteristics, such as a fingerprint or iris scan.
3. Hardware Key – a physical device for generating random codes.

Main advantages of using 2FA encryption [1, p. 8-12]:

1. Increased security: This is an additional layer of security that makes it difficult for attackers to access data.
2. Adaptability: Code generation can take place without access to the Internet and the ability to combine several authentication methods. The variability of their use intervals ranges from seconds to weeks or months.
3. Convenience: Does not require any technical knowledge or special user skills.

Main disadvantages of using 2FA encryption:

1. Cost: Hardware and biometric keys are very expensive to use.

2. Complexity: They can be difficult to set up and as a result special skills are necessary for their combining.

3. Incompatibility: Inability to use some methods on specific platforms.

The proposed approach to the development of web service and radio receiver integrations allows for flexible system configuration methods, complicates access to transmitted data in real time, and in case of their storage on a medium. Combining 2FA methods with classical cryptography will significantly improve system security. The development of technologies and portable gadgets makes it easy to integrate into existing services.

Research on the vulnerabilities of this method has shown a fairly good level of protection. But it has drawbacks in social engineering, a weak first factor of protection, loss of a physical key, and architecturally incorrect solutions in software development.

REFERENCES

1. Bedel, C., Thelander, M. (2018). *Multifactor Authentication (for Dummies).* New Jersey: y John Wiley & Sons. P. 8-12.
2. M'Raihi, D., Rydell, J., Pei, M., Machani, S. TOTP: Time-Based One-Time Password Algorithm. The *IETF Datatracker*. 2011, May,p. 5-6. Retrieved from https://datatracker.ietf.org/doc/rfc6238/

M. Dalik, T. Kadilnikova, O. Hurko

SELECTION OF VIBRATION PROTECTION FOR ROBOTIC PLATFORMS

In the modern world, there is a noticeable increase in the utilization of robotic platforms across various sectors of engineering and manufacturing. They are actively employed in transportation, agriculture, as well as in the realms of security and surveillance, demonstrating their flexibility and versatility, thereby enabling the optimization of diverse processes and enhancing operational efficiency under varied conditions.

A robotic platform can be viewed as a working mechanism, comprising a sufficiently rigid body connected to a stationary base through elastic elements. Ensuring acceptable vibration parameters of such a construction becomes imperative.