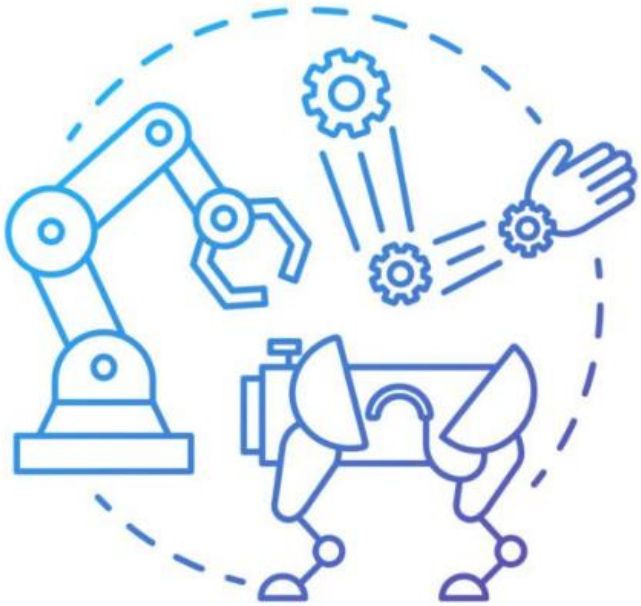
Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
кафедра комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
(КІТАР)



МАТЕРІАЛИ

ІІ Всеукраїнської конференції
«Комп’ютерно-інтегрованих технологій, автоматизації та робототехніки»
(Computer-integrated technologies, automation and robotics)
CITAR`25
16-17 травня 2025

[електронне видання]

Харків 2025

УДК: 005:004.896:62-65:338.3

Комп’ютерно-інтегрованих технологій, автоматизації та робототехніки 2025: матеріали II-ої Всеукраїнської конференції, Харків, 16-17 травня 2025.: тези доповідей / [редкол. І.Ш. Невлюдов (відповідальний редактор)].-Харків: [електронний друк], 2025. – 132 с.

У збірник включені тези доповідей, які присвячені сучасним автоматизованим технологіям Industry 4.0 та їх впровадження; інформаційні управляючі системи технологічного призначення; математичні методи в системах автоматизації; розробка та програмування в робототехніці; штучний інтелект та машинне навчання в автоматизації; інтеграція технологій у виробництві та промисловості; сенсорні технології та взаємодія людини з роботами в Industry 5.0; ефективність використання роботизованих систем у виробництві; етика та правові аспекти в робототехніці; Інтернет речей та Інтегровані системи в комп’ютерно-інтегрованих технологіях, автоматизації та робототехніки; технологічні виклики та інновації у світі робототехніки.

Редакційна колегія: І.Ш. Невлюдов, В.В. Євсєєв.

Computer-integrated technologies, automation and robotics 2025: Proceedings of II st All-Ukrainian Conference, Kharkiv, May 16-17, 2025: Thesises of Reports / [Ed. I.Sh. Nevlyudov (chief editor).] .- Kharkiv .: [electronic version], 2025. - 132 p.

The collection includes abstracts devoted to modern automated technologies of Industry 4.0 and their implementation; information control systems for technological purposes; mathematical methods in automation systems; development and programming in robotics; artificial intelligence and machine learning in automation; integration of technologies in production and industry; sensor technologies and human interaction with robots in Industry 5.0; efficiency of using robotic systems in production; ethics and legal aspects in robotics; Internet of Things.

Editorial board: Igor.Sh. Nevludov, Vladyslav.V. Yevsieiev

ЗМІСТ

O.O. Chala , D.O. Kryvenko
Challenges and trends of automation of logistics processes in bond warehouses using INDUSTRY 5.0 concepts ……. 6
М. Ю. Лазаренко, В. В. Євсєєв, О.М. Цимбал
Ефективність використання роботизованих систем у виробництві ……... 9
Vladyslav Yevsieiev
Using multi-agent systems in the management of collaborative robots …… 13
Svitlana Starykova
Using free web applications for designing mobile robots in general secondary education institutions (GSEI) …… 18
Тищенко Ю.О. , С.В. Хрустальова
Аналіз баз даних систем автоматизації ……. 23
M. S. Achkan, S. V. Sotnik
Integration of cloud technologies into modern SCADA systems: prospects and challenges … 26
Берест Б.Р. Гурін Д.В.
Актуальність віртуалізації гнучких виробничих дільниць на виробництві …….. 30
Бєлий Я.В, Сичова О.В.
Розпізнавання голосу за допомогою офлайн-бібліотеки VOSK в робототехніці ……. 34
Ігор Голод
Кіберфізичні системи в управлінні мікрокліматом: аналіз сучасних підходів ……. 38
Гурін Д.В.
Індустрія 5.0 та колаборативні роботи: перспективи та виклики ……... 43
*Дихтенко А.І. Гурін Д.В***.**
Аналіз сучасних систем моніторінгу та аналізу даних на виробництві ……. 47
М.Ю. Білоусов, М.Г. Стародубцев, С.В. Шибанов
Метод покращення стратегії керування технологічними процесами …… 50
С.О. Єрофєєв Д.В. Гурін
Автоматичні диспенсери для ліків: сучасний стан та перспективи розвитку …….. 57
В.Я. Коваленко
Інтелектуальні SCADA–системи ……... 60
O. R. Kolbasa, S. V. Sotnik
The significance and necessity of automating the selection of sensors and actuators …….. 63
A. Konieva, S. Sotnik
Main trends in the development of automated image processing systems …… 68
Д.В. Лукієнко, Д.В Гурін
Аналіз технологій для вебсайту-помічника абітурієнта: чому Next.JS та Google таблиці – оптимальне рішення …….. 73
Г.С. Макаренко, М.Г. Стародубцев, С.В. Шибанов
Вибір керуючих впливів на основі оперативної ідентифікації технологічного об'єкту ... 76
R.V. Marunich, S. V. Sotnik
Features of IOT application in the security sector ……. 80
K. A. Polikanov, S.V. Sotnik
Overview of modern technologies for residential automation …… 85

О.Ю. Посашков, О.М. Цимбал
Аналіз систем динамічного планування виробництва в умовах невизначеності…….. 90
Д.Є. Проценко
Порівняння методів взаємодії з асистентами …….. 93
Пустовойтенко Ф.А.
Аналіз існуючих рішень серед систем планування ресурсів підприємства та їх проблематики …….. 97
M. Rudenko, S. Sotnik
Overview of algorithmic approaches to forecasting in CRM systems ……. 101
О. О. Сириця Д.В Гурін
Сферичний робот для гуманітарного розмінування: доступне рішення для безпечного майбутнього ……. 106
О.В. Суботін, Я.І. Петрухін
Проєктування модулю отримання первинної інформації для систем контролю технологічних параметрів …….. 110
A. D. Yechevskyi, S. V. Sotnik
Research of orientation methods of autonomous mobile robots in industrial conditions ……. 115
Юрченко О.Д.
Роль SCADA-системи з використанням концепції IOT ……. 120
Д.А. Янушкевич, Л.С. Іванов, К.С. Редькін
Сучасні технології систем управління якістю Quality 5.0 та їх впровадження на підприємствах ……. 125
Б. Місан, І. Невлюдов, О. Рубан
Перспективи 3D друку усних фільмів …….. 129

FEATURES OF IoT APPLICATION IN THE SECURITY SECTOR

R.V. Marunich, S. V. Sotnik
Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Nauky av., 14
E-mail: rostyslav.marunich@nure.ua, svetlana.sotnik@nure.ua

Abstract: The theses are devoted to the peculiarities of the Internet of Things (IoT) application in the security sector. The main advantages of using IoT technologies, such as automating access control processes, improving monitoring, rapid response to threats, and integration with other security systems, are considered. The key areas of IoT application are described, including automated access control, smart video surveillance, use of sensors for threat detection, data protection, and integration with emergency response systems. Challenges related to cybersecurity, privacy protection, and reliability of IoT devices are also highlighted. The future of IoT in the security sector is associated with the introduction of artificial intelligence, quantum cryptography, and integration with 5G networks. IoT is presented as a key tool for improving the efficiency, security and automation of modern security systems.

Keywords: IoT, security, automated access control, smart video surveillance, cybersecurity, sensors, artificial intelligence.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ IoT У СФЕРІ БЕЗПЕКИ

Р. В. Маруніч, С. В. Сотник
Харківський національний університет радіоелектроніки
Україна, 61166, Харків, пр. Науки 14
E-mail: rostyslav.marunich@nure.ua, svetlana.sotnik@nure.ua

***Анотація*: Робота** присвячена особливостям застосування Інтернету речей (IoT) у сфері безпеки. Розглядаються основні переваги використання IoT-технологій, такі як автоматизація процесів контролю доступу, покращення моніторингу, швидке реагування на загрози та інтеграція з іншими системами безпеки. Описано ключові напрями застосування IoT, включаючи автоматизований контроль доступу, розумне відеоспостереження, використання сенсорів для виявлення загроз, захист даних та інтеграцію з системами екстреного реагування. Також висвітлено виклики, пов'язані з кібербезпекою, захистом приватності та надійністю IoT-пристроїв. Майбутнє IoT у сфері безпеки пов'язане з впровадженням штучного інтелекту, квантової криптографії та інтеграцією з мережами 5G. IoT представлено як ключовий інструмент для підвищення ефективності, безпеки та автоматизації сучасних систем захисту.

***Ключові слова*: IoT**, безпека, автоматизований контроль доступу, розумне відеоспостереження, кібербезпека, сенсори, штучний інтелект.

RELEVANCE OF THE WORK. The Internet of Things (IoT) and automation are among the most important technological trends of our time, which actively influence various spheres of life and business [1-8]. Their relevance is driven by reducing production costs, optimizing resource use, and increasing productivity. IoT enables remote monitoring and control of devices, which reduces maintenance and energy costs. In addition, these technologies significantly improve the quality of life, making it more convenient, safer, and more comfortable thanks to smart devices such as smart home or wearables. IoT is one of the most important technologies of our time, which has a significant impact on various areas of life, including security. IoT allows you to connect various devices to the network, which makes it possible to automate processes, collect real-time data, and respond quickly

to threats [9, 10]. In the security sector, IoT plays a key role in providing physical and cyber security, improving monitoring and automating response systems.

The relevance of researching the issue of the specifics of IoT application in the security sector is that the growing number of connected devices and their integration into critical systems require an in-depth analysis of risks, protection methods and strategies for the effective use of these technologies. In particular, it is important to investigate how IoT can improve security, as well as the challenges posed by cyber threats and network vulnerabilities. This makes the study particularly relevant in the context of modern requirements for data protection, confidentiality, and system stability.

MATERIALS AND RESEARCH RESULTS. In today's world, where threats in both the physical and cyber environments are becoming increasingly complex and diverse, IoT opens up new opportunities for improving security. Thanks to its ability to integrate various devices, collect real-time data, and automate processes, IoT is becoming a powerful tool for preventing and responding to threats. Let's take a look at the main security benefits of IoT that make this technology indispensable for ensuring protection at various levels.

So, let's identify the main advantages of IoT in the security sector:

1. Automation of access control processes Because one of the main advantages of IoT is the ability to automate access control to facilities. Thanks to smart locks, face recognition systems, and biometric sensors, you can ensure reliable user identification. For example, enterprises use RFID cards that are synchronized with centralized control systems. This allows you to restrict access to certain areas only to authorized persons, which significantly increases the level of security.

2. Improved monitoring, as IoT allows for the implementation of smart video surveillance systems that not only record events but also analyze them using artificial intelligence. Such systems are able to recognize dangerous situations, such as a suspicious object left behind or a crowd in a restricted area. This allows them to respond quickly to potential threats and prevent their development.

3. Rapid response to threats IoT devices such as motion, gas, or temperature sensors can quickly detect dangerous situations, such as a fire, gas leak, or unauthorized access. These devices can automatically send signals to emergency response systems, minimizing response times and preventing serious consequences.

4. Integration with other security systems as IoT allows you to integrate various security systems, such as video surveillance, access control, fire alarms, and emergency response systems, into a single network. This provides an integrated approach to security and allows you to effectively manage all processes from a single control center.

Let's look at the key areas of IoT application in the security sector to understand how this technology is transforming security approaches at different levels:

1. Automated access control because IoT allows you to create intelligent access control systems that use biometric data, RFID cards, or QR codes to identify users. Such systems provide a high level of security and allow you to restrict access to certain areas only to authorized persons.

2. Smart video surveillance because IoT-connected cameras can not only record events but also analyze them using artificial intelligence. For example, they can recognize faces, detect suspicious objects, or analyze human behavior. This allows you to respond quickly to potential threats.

3. Use sensors to detect threats because IoT sensors [11], such as motion, temperature, gas, or smoke sensors, can quickly detect dangerous situations. For example, in the event of a fire, the sensors can automatically activate the fire alarm system and send a signal to the emergency services.

4. Data protection and cybersecurity Since IoT devices are connected to the network, they are often targeted by cybercriminals [12]. To protect data, encryption methods, multi-factor authentication, and analysis of abnormal network traffic behavior are used. This ensures a high level of cybersecurity.

5. Integration with emergency response systems Because IoT allows security systems to integrate with emergency response services. For example, in the event of a fire or burglary, the system can automatically send a signal to the police, fire department, or paramedics, allowing for a quick response to incidents.

Despite the significant advantages and broad capabilities of IoT in the security sector, this technology also faces a number of challenges that may affect its effectiveness and reliability, which we will discuss below.

One of the most serious challenges related to the use of IoT in the security sector is cybersecurity. Since IoT devices are constantly connected to the network, they become potential targets for cyberattacks. Hackers can exploit vulnerabilities in device software to gain unauthorized access to security systems, which can lead to serious consequences, such as leakage of confidential data or even physical hacking of facilities. To protect IoT devices, it is necessary to implement modern data encryption methods, regularly update software to eliminate vulnerabilities, and continuously monitor network traffic to detect suspicious activity. In addition, it is important to provide multi-factor authentication to increase the level of protection.

Another important challenge is privacy protection. IoT devices collect a huge amount of data, including video, audio, location, and other sensitive information. This data can be used to violate users' privacy if it falls into the hands of intruders. To prevent such situations, it is necessary to implement strict data protection mechanisms, including encryption of information at all stages of its transmission and storage. It is also important to ensure transparency in the collection and use of data so that users can control what information is collected and how it is used.

Reliability of IoT devices is another key aspect that requires attention. For security reasons, devices need to operate smoothly, especially in critical situations such as fire, hacking, or other emergencies. Any failure of the devices can lead to serious consequences, including loss of property or even life. Therefore, it is necessary to ensure high quality equipment, regular maintenance, and the availability of backup power in case of a power outage. In addition, it is important to develop systems that can quickly recover from failures.

Hardware compatibility is another challenge faced by developers and users of IoT systems. Since IoT devices are manufactured by different companies, they often have different standards and communication protocols, making it difficult to integrate them into a single system. For IoT systems to function efficiently, it is necessary to ensure high compatibility between different components. This can be achieved by developing unified standards and protocols that allow devices from different manufacturers to work together seamlessly.

The future of IoT in the security sector is associated with innovative technologies that will further improve the efficiency and reliability of security systems. One of the key areas of development is the introduction of artificial intelligence (AI). AI will allow analyzing huge amounts of data collected by IoT devices and detecting anomalies in real time. For example, AI can recognize suspicious human behavior, predict potential threats, and automatically make decisions to eliminate them. This will significantly increase security and prevent incidents before they occur.

Another promising area is quantum cryptography. In the future, quantum technologies may become the main tool for data protection in IoT systems. Quantum cryptography provides a high level of protection because it is based on the principles of quantum mechanics, which makes it virtually indestructible to modern hacking methods. This is especially important for protecting critical data, such as information on access to strategic facilities or personal data of users.

Integration with 5G networks is another step in the development of IoT in the security sector. 5G networks provide faster data exchange, low latency, and high bandwidth, allowing IoT devices to operate more efficiently. This is especially important for systems that require instant response, such

as emergency alert systems or automated access control. Thanks to 5G, IoT devices will be able to exchange data in real time, which will significantly increase their efficiency.

Last but not least, digital twins are an important area. Digital twins are virtual copies of physical objects that allow you to model various scenarios and analyze their impact on the security system. For example, with the help of digital twins, you can simulate various emergencies, such as a fire or a break-in, and study how the security system responds to them. This allows you to improve security systems and prepare for different scenarios.

CONCLUSIONS. The study analyzed the current capabilities of IoT technology in ensuring security. The main work was aimed at studying the potential of the Internet of Things as an innovative tool for protecting various objects and information systems. The study found that IoT has significant security benefits. In particular, the technology allows automating access control, significantly improving monitoring systems, providing an extremely fast response to potential threats, and integrating various security systems into a single complex. The key areas of IoT application were identified, including intelligent access control, smart video surveillance, the use of sensors to detect threats, cybersecurity and data protection, and integration with emergency response systems.

REFERENCES:

1. Marunich, R., & et al. (2024). Approaches to ensuring the effective implementation of iot technologies in various industries. International Conference «DIGITAL INNOVATION & SUSTAINABLE DEVELOPMENT 2024». – pp. 22-23

2. Yechevskyi A., & et al. (2024). Methods Of Identification Of Objects On Industrial Lines. International Journal of Academic Engineering Research (IJAER). – Vol. 8, Issue 11. – pp. 48-55

3. Polikanov, K., & et al. (2024). Smart home with house module: overview of automation technologies. International Conference «DIGITAL INNOVATION & SUSTAINABLE DEVELOPMENT 2024». – pp. 20-21

4. Hubar, A.Y., Sotnik, S.V. Impact of automation and CALS technologies on human factor in production. The 5th International scientific and practical conference "Perspectives of contemporary science: theory and practice" (June 24-26, 2024) SPC "Sci?conf.com.ua", Lviv, Ukraine, 2024. – c. 243-249

5. Sotnik, S. V. (2024). Development of automated control system and registration of metal in continuous casting. Radio Electronics, Computer Science, Control. – pp. 197-211

6. Sotnik, S. V. (2024). Features of using REST architecture for development of ARS for information systems. Міжнародна науково-практична конференція «Інформаційні системи в управлінні проєктами та програмами», Коблево, 9–13 вересня 2024 р. Збірник праць. – Харків: ХНУРЕ. – pp. 42 – 45

7. Danylenko, M. M., & et al. (2025). Comparative analysis of modern SCADA packages for production automation. International Journal of Academic Engineering Research (IJAER). – Vol. 9. – 2. – pp. 26-34

8. Khalimonov, Y. I., & et al. (2024). Integration of IoT into security systems: opportunities and risks. Комп'ютерно-інтегровані технології автоматизації технологічних процесів на транспорті та у виробництві: матеріали всеукр. наук.-практ. конф. здобувачів вищ. освіти і молодих учених, 20 листоп. 2024 р. – pp. 117-121

9. Lykho, T. A. & et al. (2024). Pattern recognition and computer vision technologies in decision support systems of robotic systems. Proceedings of the XVII International scientific and practical conference «Information technologies and automation – 2024». – pp. 645-648

10. Халімонов, Я. І., та інш. (2024). Створення інтелектуального модулю для автоматизованого моніторингу середовища у приватних та комерційних приміщеннях з використанням комп'ютерно-інтегрованих технологій. International Conference on Advanced

Trends in Radioelectronics and Telecommunications dedicated to the 85th anniversary of the Department of Theoretical Radio Engineering and Radio Measurements. – 1. – pp. 176 -181

11. Khalimonov, Y., & et al. (2024). Approaches to ensuring proper working conditions using sensor technologies IoT. International Conference «DIGITAL INNOVATION & SUSTAINABLE DEVELOPMENT 2024», 2024 – pp. 24-25

12. Sotnik, S. (2024). Integration of IoT into security systems: opportunities and risks. International Journal of Academic Engineering Research (IJAER), 2024. – Vol. 8, Issue 11. – pp. 56-61