КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.705
УДК 004.021

Олійник Ярослав Сергійович
студент Факультету інформаційних технологій та математики
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0009-0005-4364-0934
ysoliinyk.fitm23m@kubg.edu.ua

Платоненко Артем Вадимович
кандидат технічних наук, доцент
доцент кафедри інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-2962-5667
a.platonenko@kubg.edu.ua

Черевик В'ячеслав Михайлович
кандидат технічних наук, доцент
доцент кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-2735-5341
v.cherevyk@kubg.edu.ua

Ворохоб Максим Віталійович
PhD in Cybersecurity
старший викладач кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-5160-7134
m.vorokhob@kubg.edu.ua

Шевчук Юрій
DataArt, 3530 Carol Ln, Northbrook, Illinois 60062, USA
ORCID ID: 0009-0008-3331-3886
shev4ukyuri@gmail.com

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕХНОЛОГІЯХ IOT

Анотація. У даній роботі розглянуті сучасні IoT-системи, які є невід'ємною частиною технологічного прогресу. Вони знайшли застосування у промисловості, транспорті, системах розумних будинків та інших технічних сферах. Проте, велика кількість підключених пристроїв, їхні обмежені обчислювальні ресурси та залежність від бездротових мереж роблять дані системи надзвичайно вразливими до атак, спрямованих на порушення конфіденційності, цілісності та доступності даних. У статті розглядається метод захисту інформації в IoT-системах, який враховує вразливості бездротових мереж і пристроїв, таких як IP-камери. Оскільки більшість IoT-пристроїв працюють у бездротових мережах, що робить їх особливо вразливими до атак типу відмови в обслуговуванні. Завдяки застосуванню багаторівневої автентифікації (використання паролів і двофакторної автентифікації), що дозволило знизити ризик несанкціонованого доступу до пристрою. Розглянуто метод захисту інформації для IoT-систем, який враховує специфічні вразливості та загрози, характерні для цих технологій. Досліджено загрози, зокрема атаки з використанням WiFi-jammer, які спричиняють відмову в обслуговуванні, та компрометацію RTSP-потоків відео. Запропонований метод захисту інформації передбачає багаторівневий підхід, який включає

шифрування даних, частотне перемикання для уникнення блокування сигналів та механізми захисту RTSP-потоків. Даний метод захисту інформації має велике практичне значення, оскільки може бути застосований для забезпечення безпеки в широкому спектрі IoT-систем. Експериментальна перевірка, що була реалізована на прикладі бездротової IP-камери TP-Link Tapo C100 продемонструвала ефективність запропонованих рішень у зниженні впливу атак та забезпеченні надійного функціонування IoT-пристроїв. У рамках проведеного дослідження було досягнуто комплексного розуміння вразливостей IoT-систем перед атаками на основі WiFi jammer, а також розроблено ефективні заходи захисту для забезпечення стабільності та безпеки таких систем. Подальші дослідження дозволять удосконалити існуючі методи захисту та розширити можливості для їх інтеграції в більш складні та масштабні IoT-системи.

Ключові слова: IoT; Wi-Fi; RTSP; технології інтернету речей; подавління; кіберзагрози, мережеві атаки; інформаційна безпека; захист від атак.

ВСТУП

Технології Інтернету речей (IoT) стали ключовим елементом цифрової трансформації у багатьох сферах, таких як промисловість, транспорт, медицина, розумний дім та державне управління. Взаємодія пристроїв IoT забезпечує автоматизацію процесів, збір і аналіз даних у реальному часі, а також підвищення ефективності роботи систем. Водночас поширення IoT-систем супроводжується новими викликами, серед яких головними є загрози інформацій безпеці.

Постановка проблеми. IoT-пристрої [9], на відміну від традиційних обчислювальних систем, мають обмежені ресурси: потужність процесора, об’єм пам’яті та енергоспоживання. Це обмежує можливість впровадження складних механізмів захисту, таких як асиметричне шифрування, або багатофакторна автентифікація. Крім того, більшість IoT-пристроїв працюють у бездротових мережах, що робить їх особливо вразливими до атак типу відмови в обслуговуванні (DoS), перехоплення даних (Man-in-the-Middle) або фізичного подавлення сигналів, таких як атаки WiFi-jammer.

Аналіз останніх досліджень і публікацій. Основна проблема полягає у створенні методу захисту інформації в IoT-системах, який враховує специфіку атак із використанням WiFi-jammer. Зокрема, запропонована модель об’єднує механізми захисту передачі даних, методи виявлення та обмеження впливу атак на рівні пристроїв, а також заходи для забезпечення безпеки потокового передавання RTSP, на відміну від існуючих підходів, які здебільшого фокусуються на окремих аспектах безпеки (наприклад, шифрування даних чи фізичний захист), запропонована модель є багаторівневою та враховує всі основні вразливості IoT-систем. Вона забезпечує інтегрований захист, охоплюючи як рівень передачі даних, так і рівень пристроїв та інфраструктури.

Мета статті. Метою цієї роботи є розробка методу захисту інформації в IoT-системах, який враховує специфічні загрози безпеки, включаючи атаки WiFi-jammer та компрометацію потокового передавання даних через RTSP. Запропонований метод має забезпечити високу ефективність у реальних умовах, зберігаючи при цьому доступність і продуктивність пристроїв.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Методи дослідження.
Аналіз загроз та вразливостей IoT.
Проведено аналіз характерних для IoT-систем кіберзагроз, що включає:

- Загрози WiFi-jammer [4]. Атаки, спрямовані на блокування радіосигналів, викликають збої у функціонуванні бездротових IoT-пристроїв.
  Досліджено особливості дії WiFi-jammer на камеру Tapo C100 [10], яка функціонує в стандартних мережах Wi-Fi.
- Загрози RTSP-стрімінгу. Протокол RTSP, що використовується для передавання відеоданих у реальному часі, вразливий до атак типу «людина посередині» (Man-in-the-Middle), що можуть призвести до витоку або маніпуляції відео.
- Атаки на автентифікацію та авторизацію. Досліджено ризики, пов'язані із застосуванням стандартних паролів або слабкої автентифікації в IoT-пристроях.

МЕТОДИ ДОСЛІДЖЕННЯ

Для реалізації методу та проведення експериментів використано:

- Програмні засоби: VLC (VideoLAN Client) — медіа-плеєр і сервер потокового передавання, Nmap (Network Mapper) — сканер мереж [5], Hydra — інструмент для виконання брутфорс-атак (Kali linux).
- Апаратні засоби: IP-камера Tapo C100, плата ESP8266, маршрутизатор, смартфон, ноутбук.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Вразливості IoT-систем

IoT-системи [1], [3], [6] представляють собою складні багаторівневі мережі, які включають різноманітні пристрої, сенсори, шлюзи та сервери. Через специфіку їхньої архітектури, використання бездротових мереж і обмежені ресурси вони особливо вразливі до кіберзагроз. Основні типи вразливостей можна класифікувати за рівнями системи.

На рівні пристроїв:

- Обмежені обчислювальні ресурси IoT-пристроїв не дозволяють використовувати складні механізми шифрування або автентифікації.
- Використання стандартних або слабких паролів значно полегшує зловмисникам доступ до пристроїв.
- Відсутність регулярних оновлень програмного забезпечення залишає пристрої вразливими до відомих атак.

На рівні передачі даних:

- Використання незахищених протоколів, таких як RTSP [2] без шифрування, робить потоки даних доступними для перехоплення.

- Відсутність шифрування переданих даних дозволяє зловмисникам проводити атаки типу «людина посередині» (Man-in-the-Middle).
- IoT-пристрої часто працюють у стандартних частотних діапазонах (наприклад, Wi-Fi 2.4 GHz), що робить їх вразливими до атак WiFi-jammer.

Основні принципи розробки методу захисту

Методи захисту складається з таких основних компонентів:

Таблиця 1

Компоненти методу захисту IoT

Компонент методу	Мета	Засоби реалізації
Шифрування даних	Забезпечення конфіденційності та цілісності даних, що передаються між пристроями IoT.	– Симетричне шифрування AES – Асиметричне шифрування ECC
Анти-Jamming стратегії	Захист від атак WiFi-jammer.	– Частотне перемикання (Frequency Hopping) – Проктокол WPA3 знижує ризик атак
Захист RTSP-потоків	Забезпечення безпеки потокового передавання відео за протоколом RTSP.	– Посилена автентифікація – Ізолювання пристроїв
Механізми виявлення аномалій	Моніторинг активності IoT-пристроїв для виявлення загроз.	– Системи виявлення вторгнень (IDS) – Алгоритми машинного навчання
Архітектура методу	Багаторівнева модель, яка забезпечує комплексний захист IoT-мережі.	– **Рівень пристроїв**: Шифрування даних (AES), захист від фізичного доступу – **Рівень передачі даних**: Захист RTSP, частотне перемикання – **Рівень аналізу трафіку**: IDS, ML алгоритми
Переваги методу	Покращення стабільності та безпеки роботи IoT-пристроїв, навіть у випадках з обмеженими ресурсами.	– Зменшення впливу атак WiFi-jammer – Забезпечення конфіденційності й цілісності RTSP-потоків – Підвищення загального рівня захисту IoT-пристроїв

Експериментальна демонстрація атак

На базі створеної IoT-мережі було змодельовано кілька реальних сценаріїв атак (рис. 1):

- Атака DDoS: За допомогою ESP8266 (WiFi jammer) було організовано атаку на роутер, до якого підключена IP-камера Tapo C100.
- У результаті було виявлено, що перевантаження мережі призводить до втрати зв’язку з пристроєм і припинення передачі даних.
- Атака Man-in-the-Middle (MitM): За допомогою інструментів сканування та підбору стандартних облікових даних було отримано доступ до відеопотоку тестового пристрою (IP-камера Tapo C100).

ISSN 2663 - 4023

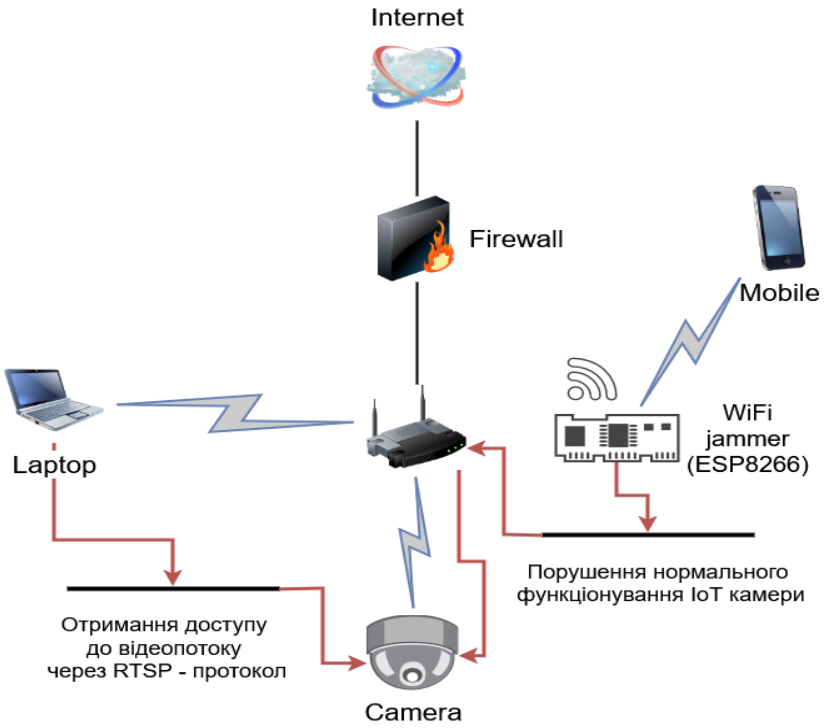

Рис. 1. Архітектура IoT-мережі з моделлю атаки за допомогою WiFi-jammer та отримання доступу до відеопотоку

У ході дослідження було розроблено та впроваджено захисні механізми. Їх ефективність оцінювалася за наступними критеріями:

Конфіденційність даних

Застосування багаторівневої автентифікації (використання паролів і двофакторної автентифікації) дозволило знизити ризик несанкціонованого доступу до пристрою.

Стійкість до атак

Перехід на протокол WPA3 зменшує ризик атак через вдосконалене шифрування та захист від пасивного перехоплення даних.

Налаштування IoT-пристроїв для роботи на 2,4 ГГц і 5 ГГц з можливістю динамічної зміни частоти.

Моніторинг і виявлення загроз

Застосування інструментів моніторингу мережевого трафіку, забезпечило виявлення підозрілої активності. Виявлення DDoS-атаки дозволило активувати механізми блокування в режимі реального часу.

Підсумок результатів

Дослідження підтвердило, що ефективний захист IoT-систем можливий за умови комплексного підходу [7], [8], [11], [12], який включає:

- Впровадження сучасних методів автентифікації та шифрування даних [14], [15].
- Регулярне оновлення прошивки пристроїв для усунення виявлених вразливостей.
- Використання інструментів моніторингу для раннього виявлення та реагування на загрози [16], [17], [18].

Отримані результати демонструють, що комбінація цих підходів значно підвищує рівень захисту IoT-систем. Проте, залишаються відкритими питання щодо забезпечення безпеки пристроїв із низькими обчислювальними ресурсами та вразливостей, які виникають через людський фактор (наприклад, використання слабких паролів).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження було розглянуто метод захисту інформації для IoT-систем, який враховує специфічні вразливості та загрози, характерні для цих технологій. Метод поєднує кілька важливих компонентів захисту, серед яких шифрування даних, анти-Jamming стратегії, автентифікація доступу та захист потоків RTSP. Важливою особливістю цього методу є його адаптивність до обмежених ресурсів IoT-пристроїв, що є характерною рисою більшості сучасних пристроїв.

Розглянутий метод захисту має велике практичне значення, оскільки може бути застосована для забезпечення безпеки в широкому спектрі IoT-систем. Його впровадження дозволить знизити ризики, пов’язані з перехопленням даних та відмовами в обслуговуванні через атаки WiFi-jammer, а також запобігти несанкціонованому доступу до відео-потоків. Це, в свою чергу, підвищить рівень безпеки в таких сферах, як розумні будинки, промислові IoT-мережі, системи відеоспостереження та інші застосування, де IoT-пристрої використовуються для передачі чутливих даних.

Таким чином, розглянутий метод захисту інформації в IoT-системах є важливим кроком до створення безпечного середовища для використання IoT-технологій. Він забезпечує ефективний захист від атак WiFi-jammer, захищає передану інформацію через RTSP-протокол, а також пропонує стійкі стратегії для підвищення безпеки IoT-пристроїв у реальних умовах. Подальші дослідження дозволять удосконалити існуючі методи захисту та розширити можливості для їх інтеграції в більш складні та масштабні IoT-системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cvetković, A., Radojčić, V., Adamović, S. (2021). Multi-factor Authentication for the Internet of Things. *XXII MEĐUNARODNI NAUČNI SKUP, 22(7),* 61–64. https://doi.org/10.7251/ZRSNG2101013C
2. Schulzrinne, H., Rao, A., Lanphier, R. (1998). *Real Time Streaming Protocol (RTSP).* https://doi.org/10.17487/RFC2326
3. *IoT Security Foundation. Best Practice Guidelines for IoT Security.* (2022).
4. Pirayesh, H., Zeng, H. (2022). Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials, 24(2),* 767–809. https://doi.org/10.1109/COMST.2022.3159185
5. *Nmap: The Network Mapper.* (n.d.). https://nmap.org/
6. Ashton, K. (2009). That “Internet of Things” Thing. *RFID Journal.*
7. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. NISTIR 8228.* (2019). National Institute of Standards and Technology (NIST).
8. *IoT Security Foundation Guidelines. Recommendations for the security of IoT devices.* (n.d.). https://www.iotsecurityfoundation.org/
9. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88,* 10–28.
10. *Official documentation of IP-camera TpLink Tapo C100. User manual and specifications.* (n.d.). https://www.tp-link.com/uk-ua/support/download/tapo-c100/

11. Sokolov, V., Skladannyi, P., & Platonenko, A. (2023). Jump-Stay Jamming Attack on Wi-Fi Systems. In: *IEEE 18th International Conference on Computer Science and Information Technologies*, 1–5. https://doi.org/10.1109/CSIT61576.2023.10324031
12. Sokolov, V., Skladannyi, P., Astapenya, V. (2023). Bluetooth Low-Energy Beacon Resistance to Jamming Attack. In: *IEEE 13th International Conference on Electronics and Information Technologies*, 270–274. https://doi.org/10.1109/ELIT61488.2023.10310815
13. Sokolov, V., Skladannyi, P., Korshun, N. (2023). ZigBee Network Resistance to Jamming Attacks. In: *IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics*, 161–165. https://doi.org/10.1109/UkrMiCo61577.2023.10380360
14. Sokolov, V., Skladannyi, P., Astapenya, V. (2023). Wi-Fi Interference Resistance to Jamming Attack. In: *IEEE 5th International Conference on Advanced Information and Communication Technologies*, 1–4. https://doi.org/10.1109/AICT61584.2023.10452687
15. Sokolov, V., Skladannyi, P., Mazur, N. (2023). Wi-Fi Repeater Influence on Wireless Access. In: *IEEE 5th International Conference on Advanced Information and Communication Technologies*, 33–36. https://doi.org/10.1109/AICT61584.2023.10452421
16. Kriuchkova, L., Sokolov, V., Skladannyi, P. (2024). Determining the Zone of Successful Interaction in RFID Technologies. In: *IEEE 29th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory*, 168–171. https://doi.org/10.1109/diped63529.2024.10706153
17. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Oliinyk Yaroslav
Student of Faculty of Information Technologies and Mathematics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0009-0005-4364-0934
ysoliinyk.fitu19@kubg.edu.ua

Artem Platonenko
PhD, Associate Professor, Docent of the Department of Information and
Cyber Security named after Professor Volodymyr Buryachok,
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-2962-5667
a.platonenko@kubg.edu.ua

Vyacheslav Cherevyk
PhD, Associate Professor,
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-2735-5341
v.cherevyk@kubg.edu.ua

Maksym Vorokhob
PhD in Cybersecurity
Senior Teacher of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-5160-7134
m.vorokhob@kubg.edu.ua

Yurii Shevchuk
DataArt, 3530 Carol Ln, Northbrook, Illinois 60062, USA
ORCID ID: 0009-0008-3331-3886
shev4ukyuri@gmail.com

METHODS OF INFORMATION SECURITY IN IOT-TECHNOLOGIES

Abstract. This paper examines modern IoT systems, which are an integral part of technological progress. They have found application in industry, transport, smart home systems and other technical areas. However, the large number of connected devices, their limited computing resources and dependence on wireless networks make these systems extremely vulnerable to attacks aimed at violating the confidentiality, integrity and availability of data. The article considers a method for protecting information in IoT systems, which takes into account the vulnerabilities of wireless networks and devices such as IP cameras. Since most IoT devices operate in wireless networks, this makes them particularly vulnerable to denial of service attacks. Thanks to the use of multi-level authentication (using passwords and two-factor authentication), which allowed reducing the risk of unauthorized access to the device. A method for protecting information for IoT systems is considered, which takes into account the specific vulnerabilities and threats characteristic of these technologies. Threats, including attacks using WiFi jammers that cause denial of service and compromise of RTSP video streams, were investigated. The proposed information protection method involves a multi-level approach that includes data encryption, frequency switching to avoid signal blocking, and RTSP stream protection mechanisms. This information protection method is of great practical importance, as it can be used to ensure security in a wide range of IoT systems. Experimental testing, which was implemented using the example of the TP-Link Tapo C100 wireless IP camera, demonstrated the effectiveness of the proposed solutions in reducing the impact of attacks and ensuring reliable operation of IoT devices. As part of the research, a comprehensive understanding of the vulnerabilities of IoT systems to WiFi jammer-based attacks was achieved, and effective protection measures were developed to ensure the stability and security of such systems.

Further research will allow improving existing protection methods and expanding the possibilities for their integration into more complex and large-scale IoT systems.

Keywords: IoT; Wi-Fi; RTSP; Internet of Things technologies; suppression; cyber threats, network attacks; information security; protection against attacks.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Cvetković, A., Radojčić, V., Adamović, S. (2021). Multi-factor Authentication for the Internet of Things. *XXII MEĐUNARODNI NAUČNI SKUP, 22(7),* 61–64. https://doi.org/10.7251/ZRSNG2101013C
2. Schulzrinne, H., Rao, A., Lanphier, R. (1998). *Real Time Streaming Protocol (RTSP).* https://doi.org/10.17487/RFC2326
3. *IoT Security Foundation. Best Practice Guidelines for IoT Security.* (2022).
4. Pirayesh, H., Zeng, H. (2022). Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials, 24(2),* 767–809. https://doi.org/10.1109/COMST.2022.3159185
5. *Nmap: The Network Mapper.* (n.d.). https://nmap.org/
6. Ashton, K. (2009). That "Internet of Things" Thing. *RFID Journal.*
7. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. NISTIR 8228*. (2019). National Institute of Standards and Technology (NIST).
8. *IoT Security Foundation Guidelines. Recommendations for the security of IoT devices*. (n.d.). https://www.iotsecurityfoundation.org/
9. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88,* 10–28.
10. *Official documentation of IP-camera TpLink Tapo C100. User manual and specifications.* (n.d.). https://www.tp-link.com/uk-ua/support/download/tapo-c100/
11. Sokolov, V., Skladannyi, P., & Platonenko, A. (2023). Jump-Stay Jamming Attack on Wi-Fi Systems. In: *IEEE 18th International Conference on Computer Science and Information Technologies*, 1–5. https://doi.org/10.1109/CSIT61576.2023.10324031
12. Sokolov, V., Skladannyi, P., Astapenya, V. (2023). Bluetooth Low-Energy Beacon Resistance to Jamming Attack. In: *IEEE 13th International Conference on Electronics and Information Technologies*, 270–274. https://doi.org/10.1109/ELIT61488.2023.10310815
13. Sokolov, V., Skladannyi, P., Korshun, N. (2023). ZigBee Network Resistance to Jamming Attacks. In: *IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics*, 161–165. https://doi.org/10.1109/UkrMiCo61577.2023.10380360
14. Sokolov, V., Skladannyi, P., Astapenya, V. (2023). Wi-Fi Interference Resistance to Jamming Attack. In: *IEEE 5th International Conference on Advanced Information and Communication Technologies*, 1–4. https://doi.org/10.1109/AICT61584.2023.10452687
15. Sokolov, V., Skladannyi, P., Mazur, N. (2023). Wi-Fi Repeater Influence on Wireless Access. In: *IEEE 5th International Conference on Advanced Information and Communication Technologies*, 33–36. https://doi.org/10.1109/AICT61584.2023.10452421
16. Kriuchkova, L., Sokolov, V., Skladannyi, P. (2024). Determining the Zone of Successful Interaction in RFID Technologies. In: *IEEE 29th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory*, 168–171. https://doi.org/10.1109/diped63529.2024.10706153
17. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.