DOI:10.32703/2617-9059-2024-43-7

UDC 656.221.5:681.2.08

Iryna Voronko[1*]

[1]Candidate of Technical Sciences, Senior Lecturer, Department of Automation and Computer-Integrated Transport Technologies, State University of Infrastructure and Technology, Kyrylivska str., 9, Kyiv, Ukraine, 04071. ORCID: https://orcid.org/0000-0003-3599-6672

[*]**Corresponding author:** ir.voronko@gmail.com

The security of IoT systems in railway transport

The widespread adoption of Internet of Things (IoT) devices in the railway industry is creating new cybersecurity challenges. These devices, which collect and transmit data on train movements, infrastructure and passengers, can be vulnerable to cyberattacks, which can lead to disruption of operations, security threats or compromise of sensitive data. A wide range of potential threats have been described, such as unauthorised access, data misuse and denial of service (DoS) attacks. These threats can have serious consequences, such as train accidents, data theft, or disruption of supply chains. The article is devoted to the study of the cybersecurity aspects of IoT systems in railway transport and the identification of the necessary measures to ensure the safety and reliability of these systems. Potential threats to IoT on the railway, including vulnerabilities of network devices and insufficient protection of network traffic, are considered. Simple and effective cybersecurity measures are proposed, including authentication and authorisation of IoT devices, network connection protection, and monitoring of potential threats. Threat modeling using the Microsoft Threat Modeling Tool allowed us to identify the main security issues and propose solutions. The conclusions of the article emphasise the importance of investing additional resources in ensuring the cybersecurity of IoT systems in railway transport and recommend active cooperation with experts in this field for the successful implementation of digital transformation in the railway industry.

Keywords: *The Internet of Things (IoT), cybersecurity, cyberattacks, data protection, security of IoT systems, threats, vulnerabilities, unauthorised access, railway transport.*

Introduction. The development of the Internet of Things (IoT) has created new opportunities in the railway transport industry, but it has also brought with it cybersecurity threats. With almost every connected IoT device, we can access infrastructure and personal data. However, there are also new risks associated with IoT due to its interoperability, applications and autonomous decision-making [1-3]. This creates an opportunity for abuse and potential system vulnerabilities, which has led to the issues of data security and privacy becoming increasingly relevant (Fig. 1).

The Internet of Things is a combination of mobile networks, social networks, the Internet, and smart devices that provide users with various services and applications.

Security at various levels has a direct impact on the success of IoT systems, as it ensures secure interaction of objects, reliability, and interoperability. IoT has reached a point where it can connect different spaces, such as digital and physical space, where different sensors interact with physical objects. These sensors are used in a wide range of applications, from toys to healthcare systems and the industrial sector. This illustrates how the vulnerabilities of the digital world affect the real world. A system will only be considered successful if it is guaranteed to provide security against vulnerabilities. The success of IoT applications and infrastructure depends heavily on security guarantees and the absence of vulnerabilities.

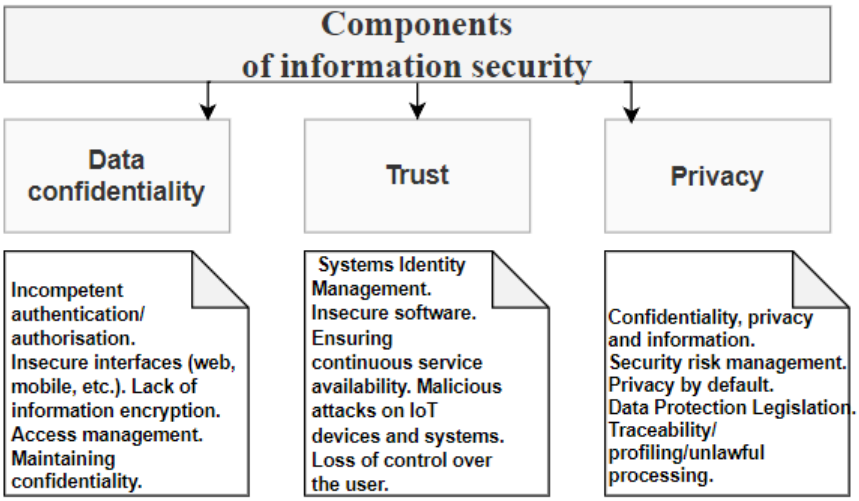

Fig. 1. **Components of information security**

A review of recent research and a statement of the problem. In recent years, there has been a great deal of research into the cybersecurity issues surrounding the IoT in the railway industry. These issues include the lack of adequate security for network devices and the lack of sufficient protection for network traffic. Researchers have identified a wide range of potential threats, including unauthorised access, data misuse and denial of service (DoS) attacks [1-3, 5]. These threats can have serious consequences, such as train accidents, data theft, or disruption of supply chains.

The purpose and objectives of the study. The objective of this study is to identify the necessary measures to ensure the safety and reliability of IoT systems in railway transport and to develop recommendations for their solution. The specific objectives of this study are as follows:

- To study the main problems of IoT cybersecurity in the railway industry;
- To analyse existing cybersecurity methods and technologies;
- To develop recommendations for ensuring the security of IoT systems in the railway industry.

In order to achieve this goal, the analysis of the latest research in this area is employed, as well as threat modeling using the Microsoft Threat Modeling Tool software.

Materials and methods of the study. The requirements for the Internet of Things security system consist of 6 main criteria [4-6]:

1. Confidentiality criterion - all data is protected;
2. Integrity criterion - data is reliable;
3. Availability criterion - data is available when and where it is needed;
4. Fail-safe criterion - reliable audit trail;
5. The criterion of authenticity - components can confirm their identity;
6. Secrecy criterion - the service does not automatically see customer data.

Data protection risks arise when IoT objects collect and aggregate data-related fragments [4, 5]. As time and frequency provide context for viewing events, personal data is transformed by matching a certain number of points. This is one aspect of the big data challenge, and security professionals must consider the potential privacy risks associated with the entire data set. Key security concerns in IoT scenarios include data privacy, secrecy, and trust.

Data privacy protection has several aspects to consider. First of all, insufficient authentication and authenticity can create problems. This implies that the system may be unable to verify the authenticity of the individual attempting to access the data. Insecure interfaces, such as the Internet or mobile phones, can also pose a risk to data privacy. Lack of transport encryption can result in data being made available for unauthorised access. Confidentiality and access control are other important aspects of data protection. Secrecy also has its aspects that need to be considered. These include data protection, risk management, and confidentiality. The concept of secrecy by default implies that data protection should

be incorporated into the system from its inception. A privacy policy represents a crucial instrument for guaranteeing privacy. The tracking, profiling and illicit processing of data can also contravene privacy.

Another crucial aspect of IoT systems is trust. This encompasses identity management systems that ensure trust between users and the system. Insecure software or firmware can undermine trust in the system. Trust is also required to ensure service continuity and availability. Malicious attacks on IoT devices and systems can erode trust. Furthermore, the loss of user verification and the difficulty in decision-making can also affect system trust.

To illustrate the security requirements of the Internet of Things, its architecture is modelled in four layers: sensor, network, service, and interface. Each layer can have corresponding security controls, including access control, authentication, data integrity and confidentiality, availability, and the ability to protect IoT tools from viruses and attacks. Table 1 provides a summary of the most important security threats in IoT [5].

Table 1. **The most prevalent Internet of Things (IoT) vulnerabilities across all levels of the architectural framework.**

Security issues	Interface layer	Service layer	Network layer	Sensor layer
Insecure web interface	+	+	+	
Insufficient authentication	+	+	+	+
Insecure network services		+	+	
Lack of transport encryption		+	+	
Privacy issues		+	+	+
Insecure cloud interface	+			
Insecure mobile interface	+		+	+
Insecure configuration	+	+	+	
Insecure software/firmware	+		+	
Poor physical security			+	+

In order for modern manufacturing facilities and smart cities to be connected to a single platform, a security architecture must be created that is optimised primarily for devices connected to the Internet of Things. The security system that is created should monitor each device connected to the network individually, warn of possible malicious access, and protect or disable devices that pose a threat when necessary [3-6]. Consequently, the development and implementation of standards represent a pivotal aspect of the Internet of Things (IoT) ecosystem.

At the vanguard of this endeavor is the standardisation of IoT protocols, which is currently spearheaded by several prominent organisations, including the IEEE (Institute of Electrical and Electronics Engineers) and ISO/IEC (International Electrotechnical Commission).

Sensors represent a crucial element of Internet of Things devices, as they facilitate the collection of a diverse range of data from the physical environment [5-8]. Such sensors are capable of measuring a multitude of parameters, including temperature, humidity, light intensity, and pressure. The data is then transmitted to the central IoT nodes for further analysis and utilisation. Given that sensors are situated within and interact with the physical world, it is of the utmost importance to guarantee their security to prevent potential attacks and infringements upon privacy.

The Internet of Things presents a multitude of security challenges for sensors, including the following [5]:

a) Sensors can be physically damaged or compromised [7, 8]. For instance, attackers may attempt to short-circuit the sensor's contacts, impose electromagnetic interference, or affect the ambient temperature.

b) Sensors often collect personal data, such as location, physiological indicators, or audio recordings. It is of paramount importance to protect this data from unauthorised access and misuse.

c) Attackers may attempt to falsify data, correlate it, or introduce errors to distort analysis and decision-making [8].

To guarantee the security of IoT devices at the sensor level, the methods illustrated in Fig. 2 must be employed.

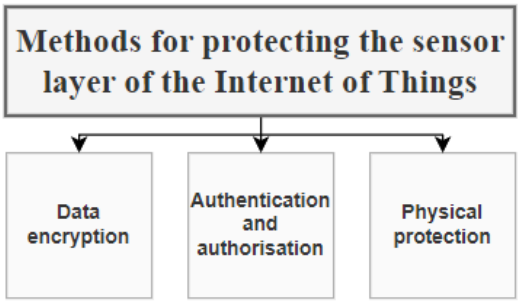

Fig. 2. **Protection methods at the sensor level of the Internet of Things**

Data encryption: the use of data encryption allows for the protection of data from unauthorised access [5, 8]. The utilisation of robust encryption algorithms will diminish the probability of sensitive data being divulged.

It is of paramount importance to implement authentication and authorisation mechanisms to verify access rights to sensors and data transmission [5]. This will prevent unauthorised access and manipulation of data.

Physical protection can be achieved through the use of protective enclosures, access control to devices, or the implementation of tampering detection mechanisms [5, 8].

It is of paramount importance to ensure the security of IoT devices at the sensor level during the development of this technology. The main challenges faced by IoT sensors include physical attacks, privacy violations, and data fraud.

In order to ensure the security of IoT devices at the network level, it is necessary to conduct a comprehensive analysis of the potential threats and vulnerabilities. One of the most prevalent threats is the interception of communications with intruders via attacks on the network stack of devices [5, 9]. Such attacks may exploit vulnerabilities in communication protocols and security services installed on IoT devices.

In order to guarantee the security of the network level of IoT devices, a number of security measures are employed. One such measure is the encryption of communication between devices. The utilisation of contemporary encryption algorithms, such as the Advanced Encryption Standard (AES), enables the safeguarding of data transmitted between IoT devices from interception and decryption by unauthorised third parties [10]. Furthermore, in order to guarantee the security of the network, it is essential to implement network security measures such as firewalls and intrusion detection systems. Firewalls permit the regulation of traffic leaving and entering the IoT network, with the capacity to block any connections that may be deemed suspicious [11]. Intrusion detection systems are designed to monitor and identify any unusual activity within the network, thereby alerting the user to potential attacks.

It has been demonstrated in practice that a significant proportion of IoT devices possess software vulnerabilities that can be exploited by attackers. It is not uncommon for device manufacturers to fail to provide regular updates, which can result in the continued presence of vulnerabilities in devices. Nevertheless, the implementation of regular software updates for IoT devices represents a pivotal aspect of network-level security. Updates permit the rectification of identified vulnerabilities and the incorporation of novel security measures. Furthermore, it is of significant importance that device manufacturers implement automatic update mechanisms, which would facilitate the process of maintaining security for users [11].

It is of paramount importance to ensure the security of IoT devices at the network level to protect the privacy of users and to prevent any unwanted attacks. A comprehensive approach to the security of IoT devices at the network level necessitates the integration of several key elements, including threat analysis, encryption, the utilisation of network security measures, and the implementation of regular software updates.

One of the most crucial aspects *of ensuring the security of IoT devices at the service level* is to achieve technical security alignment. This entails the development and implementation of common security standards and protocols that can be applied to a range of IoT devices. For instance, standards such as MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), and TLS (Transport Layer Security) facilitate secure connections, authentication, authorisation, and data confidentiality [5, 10]. Additionally, there is a prevalent security protocol known as Zigbee, which is employed to establish secure networks with embedded devices [5, 10].

Nevertheless, ensuring security at the service level of IoT devices is not solely a technical matter. It is also important to consider the physical security of devices, as this plays an important role in preventing unauthorised access and misuse. Physical security measures may include the implementation of access control mechanisms, the use of protective enclosures, and the restriction of physical access to critical components [11].

In order to guarantee the security of IoT devices at the service level, it is essential to implement a rigorous and comprehensive security lifecycle management strategy. This implies that security must be contemplated at each stage, including the conceptualisation, construction, manufacturing, implementation, and operation of devices. For instance, the application of the tenets of the Secure Software Development Lifecycle (SSDLC) enables the identification and rectification of potential vulnerabilities at the nascent stages of development [10]. Furthermore, it is essential to implement regular software updates and patches to address known security vulnerabilities and protect devices from emerging threats [5, 9].

To ensure the security of IoT devices at the service level, it is necessary to adopt a comprehensive approach that encompasses technical, physical, and managerial aspects. Technical security alignment, physical security, and security lifecycle management are essential elements in ensuring the security of IoT devices at the service level.

At the interface level of Internet of Things devices, there are a significant number of issues that require reliable security measures. Each layer of the IoT network presents its distinctive challenges, necessitating the implementation of bespoke security measures. One of the most crucial aspects is the assurance of security at the level of the IoT device. Even devices with limited resources must be protected to ensure the confidentiality, integrity, and trustworthiness of data exchanged on the network [12].

Furthermore, it is necessary to reconcile consumer privacy and business privacy in the context of the IoT. The vast quantity of data generated by IoT devices is considerable, and it is of the utmost importance to ensure that it is adequately protected and processed in order to prevent privacy breaches and potential cyberattacks [12].

Ensuring security at the interface level of IoT devices is a complex task that requires an integrated approach and the use of specialised methods and protocols. Adherence to these principles will help ensure the security, confidentiality and reliability of the IoT network.

IoT systems in the railway transport industry can be subject to cyberattacks due several vulnerabilities. One such vulnerability is the insufficient security of network devices. A significant proportion of the IoT devices deployed on railways lack inherent security features, as they were designed with a primary focus on functionality and efficiency. Insufficient security of network devices can serve as an entry point for attackers who can exploit these vulnerabilities to gain unauthorised access to the system and carry out cyberattacks. For instance, attackers may alter device settings, execute malicious code, or even deactivate the devices entirely [7, 13].

Another potential vulnerability is the insufficient protection of network traffic. A significant proportion of IoT devices on railways communicate over open networks without adequate encryption.

This implies that attackers can to intercept transmitted data and gain access to confidential information or modify data remotely [14-16].

It is evident that cyberattacks on rail transport can have serious consequences. One potential consequence is a breach of passenger safety. Attackers can utilise cyberattacks to disable train speed control systems or security systems, which could result in accidents, injuries to passengers, or even fatalities [16]. Furthermore, cyberattacks can also result in difficulties in the transportation of goods. Attackers can utilise cyberattacks in order to disrupt cargo monitoring systems or those responsible for managing cargo flows. Such incidents can result in the loss or damage of cargo, financial losses for companies, and delays in the global supply chain [14-16].

The preceding discussion highlights the necessity of robust cybersecurity measures in IoT systems employed in rail transport. Security gaps can have significant consequences for passenger safety, train efficiency, and freight reliability.

The Internet of Things in railways encompasses a multitude of interconnected devices, including sensors, controllers, and monitors, which facilitate the efficient operation of railway infrastructure [14-16]. However, it also creates new cybersecurity threats that can have serious consequences for passenger safety and the operation of railway systems. In light of the above, it is necessary to examine the structural scheme of security measures designed to safeguard IoT systems in railway transport (Fig. 3).

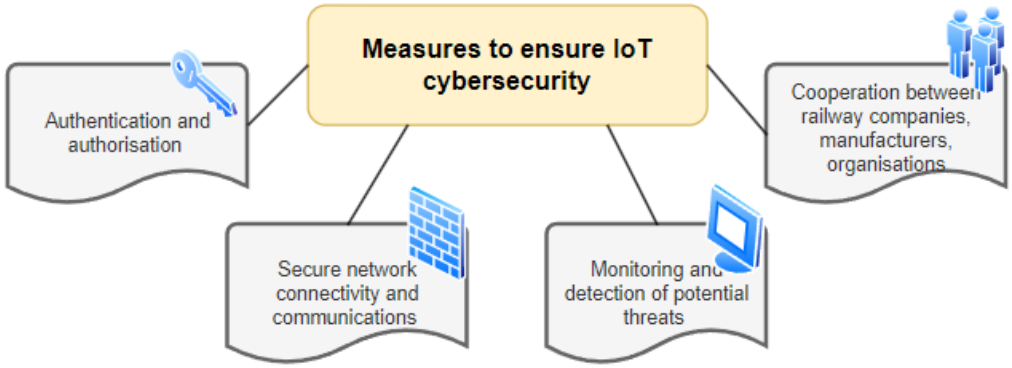

Fig. 3. **The measures that are in place to ensure the cybersecurity of the Internet of Things**

The initial step in ensuring cybersecurity in rail transport is the authentication and authorisation of IoT devices (Fig. 3). This process ensures that the connected devices in the IoT network are identified and accessed legitimately. A variety of authentication methods may be employed to achieve these objectives, including encryption, digital signatures, and authentication protocols such as OAuth or OpenID. Authorisation, in turn, defines access levels and allows for the control of user rights to interact with the IoT system in railway transport [17].

One of the most crucial elements of IoT security in railway transport is the safeguarding of network connections and communications between connected devices (Fig. 3). This is achieved through the utilisation of secure data transfer protocols, such as SSL/TLS, which provide encryption and identification of the parties exchanging information. Furthermore, it is essential to consider the implementation of protective measures against cyberattacks such as DDoS (distributed denial of service), which can result in the denial of service and the disruption of the operation of IoT systems on the railways [17].

Monitoring and detection of potential cybersecurity threats (Fig. 3) represent a pivotal aspect of security measures for IoT systems in railway transport. In order to achieve this, it is possible to utilise internet threat detection systems (intrusion detection system, IDS) and internet protection systems (intrusion prevention system, IPS) in order to detect and prevent attacks on IoT network traffic. A block diagram of the IDS and IPS systems is presented in Fig. 4.

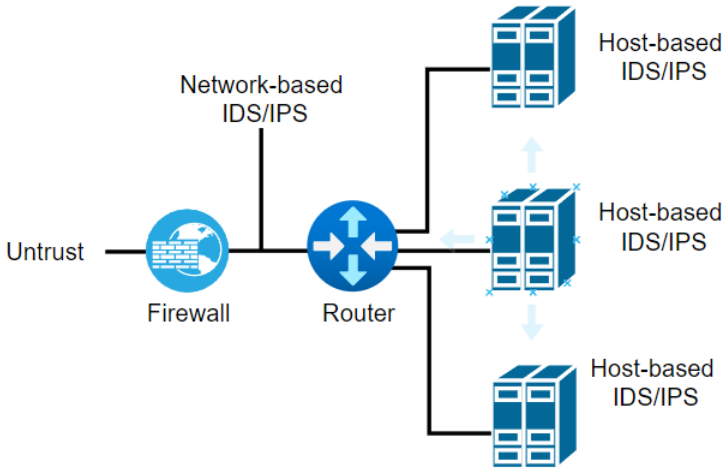

Fig. 4. **A block diagram of the IDS/IPS systems is provided below**

Furthermore, it is recommended that a centralised monitoring system be installed, which would allow for a rapid response to potential threats and the analysis of security events [52].

In order to achieve a high level of cybersecurity in the field of IoT in the railway transport sector, it is important to cooperate between railway companies, device manufacturers, and cybersecurity organisations (Fig. 3). This interaction between the parties allows them to share best practices, identify and develop solutions to potential threats, and respond to new vulnerabilities and attacks. Furthermore, joint initiatives to create security standards and certification can assist in enhancing the security of IoT systems on railways [17].

Utilising the Microsoft Threat Modeling Tool software [18], we will develop a simplified scheme of IoT use on the railway (Fig. 5). Modeling this system will assist in identifying potential threats and implementing measures to address them, even before the system is fully implemented on the railway section.

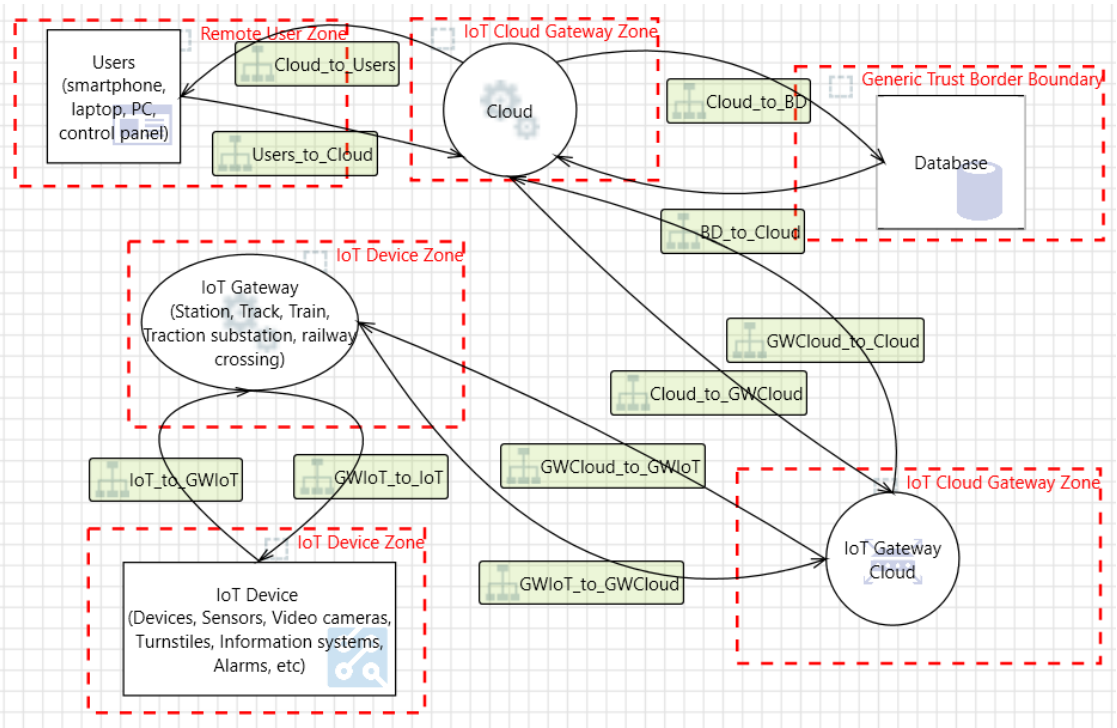

Fig. 5. **Threat Modeling Scheme**

The Microsoft Threat Modeling Tool represents a pivotal component of the Microsoft Security Development Lifecycle (SDL), which enables software developers to identify and mitigate potential security issues at an early stage of development, when they are still relatively straightforward and cost-effective to resolve. Consequently, this markedly reduces the overall cost of development.

Following the development of the model within the application environment and the execution of the simulation, a report is generated, which lists the potential threats and provides guidance on how to resolve them.

After analysing the threat modeling report, we can identify specific system vulnerabilities that need to be addressed during the implementation of IoT technologies in the railway sector (Table 2). This will help to increase the efficiency of spending money on the development and implementation of IoT in the Ukrainian railway transport system.

Table 2. **List of major system vulnerabilities**

№	Vulnerability and solutions
1	If there are no restrictions on access to the database at network or host firewall level, anyone can attempt to connect to the database from an unauthorised location. The solution to this problem is quite simple, simply configure the firewall to only allow access from authorised locations.
2	The possibility of malicious code being executed in the gateway by people outside the system. The solution is to prohibit the execution of unknown code on corporate devices.
3	Possible use of weak authorisation checks on devices and remote execution of unauthorised and confidential commands. This can be overcome by using authorisation checks on the device if it supports different actions requiring different levels of authorisation.
4	Hackers can exploit known vulnerabilities in a device if the firmware is not updated promptly. Solution: Timely software updates for IoT devices.
5	Possibility of unauthorised access to the system and access to confidential information in the gateway. Workaround: Use Bitlocker encryption.
6	An attacker can access the admin interface or privileged services such as WiFi, SSH, shared folders, FTP, etc. on the devices, so it is necessary to secure all admin interfaces with strong accounts.

The table below shows the top 6 security challenges associated with IoT adoption. The rest of the less significant issues are listed in the modeling report provided by the threat modelling software. The table shows the top 6 security challenges associated with the deployment of the Internet of Things. The rest of the less significant issues are listed in the modeling report provided by Threat Modeling.

Conclusions. The paper examines the security aspects of IoT at different levels and identifies the need to implement reliable security systems for IoT technologies in railway transport. It was found that security is one of the main factors affecting the successful implementation of digital transformation in the railway industry.

The modeling of IoT security threats carried out using the Microsoft Threat Modeling Tool software allowed the identification of the main security problems of the IoT system on the railway. The proposed easy-to-implement measures were considered as ways to solve these problems and ensure the reliability and security of the IoT system.

It was found that the introduction of the Internet of Things in rail transport will require additional efforts to ensure cybersecurity. This means that it is necessary to invest additional resources in the development and implementation of modern security systems that ensure the reliable and safe operation of IoT in rail transport.

Therefore, it is recommended to pay due attention to cybersecurity when implementing digital transformation projects. Project participants should actively cooperate with cybersecurity experts and

implement reliable security systems that guarantee protection against possible threats and misuse in the area of IoT on the railway. It should be borne in mind that the cost of developing and implementing these systems will be justified in the context of ensuring the safety and efficiency of rail transport in the context of digital transformation.

REFERENCES

1. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks / *Journal of Information Security and Applications*, *38*, 8-27. https://doi.org/10.1016/j.jisa.2017.11.002.
2. Opirskyy, I., Holovchak, R., Moisiichuk, I., Balianda T., & Haraniuk, S. (2021). Problemy ta zahrozy bezpetsi IoT prystroiv/ *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika»*, *3*(11), 31–42. https://doi.org/10.28925/2663-4023.2021.11.3142. [in Ukrainian].
3. Dongre, N., Atique, M., Shaik, Z. A., & Raut, A. D. (2022, January). A survey on security issues and secure frameworks in internet of things (iot). In *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 173-181). IEEE. https://doi.org/10.1109/ICSSIT53264.2022.9716413.
4. Jaiswal, S., & Gupta, D. (2017). Security requirements for internet of things (IoT). In *Proceedings of International Conference on Communication and Networks: ComNet 2016* (pp. 419-427). Springer Singapore.. https://doi.org/10.1007/978-981-10-2750-5_44.
5. Shancang Li, & Li Da Xu (2020). *Securing the Internet of Things*. Syngress.
6. Serajuddin, M., Hasan, Z., Khan, A., & Akhtar, A. (2023). Impact of IoT on Security and Data Protection. *Journal of Informatics Education and Research*, *3*(2). https://doi.org/10.52783/jier.v3i2.367.
7. Singh, P., Elmi, Z., Meriga, V. K., Pasha, J., & Dulebenets, M. A. (2022). Internet of Things for sustainable railway transportation: Past, present, and future. *Cleaner Logistics and Supply Chain*, *4*, 100065.. https://doi.org/10.1016/j.clscn.2022.100065.
8. Stellios, I., Kotzanikolaou, P., Psarakis, M., & Alcaraz, C. (2021). Risk assessment for IoT-enabled cyber-physical systems. *Advances in Core Computer Science-Based Technologies: Papers in Honor of Professor Nikolaos Alexandris*, 157-173. https://doi.org/10.1007/978-3-030-41196-1_8
9. Miloslavskaya, N., & Tolstoy, A. (2019). Internet of Things: information security challenges and solutions. *Cluster Computing*, *22*, 103-119. https://doi.org/10.1007/s10586-018-2823-6.
10. Shandilya, S.K., Chun, S.A., & Shandilya, S. (Eds.) (2018) Internet of Things Security: Fundamentals, Techniques, and Applications (1st ed.). *River Publishers*, 162. https://doi.org/10.1201/9781003338642.
11. Anderson, R. (2020). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.
12. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013) Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions / *Future Generation Computer Systems*, 29, 1645-1660. http://dx.doi.org/10.1016/j.future.2013.01.010.
13. Kour, R. (2020). *Cybersecurity in railway: a framework for improvement of digital asset security* (Doctoral dissertation, Luleå University of Technology). URL: https://urn.kb.se/resolve?urn=urn:nbn:se:ltu:diva-78488.
14. Voronko I.O. (2020) Osoblyvosti nadiinosti ta informatsiinoi bezpeky system monitorynhu ta diahnostyky. *Informatsiino-keruiuchi systemy na zaliznychnomu transporti: naukovo-tekhnichnyi zhurnal*. *Kharkiv: UkrDUZT*, *3*, 49-50. [in Ukrainian].
15. Voronko I.O.(2021) Dyferentsialno-ihrova model zakhystu informatsii dlia kompiuternykh system transportnoi infrastruktury. *«Transportni systemy i tekhnolohii», 38,* 201-213. https://doi.org/10.32703/2617-9040-2021-38-198-19 [in Ukrainian].
16. Yash Madwanna. (2018) IoT based Railway system using ICN: Chapter 1 Problem Definition. *College of Engineering and Technology*. URL: https://www.academia.edu/35158284/IOT_based_Railway_system_using_ICN_CHAPTER_1_Problem_Definition
17. Gupta, B. B., & Quamara, M. (2020). *Internet of Things Security: Principles, Applications, Attacks, and Countermeasures*. CRC Press. https://doi.org/10.1201/9780429353529.
18. Microsoft Threat Modeling Tool (2022). URL: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool.

***Воронко Ірина Олександрівна*[1]**

[1]Кандидат технічних наук, старший викладач кафедра «Автоматизація та комп'ютерно-інтегровані технології транспорту», Державний університет інфраструктури та технологій, вул. Кирилівська, 9, м.Київ, Україна, 04071. ORCID: https://orcid.org/0000-0003-3599-6672

Безпека систем інтернету речей на залізничному транспорті

Широке впровадження пристроїв Інтернету речей (IoT) в залізничній галузі створює нові виклики кібербезпеки. Ці пристрої, які збирають та передають дані про рух поїздів, інфраструктуру та пасажирів, можуть бути вразливими до кібератак, що може призвести до порушення роботи, створення загроз безпеці або компрометації конфіденційних даних. Описано широкий спектр потенційних загроз, таких як несанкціонований доступ, зловмисне використання даних та атаки типу "відмова в обслуговуванні" (DoS). Дані загрози можуть мати серйозні наслідки, такі як аварії поїздів, крадіжка даних або порушення логістичних ланцюгів. Стаття присвячена дослідженню аспектів кібербезпеки систем IoT на залізничному транспорті та визначенню необхідних заходів для забезпечення безпеки та надійності цих систем. Розглянуто потенційні загрози для IoT на залізниці, включаючи вразливості мережевих пристроїв та недостатній захист мережевого трафіку. Запропоновано прості та ефективні заходи забезпечення кібербезпеки, такі як автентифікація та авторизація пристроїв IoT, захист мережевого з'єднання та моніторинг потенційних загроз. Моделювання загроз за допомогою Microsoft Threat Modeling Tool дозволило ідентифікувати основні безпекові проблеми та запропонувати шляхи їх вирішення. Висновки статті підкреслюють важливість вкладення додаткових ресурсів у забезпечення кібербезпеки систем IoT на залізничному транспорті та рекомендують активну співпрацю з експертами з цієї галузі для успішної реалізації цифрової трансформації у залізничній індустрії.

Ключові слова: *Інтернет речей (IoT), кібербезпека, кібератаки, захист даних, безпека IoT-систем, загрози, вразливості, несанкціонований доступ, залізничний транспорт.*