UDK 004; 62-5

CYBERSECURITY OF DIGITAL TWINS OF INTELLIGENT CONTROL SYSTEMS OF MOBILE EQUIPMENT

[1]Puzanova K. A., [2]Puzanov A. V.
[1]Moscow Aviation Institute (National Research University), Moscow, Russia, puzanova_2017_ksu@mail.ru
[2]Kovrov State Technological Academy named V.A. Degtyarev, Kovrov, Russia, puzanov@dksta.ru

With the development of information technologies and the corresponding element base, there is a separate direction of illegal actions aimed at digital twins and systems for managing technical objects. The paper considers general issues of the direction of ensuring cybersecurity of digital twins and associated intelligent control systems of mobile equipment.

A digital twin is a virtual copy of a real object – a system, structure or process that reliably reproduces all processes occurring on the original object in real time, so that at each moment in time the co-standing parameters of the digital twin correspond to the parameters of the state of the physical object. Modern technical objects are equipped with an intelligent control system, including hardware and software, digital sensors, interfaces and other means of interaction with the outside world and between internal components [1–3]. Intelligent control systems - devices equipped with information mining tools and interacting with each other and the environment. The progress of technological advances in low-power microelectronics has predetermined the widespread adoption of devices based on them in technical facilities of the industrial and household segments, stationary and mobile versions.

Currently, there is an increase in the number of incidents (crimes) in the field of information technology, in relation to technical facilities with digital control systems. In 2018, the number of smart devices connected to the Web was estimated at 22 billion with the prospect of growth to about 40 billion by 2025 (data from the research company Strategy Analytics). These smart devices can contain vulnerabilities that can be exploited by cybercriminals and result in user or community threats [2]. Thus, the task of increasing the resistance to cyber-attacks of digital twins and related technical objects is an urgent scientific and technical task.

Security concerns for digital twins and intelligent technical facility management systems [3]:

- vulnerability of devices and systems;
- convergence of information and operational technologies;
- outdated industrial control systems;
- unsafe protocols;
- human factor;
- unused functions;
- ensuring the safety of the product after its implementation.

One of the reasons for the development and updating of cyber threats is the fact that the basic technologies for the implementation of both digital twins and related digital control systems for technical objects are developed without taking into account security requirements, since the main task of manufacturers was to minimize the cost and time of development, reduce unnecessary production costs and increase the volume of products. As a result of such a policy, basic models, central and nodal mick-rochips operate at extreme modes. Due to insufficient computing resources, most security tools for technical objects cannot be installed in inherited devices, which makes them an easy target for cybercrime [4].

Cybersecurity is considered as a system for protecting information and automated control systems from cyber-attacks, it is designed to ensure:

1. Continuity of operation.
2. Efficiency of the control system in accordance with the set goals [5].
3. Stability of control system parameters preservation [6].
4. Control system reliability [7].
5. The required level of confidence in the cybersecurity system [8].
6. The ability to adapt the management system to new and abnormal situations.
7. Substantiating the structure of the cybersecurity system based on the digital risk management model [9, 10].

The main areas of cyber threats [11]:

1. Intentional actions: malware; exploit; target attack; DDoS attack; compromised device; loss of confidentiality; modification of information.
2. Information interception: man-in-the-middle attack; connecting to an active session interception of information; network intelligence; intercept the connection
3. Disconnection: Power off; Device failure System failure loss of support service.
4. Technical failure: software-level vulnerabilities: third-party bugs.
5. Disasters: natural disasters; IoT crashes.
6. Physical attack: device modification; destruction of the device.

Components of intelligent mobile control systems that are potentially vulnerable to cyber attacks:

– digital modules of control systems (equipped with built-in technologies for collecting, processing, storing, transmitting information, intelligent decision-making);
– computer systems;
– communication components (between devices, including through the network);
– information processing components (of various types: video or audio, data generated in real time by intelligent sensors, devices, etc.);
– collaborative systems (industrial robots performing complex tasks using intelligent self-training systems);
– systems of artificial intelligence, machine learning, predictive analytics;
– monitoring systems (components of data collection and accumulation and processing, including safety of system components);
– virtual reality systems.

The cybersecurity of digital twins is implemented on the base platform using its software and hardware. In addition, data exchange channels are protected using software and hardware protection, integrity control and storage of transmitted data.

Cybersecurity of intelligent systems for managing technical facilities is implemented in the following areas: hardware, software or combined protection [12]. The hardware protection may be as built into the processor or as a separate device. Protection of intelligent control systems of technical facilities is designed to ensure the integrity of system and application software, data protection (encryption of collection, transmission, storage), as well as protection of communication lines (encryption, integrity control).

Conclusion.

With the development of information technologies and the corresponding element base, a separate direction of illegal actions arises, focused on digital twins and systems for managing technical objects. Depending on the technical and software solutions used, it is necessary to use software and hardware to minimize the likelihood of damage to systems, as well as to restore them as soon as possible.

The need to ensure cybersecurity of the digital twins themselves as virtual standards of a real object is updated, since the digital twin changes to assess the relevance of the work of the real object and identify deviations in work caused by a cyber attack, as well as assess damage caused by a cyber attack.

The last, but no less important point is the cybersecurity of transmission, integrity control and data storage systems.

References

1. National Technology Initiative (NTI) [Electronic resource]. – Mode of access: https://fea.ru/compound/national-technology-initiative. – Date of access: 03.08.2021.

2. Puzanov, A. V. Multidisciplinary analysis of control systems of mobile equipment / A. V. Puzanov // Automation. Modern technology. – 2016. – № 10. – P. 13–17.

3. Puzanov, A. V. Transdisciplinary models of hydraulic drives of mobile machinery // System analysis and applied informatics. – 2018. – № 4. – P. 51–55.

4. Internet of things – from research and innovation to market deployment [Electronic resource] / O. Vermesan, P. Friess (eds.). – Aalborg: River Publishers, 2014. – 373 p. – (River Publishers Series in Communications). – Mode of access:https://www.riverpublishers.com/pdf/ebook/RP_E978879310589702958.pdf. – Date of access: 20.06.2021.

5. Vereshchagina, E. A. Internet of Things Security Issues. Textbook / E. A. Vereshchagina, I. O. Kapetsky, A. S. Yarmonov. – M.: World of Science, 2021.

6. Erguler, I. A potential weakness in RFID-based Internet-of-things systems / I. Erguler // Pervasive and Mobile Computing. – 2015. – Vol. 20. – P. 115–126.

6. Encyclopedia of Cybernetics V. M. Glushkov. – Kyiv, 1974. – Vol. 1.

7. Gorsky, Yu. M. Homeostatics of living, technical, social and eco-logical systems / Yu. M.Gorsky [et al.]. – Novosibirsk: Science, 1990.

8. GOST 27.002–2015. Interstate standard. Reliability in technology. Terms and definitions.

9. GOST R ISO/IEC 15408-1-2012 Information technology. Methods and means of safety assurance. Criteria for assessing the safety of information technologies.

10. Minzov, A. S., A. Yu. Nevsky, O. R. Baronov Monograph / ed. by A. S. Minzov. – M.: VNIIgeosystems, 2019. – 110 p.

11. Minzov A. S., Cheremisina E. N., Tokareva N. A., Bobyleva S. V. Modeling of information security risks in the digital economy: monograph/ed. by A. S. Minzova. – M.: COURSE, 2021. – 112 p.

12. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures / ENISA. – Hague: European Union Agency For Network And Information Security, 2017. – 103 p. Doi: 10.2824/03228.

13. Information security of IoT devices using hardware support [Electronic resource]. – Mode of access: https://habr.com/ru/post/534300/. – Date of access: 20.06.2021.

14. Global information infrastructure, aspects of the Internet protocol and the network of subsequent generations [Electronic resource]: Overview of the Internet of Things. – ITU, 2012. – 22 p. – Mode of access: https://iotas.ru/files/documents/wg/T-REC-Y.2060-201206-I!! PDF-R.pdf/. – Date of access: 20.06.2021.

15. GOST R 57700.37-2021 Computer models and modeling. Digital product twins. General provisions. Official edition. – M.: FSBI "RST", 2021, – 15p.

16. What is a security breach [Electronic resource].– Mode of acess: https://www.kaspersky.ru/resource-center/threats/what-is-a-security-breach. – Date of access: 20.06.2021.

17. Gartner Identifies Three Factors Influencing Growth in Security Spending [Electronic resource]. – Mode of access: https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-iden tifies-three-factors-influencing-growth-i. – Date of access: 26.06.2021.