спотворень на рівні сенсорів, шлюзів, сервісів обробки та під час формування керуючих рішень. У таких умовах інтервальний моніторинг передбачає здійснення контролю в межах допустимого інтервалу змін, який залежить від режиму функціонування, шумів, затримок та невизначеностей моделі. Підтвердження цьому висвітлено в роботі [1], де розглядаються інтервальні спостерігачі, стійкі до атак у ролі засобу оцінювання стану. Такий стан розглядається за умов прихованих атак, які спричиняють маскування порушення цілісності в допустимих межах фіксованого порогу.

Аналіз роботи [2], де представлено удосконалений метод інтервального оцінювання дозволив виявити та сформувати три основні взаємопов'язані проблеми інтервального моніторингу: складність відокремлення початкової фази вторгнень від штатних коливань системи, швидка втрата інформативності фіксованих меж контролю у змінних умовах функціонування, збільшення кількості хибних спрацювань за умов підвищення чутливості моніторингу.

Отже, перспективним напрямком вирішення зазначених проблем є поєднання інтервального моніторингу з інтелектуальним уточненням меж штатного функціонування системи. Важливим є інтелектуальне коригування інтервалів за поточним профілем функціонування системи. Доцільно формалізувати правила коригування, вибір ознак порушення цілісності та узгодження моніторингу з допустимим рівнем хибних спрацювань тривог.

1. Degue K.H., Ny J.L., Efimov D. Stealthy attacks and attack-resilient interval observers. *Automatica*. 2022. Vol. 146. URL: https://doi.org/10.1016/j.automatica.2022.110558 (дата звернення: 04.05.2026).
2. Fan J., Huang J., Zhao. X. Improved interval estimation method for cyber-physical systems under stealthy deception attacks. *IEEE Transactions on Signal and Information Processing Over Networks*. 2022. Vol. 8. P. 1-11.

Алгоритм аудіостеганографії без внесення змін у файл-контейнер

УДК 004.056.5

Костянтин Фріга[1], Юрій Дорофєєв[2], Ірина Назарова[3]

Національний університет «Одеська політехніка»,
[1]10252733@stud.op.edu.ua, [2]dym@op.edu.ua, [3]nazarova.i.v@op.edu.ua

Переважна більшість методів аудіостеганографії передбачає вбудовування корисного повідомлення безпосередньо в аудіоконтейнер, причому одним з основних показників якості методу є степень непомітності внесених змін з точки зору слухової системи людини [1], [2].

В [3], [4] розглянуто спосіб прихованого передавання інформації за допомогою монохромних, кольорових графічних файлів та аудіофайлів без зміни контейнера на основі методу Zero Distortion Technique (метод нульового спотворення - МНС). На відміну від традиційних методів аудіостеганографії, де повідомлення безпосередньо вбудовується в сигнал і може змінювати його структуру, у МНС контейнер використовується як готова бітова послідовність.

Повідомлення відновлюється за координатами позицій, у яких у контейнері вже наявні потрібні бітові фрагменти.

У роботі [4] розглянуто застосування методу нульового спотворення саме в аудіостеганографії. Автори описують підхід, за якого аудіоконтейнер не змінюється, приховане повідомлення передається побітово (один біт повідомлення на один семпл аудіоконтейнера), відновлюється за матрицею індексів. Для захисту цієї матриці використовується Indexed Based Chaotic Sequence, тобто хаотична перестановка координат [3].

Метою роботи є суттєве зменшення обсягу координатних даних при використанні методу МНС для прихованого передавання текстових даних. У запропонованому варіанті використано 6-8-бітове контейнерозалежне кодування, за якого одна координата відповідає не окремому біту, а цілому 6-8-бітовому коду символу. Для цього програма аналізує конкретний аудіофайл, визначає наявні бітові комбінації у MSB-вікні та формує адаптивний алфавіт, залежний від структури контейнера. Додатково передбачено перевірку достатності координат, заборону повторного використання позицій і хаотичну перестановку матриці координат на основі логістичного відображення.

Під час декодування використовується той самий контейнер і відповідний масив координат.

Якщо аудіофайл або індексний масив було змінено, зв'язок між координатами та бітовими фрагментами може порушуватися, тому повідомлення може відновлюватися неправильно. Результати тестування показали, що запропонований підхід при збереженні головної властивості МНС дозволяє отримати зменшення розміру службового індексного файлу не менше, ніж у k разів, де k – розрядність використаної кодировки символів, порівняно з побітовим варіантом та використанням матриці координат.

Окремо розглянуто вплив типових атак на бітову структуру аудіосигналу: заміна молодших бітів не має впливу на повідомлення, якщо робочі коди формуються з MSB-області, тоді як адитивна шумова атака є більш небезпечною через можливий вплив на старші біти при переповненні молодших.

Отже, запропоноване удосконалення зменшує службові витрати МНС і зберігає незмінність контейнера, але потребує суворої відповідності отриманого масиву індексів аудіоконтейнеру.

1. Joshi R., Trivedi M.C., Goyal V., Bhati D. Recent Trends for Practicing Steganography Using Audio as Carrier: A Study. Advances in Data and Information Sciences. Singapore: Springer, 2023. Vol. 522. P. 549-555. URL: https://doi.org/10.1007/978-981-19-5292-0_52 (дата звернення: 15.04.2026).
2. AlSabhany A.A., Ali A.H., Ridzuan F., Azni A.H., Mokhtar M.R. Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. Computer Science Review. 2020. Vol. 38. Article 100316. URL: https://doi.org/10.1016/j.cosrev.2020.100316 (дата звернення: 15.04.2026).
3. Shivani, Yadav V.K., Batham S. Zero Distortion Technique: An approach

to image steganography on color images using strength of Chaotic Sequence. Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, 2014.New York: ACM, 2014. URL:
4. https://doi.org/10.1145/2677855.2677905 (дата звернення: 04.05.2026).
5. Sharma S., Yadav V.K., Trivedi M.C., Gupta A. Audio Steganography using ZDT: Encryption using Indexed Based Chaotic Sequence. Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, 2016. New York: ACM, 2016. URL: https://doi.org/10.1145/2905055.2905272 (дата звернення: 04.05.2026).

Інтеграція OIDC-провайдера в енергетичну систему для забезпечення контролю доступу

УДК 004.056.5

Андрій Волощук[1], Іван Бородій[2], Галина Осухівська[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]andrii_voloshchuk3969@tntu.edu.ua, [2]ivanborodii@tntu.edu.ua,
[3]osukhivska@tntu.edu.ua

Енергетична система, що поєднує прилади обліку, датчики параметрів мережі, релейні контролери, диспетчерські сервіси та засоби моніторингу, потребує єдиної процедури ідентифікації з метою обміну даними. Шифрування каналів MQTT/TLS, CoAP/DTLS або HTTPS/TLS захищає передавання даних від перехоплення, однак не гарантує безпеки системи. Тому інтеграція OIDC-провайдера в енергетичну систему є важливою для централізованого керування доступом, дозволяє здійснювати аудит подій та запобігати несанкціонованому підключенню. Це особливо важливо для об'єктів, де обладнання працює тривалий час, а ручне переналаштування доступу може впливати на продуктивність роботи.

OIDC-провайдер у такій архітектурі виконує роль надійної компоненти в енергетичній системі. Він видає підписані JWT-токени, а служба маршрутизації повідомлень перевіряє їх локально за відкритим ключем провайдера. Це дає змогу реалізувати модель нульової довіри, за якої кожна дія перевіряється незалежно від розташування компонента в мережі.

Узагальнену архітектуру енергетичної інфраструктури з використанням OIDC-провайдера наведено на рисунку 1.

На першому етапі роботи системи здійснюється реєстрація та підтвердження нового IoT-пристрою. Для цього доцільно використовувати сценарій Device Authorization Flow, в якому пристрій ініціює запит, отримує службові коди, а оператор підтверджує підключення через SCADA-консоль або інший захищений інтерфейс. Після підтвердження OIDC-провайдер видає підписаний токен доступу, де введення обладнання потребує участі відповідального персоналу [1].

Другий етап полягає у передаванні токена до служби маршрутизації повідомлень під час підключення. JWT-токен є не лише доказом автентифікації,