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,

а й носієм правил доступу. Поле allowed_topics визначає дозволені канали MQTT або ресурси CoAP, permitted_protocols задає допустимі протоколи обміну, roles і scope описують роль та дозволені операції, а security_level розмежовує обладнання передавання та керування [2].

Третій етап передбачає локальне застосування політик доступу. Служба маршрутизації перевіряє підпис JWT, строк дії, призначення, дозволені канали, протоколи та ролі без окремого звернення до сервера авторизації для кожного повідомлення. Усі відмови, спроби звернення до заборонених ресурсів і наближення завершення строку дії токена фіксуються в журналах безпеки, що спрощує аудит інцидентів.

Четвертий етап пов'язаний з вибором протоколу обміну. Аналітичний модуль може враховувати затримку, втрати пакетів, пропускну здатність і навантаження служби маршрутизації, однак він має рекомендувати лише ті протоколи, які зазначені у permitted_protocols конкретного пристрою. Отже, адаптивне перемикання між MQTT, CoAP і HTTPS не обходить політику безпеки, а діє в межах наперед визначених дозволів [3].

П'ятий етап стосується стійкості до відмов і кібератак. Якщо OIDC-провайдер тимчасово недоступний, обладнання з чинними токенами продовжує передавання даних до завершення строку їх дії, тоді як нові або не підтверджені підключення блокуються.

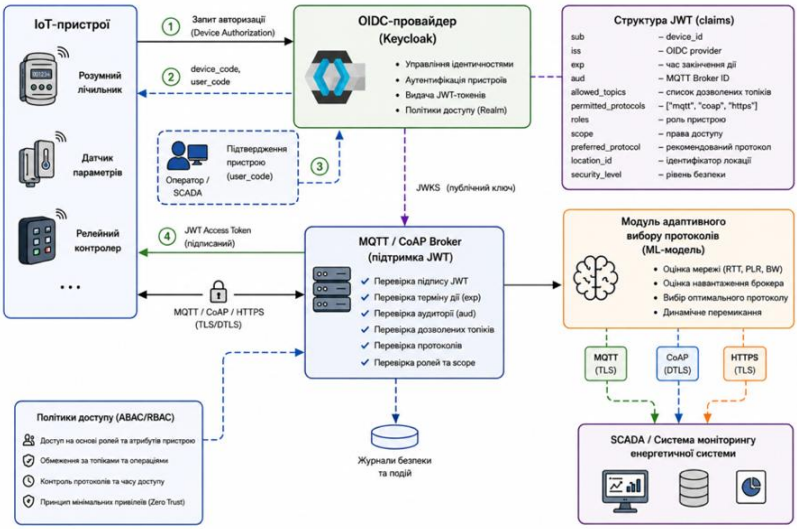

Рис. 1. Архітектура системи IoT-вузлів енергетичної інфраструктури на основі OIDC-провайдера

Така інтеграція забезпечує безперервність роботи компонентів, централізований контроль прав доступу та застосування політик у системі енергетичної інфраструктури.

1. Denniss W., Bradley J. RFC 8628: OAuth 2.0 Device Authorization Grant. IETF, 2019. URL: https://datatracker.ietf.org/doc/html/rfc8628.
2. Jones M., Bradley J., Sakimura N. RFC 7519: JSON Web Token (JWT). IETF, 2015. DOI: 10.17487/RFC7519.
3. Voloshchuk A. & Osukhivska H. Adaptive multi-protocol communication for energy systems. Scientific Journal of the Ternopil National Technical University. 2025. Vol. 119, No. 3. P. 97-106.

Ампліфікація інтегрованої системи управління інформаційною безпекою

УДК 004(056.53+413.4)::001.51

Володимир Мохор[1], Олександр Бакалинський[1], Ярослав Дорогий[2], Василь Цуркан[1,3]

[1]ІПМЕ ім. Г.Є. Пухова НАН України, v.mokhor@gmail.com, baov@meta.ua

[2]ДонНТУ, yaroslav.dorohyi@donntu.edu.ua
[3]КПІ ім. Ігоря Сікорського, v.v.tsurkan@gmail.com

Діяльність будь-якої організації орієнтована на задоволення потреб і очікувань зацікавлених сторін [1]. Серед них виокремлюється зберігання властивостей інформації. Насамперед конфіденційності (приватності), цілісності та доступності [2]. Таке виділення пов'язується з тим, що інформація є цінністю для організацій і тлумачиться як актив. До того ж з використанням продуктів, послуг на основі штучного інтелекту [3]. Це спонукає до забезпечення їх відповідального розроблення, упровадження, використання та, як наслідок, призводить до виникнення емерджентних ризиків. Тож ампліфікування інтегрованої системи управління інформаційною безпекою є актуальним.

Розробляння інтегрованої системи управління інформаційною безпекою на прикладі сфери енергетики було запропоновано в [2]. Її складники визначено з урахуванням внутрішніх і зовнішніх обставин діяльності організацій. З огляду на це інтегровано системи управління інформаційною безпекою, кібербезпекою і приватністю. Завдяки отриманому рішенню можливе забезпечення непорушності властивостей конфіденційності, приватності, цілісності, доступності інформаційних активів. У даному випадку базовим складним виокремлено систему управління інформаційною безпекою. Попри це, впровадженістю продуктів, послуг на основі штучного інтелекту зумовлено необхідність гарантування належності обробляння відповідних емерджентних ризиків. Зокрема, протидіяння негативним проявам, наприклад [3], змінювання способів розроблення, упровадження, використання і поведінки. Тому системою управління штучним інтелектом [3] пропонується розширити запропоноване в [2] інтегроване рішення [1].

Отже, ампліфікація інтегрованої системи управління інформаційною безпекою дозволить забезпечити застосовність продуктів, послуг на основі штучного інтелекту відповідно до потреб і очікувань зацікавлених сторін. І, як