Міністерство освіти і науки України

NURE

Харківський національний університет радіоелектроніки

ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»

«Automation and Development of Electronic Devices»

ADED-2024

(Випуск 2)

[електронне видання]

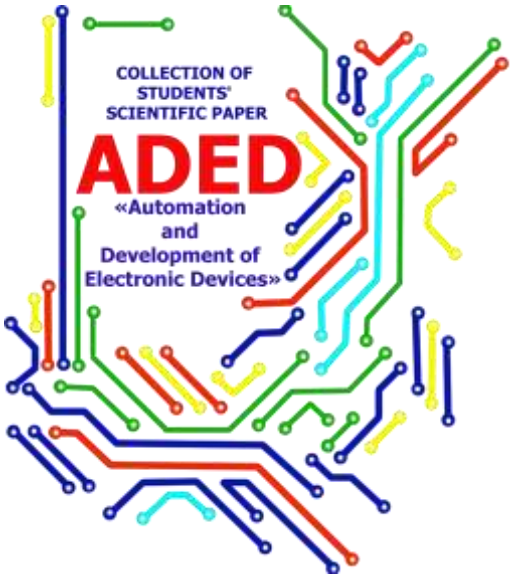
http://nure.ua/department/kafedra-komp-yuterno-integrovanih-tehnologiy-avtomatizatsiyi-ta-mehatroniki-kitam

http://itez.zntu.edu.ua/

http://kafea.kdu.edu.ua

Харків 2024

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



ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»

«Automation and Development of Electronic Devices»

ADED-2024

(Випуск 2)

[електронне видання]

Харків 2024

Автоматизація та Приладобудування («Automation and Development of Electronic Devices» ADED-2024) [Електронний ресурс] : збірник студентських наукових статей / Харківський національний університет радіоелектроніки ; [редкол.: І.Ш. Невлюдов та ін.]. – Харків : ХНУРЕ, 2024. – Вип. 2. – 290с.

Collection of Students' Scientific Paper «Automation and Development Of Electronic Devices» ADED-2024 Part 2 (Key infrastructure 2024) - Kharkiv/ The Editorial.: Nevlyudov I.Sh. (head), that all. Kharkiv: Kind of Kharkiv National Universitety of Radio Elektronics [electronic edition], 2024. – 290p with.

Рекомендовано рішенням
Науково-технічної ради
Харківського національного
університету радіоелектроніки
протокол №6 від 29.11.2018

Рекомендовано рішенням Вченої ради
факультету Автоматики і комп'ютеризованих технологій
Харківського національного
університету радіоелектроніки
протокол № 4 від 26.12.2024

Збірник містить наукові статті здобувачів першого (бакалаврського), другого (магістерського) рівнів вищої освіти кафедри комп'ютерно-інтегрованих технологій, автоматизації та робототехніки (КІТАР) Харківського національного університету радіоелектроніки, кафедри Інформаційних технологій електронних засобів (ІТЕД) Запорізького національного технічного університету та кафедри Електронних апаратів (ЕА) Кременчуцького національного університету ім. М. Остроградського які навчаються за спеціальностями: 151 Автоматизація та комп'ютерно-інтегровані технології, 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка; 172 Телекомунікації та радіотехніка, 171 Електроніка та 163 Біомедична інженерія. Статті надані в авторській редакції.

ЗМІСТ

УДК 621.121

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ IoT У СФЕРІ БЕЗПЕКИ

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

***Анотація*.** У статті досліджується застосування IoT технологій у сфері безпеки. Розглядаються основні переваги та виклики використання IoT для підвищення безпеки у різних галузях, включаючи житлові комплекси, комерційні приміщення та міське середовище. Обговорюються методи впровадження IoT для моніторингу, попередження інцидентів та забезпечення реагування на надзвичайні ситуації.

***Ключові слова*:** Інтернет речі, безпека, моніторинг, автоматизація, виявлення загроз.

FEATURES OF IoT PROTECTION IN THE SECURITY SECTOR

Marunich R.V.
Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Prospect Nauki 14
Email: rostyslav.marunich@nure.ua

Annotation. The main advantages and challenges of using IoT to improve security in various industries, including residential complexes, commercial premises, and urban environments, are considered. IoT implementation methods for monitoring, incident prevention, and emergency response are discussed.

Keywords: Internet of Things, security, monitoring, automation, threat detection.

Автоматизація, роботизація та Інтернет речі (IoT) стають дедалі актуальнішими через стрімкий розвиток технологій та зростаючі потреби суспільства у підвищенні ефективності, зниженні витрат і забезпеченні безпеки [1-6]. Вони дозволяють оптимізувати виробничі процеси, створювати інноваційні продукти та послуги, покращувати якість життя і розвивати смарт-інфраструктуру. IoT забезпечує взаємодію пристроїв, збір та аналіз даних у реальному часі, що сприяє ухваленню точних рішень та прогнозуванню. Роботизація, своєю чергою, дозволяє замінити людей у небезпечних чи рутинних процесах, підвищуючи продуктивність [11-15]. Усі ці технології є ключовими елементами цифрової трансформації, яка стає основою сучасної економіки та суспільства [16-22].

В останні роки спостерігається стрімке зростання кількості та складності кіберзагроз, що становить серйозний виклик для безпеки організацій та критичної інфраструктури. За даними провідних аналітичних агентств, щорічно фіксується збільшення кількості кібератак на 15-20%, при цьому змінюються їх характер та направленість. Особливу небезпеку становлять цільові атаки на промислові об'єкти, фінансові установи та об'єкти критичної інфраструктури.

Сучасні кіберзагрози характеризуються високим рівнем автоматизації та використанням передових технологій штучного інтелекту. Зловмисники активно застосовують методи соціальної інженерії, програми-вимагачі та розподілені атаки на відмову в обслуговуванні (DDoS). Особливо небезпечними є атаки з використанням технологій машинного навчання, які здатні адаптуватися до засобів захисту та знаходити вразливості в системах безпеки.

У зв'язку з масовим переходом на віддалену роботу та розширенням використання хмарних технологій, з'явились нові вектори атак, пов'язані з вразливістю домашніх мереж та особистих пристроїв співробітників. Це створює додаткові ризики для корпоративних мереж та даних.

Статистика показує, що понад 60% успішних кібератак відбуваються через компрометацію кінцевих пристроїв користувачів.

Традиційні методи захисту вже не здатні забезпечити належний рівень безпеки в умовах сучасних кіберзагроз [23]. Це зумовлює необхідність впровадження інноваційних рішень, зокрема систем IoT, які забезпечують комплексний моніторинг, швидке виявлення та реагування на потенційні загрози. Використання технологій Інтернету речей дозволяє створити багаторівневу систему захисту, здатну протистояти сучасним викликам у сфері кібербезпеки.

Метою даної роботи є аналіз сучасних можливостей використання технологій Інтернет речей для підвищення ефективності систем безпеки, визначення основних переваг та потенційних викликів при їх впровадженні.

Питанням впровадження IoT у системах безпеки присвячені роботи багатьох вітчизняних та закордонних науковців [24-26]. Проте, враховуючи стрімкий розвиток технологій та появу нових загроз, дана тема потребує подальшого дослідження та систематизації накопиченого досвіду.

Інтернет речей (IoT) швидко розвивається та знаходить застосування у багатьох сферах, зокрема й у безпеці (рис. 1). Завдяки сенсорам, камерам та іншим пристроям IoT забезпечує цілодобовий моніторинг і збір даних, що дозволяє запобігати небезпечним ситуаціям та швидко реагувати на надзвичайні події. У цій статті розглянемо основні переваги та виклики використання IoT у сфері безпеки.

Рисунок 1 – Приклад структури IoT для системи безпеки

На рис. 1 зображено типовий приклад структури IoT, який може використовуватись для захисту приміщень. Система включає датчики руху, камери та сервер, який збирає і аналізує дані для виявлення потенційних загроз.

Визначимо виклики та переваги впровадження IoT.

IoT технології мають ряд переваг, серед яких зручність автоматизованого моніторингу та підвищена швидкість реагування.

Проте існують також виклики, такі як забезпечення захисту особистих даних та підвищені вимоги до інфраструктури. Ключові аспекти включають:

- масштабованість систем IoT;
- захист від кібератак та конфіденційність;
- надійність мережі та живлення пристроїв.

Приклад системи реагування на надзвичайні ситуації узагальнено наведені графічно на рис. 2.

Рис. 2 показує концепцію системи, яка автоматично реагує на надзвичайні ситуації, використовуючи IoT пристрої. Це може включати сповіщення рятувальних служб та автоматичне увімкнення захисних систем.

Рисунок 2 – Приклад системи реагування на надзвичайні ситуації

IoT пропонує нові можливості для підвищення безпеки за рахунок автоматизації та обробки даних у реальному часі. Хоча існують значні виклики, які потребують вирішення, впровадження IoT у сферу безпеки є перспективним напрямом, що може підвищити рівень захисту у багатьох галузях.

Сучасні системи безпеки на базі технологій IoT знаходять широке застосування у різних сферах завдяки своїй гнучкості та ефективності. Розглянемо основні напрямки практичного використання таких систем:

1. Розумні системи відеоспостереження з AI-аналітикою. Сучасні IoT-камери в поєднанні зі штучним інтелектом забезпечують:

- розпізнавання облич та ідентифікацію осіб;
- виявлення підозрілої поведінки;
- відстеження переміщення об'єктів;
- підрахунок відвідувачів;
- виявлення залишених предметів;
- автоматичне сповіщення про інциденти.

Особливістю таких систем є можливість обробки відеопотоку в режимі реального часу та автоматичне реагування на визначені події.

2. Біометричні системи контролю доступу. IoT-пристрої в системах контролю доступу забезпечують:

- багатофакторну автентифікацію;
- зчитування біометричних даних (відбитки пальців, сканування обличчя, райдужної оболонки);
- інтеграцію з системами управління персоналом;
- облік робочого часу;
- контроль переміщення в захищених зонах;
- аудит доступу до критичних об'єктів.

3. Системи виявлення вторгнень. Комплексні IoT-рішення для виявлення вторгнень включають:

- датчики руху з підтримкою машинного навчання;
- акустичні сенсори для виявлення підозрілих звуків;
- вібраційні датчики для моніторингу огорож та стін;
- інфрачервоні бар'єри;
- лазерні системи охорони периметру.

4. Сучасні системи охорони периметру на базі IoT включають:
- Інтелектуальні огорожі з датчиками;
- дрони для автоматичного патрулювання;
- сейсмічні сенсори;
- системи раннього попередження;
- GPS-трекери для мобільних об'єктів;
- автоматичні системи блокування.

Тепер розглянемопитання особливостей впровадження IoT-систем безпеки.

При практичному впровадженні IoT-систем безпеки необхідно враховувати:
- масштабованість рішення;
- сумісність з існуючою інфраструктурою;
- надійність каналів зв'язку;
- автономність роботи;
- можливість резервування;
- захист від кібератак.

За даними досліджень, впровадження IoT-систем безпеки дозволяє [24-28]:
- знизити кількість інцидентів на 40-60 %;
- скоротити час реагування на події в 2-3 рази;
- зменшити операційні витрати на 25-30 %;
- підвищити ефективність роботи персоналу на 35-45 %.

Таким чином, практичне застосування IoT в системах безпеки демонструє високу ефективність та широкі можливості для підвищення рівня захисту об'єктів різного призначення. При цьому важливо забезпечити комплексний підхід до проектування та впровадження таких систем з урахуванням специфіки конкретного об'єкта та потенційних загроз.

У даній роботі було проведено комплексне дослідження особливостей використання технологій Інтернет речей у сфері безпеки. В результаті дослідження було визначено ключові аспекти впровадження IoT-систем та їх роль у підвищенні рівня захисту об'єктів різного призначення.

Було проаналізовано сучасний стан кіберзагроз та викликів у сфері безпеки, що підтверджує актуальність впровадження інноваційних рішень на базі IoT.

Встановлено, що традиційні методи захисту вже не забезпечують належного рівня безпеки в умовах зростаючої складності та частоти кібератак, що робить використання IoT-технологій необхідним елементом сучасних систем безпеки.

Розглянуто практичні застосування IoT в системах безпеки, включаючи розумні системи відеоспостереження з AI-аналітикою, біометричні системи контролю доступу та комплексні системи виявлення вторгнень. Показано, що використання цих технологій дозволяє суттєво підвищити ефективність захисту об'єктів та швидкість реагування на потенційні загрози.

Визначено основні виклики та особливості впровадження IoT-систем безпеки, серед яких ключовими є забезпечення масштабованості, надійності каналів зв'язку, сумісності з існуючою інфраструктурою та захист від кібератак.

Результати дослідження можуть бути використані при розробці та впровадженні систем безпеки різного призначення, від захисту приватних об'єктів до забезпечення безпеки критичної інфраструктури.

Подальші дослідження можуть бути спрямовані на розробку методів підвищення надійності та захищеності IoT-систем, а також на створення нових алгоритмів обробки даних для більш ефективного виявлення та запобігання загрозам.

ЛІТЕРАТУРА

1. Sotnik, S. V., et al. Analysis of design process of automated fire protection system // V Форум "Автоматизація, електроніка та робототехніка" (AERT-2023), 2023. – pp. 59-62.
2. Sotnik, S. V. Development of automated control system for continuous casting. Radio Electronics, Computer Science, Control, 2024. – №2. – pp. 181-189.
3. Hubar A.Y. et al. 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. – pp. 243-249.
4. Халімонов Я. І., та інші. 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, 2024. – pp. 176-181.
5. Сотник, С. В., та інші. Аналіз систем автоматизації визначення умов у житлових та робочих приміщеннях з використанням комп'ютерно-інтегрованих рішень. Автоматизація, електроніка та робототехніка (AERT-2023), 2023. – pp. 32-35.
6. Кирпота, Ф. В. та інші. Визначення функціональних вимог в автоматизованій теплиці // International Conference on Advanced Trends in Radioelectronics and Telecommunications dedicated to the 85th anniversary of the Department of Theoretical Radio Engineering and Radio Measurements, 2024, pp. 182-185.
7. Lvov, A., et al. Analysis of electronic locks existing systems // Manufacturing & Mechatronic Systems 2024: Proceedings of VIII st International Conference, Kharkiv, October 25-26, 2024. – pp. 24-27.
8. Sukhno, P., et al. Critical review of GSM network structure // Manufacturing & Mechatronic Systems 2024: Proceedings of VIII st International Conference, Kharkiv, October 25-26, 2024. – pp. 37-41.
9. Sotnik, S., et al. QR codes in production: дис. // Production & mechatronic systems, 2023. – pp. 19-22.
10. Sotnik, S. V., et al. Optimization of work: in-depth look at Kanban, Scrum and Lean // Journal of Natural Sciences and Technologies, 2024, 3 (1). – pp. 290-301
11. Зарубін, І. С. та інші. Ефективність використання роботизованих систем у виробництві //«Computer-integrated technologies, automation and robotics» CITAR-2024. 2024. – pp. 150-153.
12. Andreiev, A. S., et al. Analysis of robotics platforms for educational and research purposes. Комп'ютерні ігри та мультимедіа як інноваційний підхід до комунікації - 2024 // Матеріали IV Всеукраїнської науково-технічної конференції молодих вчених, аспірантів і студентів, Одеса, 26-27 вересня 2024 р., 2024. – pp. 25-27.
13. Sotnik, S. V., et al. Modeling design of mobile robotic platform // Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXIV Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів, 2024. – pp. 481-482
14. Sotnik, S. V., et al. Safe cobots in development of industrial robotics // European scientific

congress. Proceedings of the 8th International scientific and practical conference. Barca Academy Publishing, 2023. – pp. 80-84

15. Tverdokhlib, A., et al. Intelligent tools for optimizing information and search engines // Manufacturing & Mechatronic Systems 2024: Proceedings of VIII st International Conference, Kharkiv, October 25-26, 2024. – pp. 28-31.

16. Kaponkin, V. G., et al. The role of big data in improving functionality of search engines // The 8th International scientific and practical conference “European congress of scientific achievements” (August 12-14, 2024) Barca Academy Publishing, Barcelona, Spain, 2024. – pp. 69-76.

17. Nevludov, I. S., et al. Cloud giants: AWS, Azure and GCP: дис. // 2023 2nd International Conference on Innovative Solutions in Software Engineering Ivano-Frankivsk, 2023. – pp. 18-24.

18. Sotnik, S. V., et al. Analysis of searching methods for explosive objects using information technology and computer modeling // Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXIV Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 18-19 квітня 2024 р., 2024. – pp. 20-22.

19. Sotnik, S., et al. Gamification in science: game platforms for learning // Комп'ютерні ігри та мультимедіа як інноваційний підхід до комунікації - 2023 / Матеріали III Всеукраїнської науково-технічної конференції молодих вчених, аспірантів і студентів, Одеса, 28-29 жовтня 2023 р., 2023. – pp. 87-89.

20. Borysenko, I. A., et al. Chat gpt features in data search // The 9th International scientific and practical conference “Scientific progress: innovations, achievements and prospects” (May 29-31, 2023) MDPC Publishing, Munich, Germany, 2023. – pp. 139-143.

21. Sotnik, S. V. 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, 2024. – с. 42-45.

22. Sotnik, S. V. Implementation of game-based learning method // Комп'ютерні ігри та мультимедіа як інноваційний підхід до комунікації - 2024 / Матеріали IV Всеукраїнської науково-технічної конференції молодих вчених, аспірантів і студентів, Одеса, 26-27 вересня, 2024 р. – pp. 19-22.

23. Sotnik, S. V. Analysis of Personal Information Security Issues in Peacetime and Wartime // International Journal of Academic Engineering Research (IJAER), 2024. – Vol. 8 Issue 10. – pp. 108-113.

24. Sotnik, S., et al. Analysis of searching methods for explosive objects using information technology and computer modeling // Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXIV Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 18-19 квітня 2024 р., 2024. – pp. 20-22.

25. Boopathi, S. Securing Healthcare Systems Integrated With IoT: Fundamentals, Applications, and Future Trends // Dynamics of Swarm Intelligence Health Analysis for the Next Generation. IGI Global, 2023. – pp. 186-209.

26. Krishna, M. et al. A survey on multimedia analytics in security systems of cyber physical systems and IoT // 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC). IEEE, 2021. – pp. 1-7. // Int. Multidiscip. Sci. GeoConference Surv. Geol. Min. Ecol. Manag. SGEM, 2019, 9.2 (1). – pp. 569-577

27. Mahendra, S., Sathiyanarayanan M., Babu Vasu R. Smart security system for businesses using internet of things (iot) // 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE, 2018. – pp. 1-6