УДК 004.056:620.9

РОЗРОБКА ДИНАМІЧНОЇ МОДЕЛІ АВТОРИЗАЦІЇ ДОСТУПУ ДО РЕСУРСІВ У REST API БАНКІВСЬКОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ КОНТЕКСТНО-ЗАЛЕЖНОЇ ПЕРЕВІРКИ ПРАВ ДОСТУПУ В УМОВАХ ЕНЕРГОЕФЕКТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Порхун А.О. – МгІТ-24, магістрант, *arrttemm2003@gmail.com*
Гольдберг М.І. – к.т.н., доцент., *marjanagoldberg@gmail.com*
Київський національний університет технологій та дизайну

Мета роботи - створення динамічної моделі авторизації доступу до ресурсів у REST API банківських систем, що базується на контекстно-залежній перевірці прав доступу з урахуванням параметрів середовища та енергетичних характеристик обчислювальних вузлів, з метою підвищення рівня інформаційної безпеки й енергоефективності IT-інфраструктури.

В сучасних умовах цифрової трансформації банківська інфраструктура активно інтегрується з системами енергетичного менеджменту, «розумними» мережами (smart grid), платформами «зелених фінансів» та сервісами енергоефективності. REST API чамто виступає основним інтерфейсом для обміну даними між фінансовими установами, клієнтськими застосунками, державними енергетичними реєстрами та IoT-пристроями (наприклад, лічильниками енергоспоживання). Питання захищеного та енергоефективного доступу до таких ресурсів набуває особливого значення, оскільки будь-які витоки або надмірні обчислення призводять не лише до ризиків безпеки, але й до зайвого енергоспоживання серверної інфраструктури.

В енергетичних та фінансових платформах обмін даними відбувається в реальному часі, наприклад, при обробці транзакцій за «зеленими тарифами», аналізі енергоспоживання домогосподарств, розрахунку компенсацій за енергоощадні програми. Такі сервіси базуються на великій кількості запитів до REST API. Якщо система авторизації не буде оптимізована або побудована на статичних перевірках, це призведе до зайвих викликів, повторних перевірок і збільшення енергоспоживання дата-центрів.

Використання динамічної, контекстно-залежної моделі дозволяє:зменшити кількість непотрібних обчислень через адаптивне прийняття рішень (авторизація тільки в необхідні моменти); інтелектуально розподіляти навантаження між мікросервісами на основі контексту (локації, ризику, типу запиту), що також впливає на зниження енергозатрат у хмарній інфраструктурі; підвищити загальну енергоефективність інформаційних систем, зменшуючи обсяги несанкціонованого або надлишкового трафіку. Таким

чином, безпечний контроль доступу перетворюється не лише на питання кібербезпеки, а й на компонент «цифрового енергозбереження», що відповідає концепції Green IT.

Запропонована модель базується на підходах Attribute-Based Access Control (ABAC) і Context-Aware Authorization. Її основні елементи це: суб'єкт доступу - користувач, сервіс або пристрій IoT із набором атрибутів (роль, ризик-рівень, геолокація, тип підключення); ресурс - об'єкт REST API (фінансові або енергетичні дані, реєстр лічильників); контекст середовища - параметри, що описують умови запиту (час, тип мережі, статус пристрою, споживана потужність, рівень енергетичного навантаження серверного вузла); політика доступу - набір правил, що враховують комбінацію атрибутів і контексту для прийняття рішення (дозвіл / заборона / частковий доступ).

Новизна полягає у введенні енергетичного контексту як додаткового фактора. Наприклад, система може: обмежувати доступ до «важких» обчислювальних запитів під час пікових енергетичних навантажень; маршрутизувати запити до серверів із нижчим поточним споживанням енергії; знижувати частоту перевірок у режимі низького ризику (енергозбереження CPU).

Архітектура моделі включає:

- Policy Decision Point (PDP) що аналізує запит з урахуванням контексту.
- Policy Enforcement Point (PEP)- це інтегрований у REST API шлюз, що блокує або дозволяє запит.
- Context Collector який збирає атрибути (середовище, енергоспоживання, ризик).
- Audit Logger, веде журнал дій для оцінки впливу політик на безпеку та енергоефективність.

Реалізація може базуватися на відкритих платформах (Keycloak, OPA, XACML), розширених модулями моніторингу енергоспоживання.

Модель може застосовуватись у:

- Банківських API, що підтримують сервіси «зеленого кредитування» чи фінансування енергоощадних проєктів.
- Інтелектуальних енергомережах, де REST API забезпечує обмін даними між датчиками споживання та аналітичними платформами.
- Енергосервісних компаніях, які використовують банківські шлюзи для автоматичних платежів і контролю енергоресурсів.У таких системах контекстно-залежна авторизація дозволяє зменшити кількість запитів до бази даних і процесорних обчислень, підвищити безпеку обміну та знизити

енерговитрати дата-центрів до 10–15 %, завдяки скороченню надлишкових перевірок та адаптивному управлінню навантаженням.

Подальший розвиток роботи доцільно спрямувати на розширення контекстної моделі за рахунок інтеграції додаткових факторів, таких як стан мережевого трафіку, прогноз навантаження на сервери, кліматичні параметри середовища та динаміка цін на енергоресурси. Це дозволить створювати більш адаптивні та «енергетично свідомі» політики доступу. Також доцільною буде інтеграція із системами моніторингу енергоспоживання дата-центрів і сервісами «зелених IT», що забезпечить динамічну оптимізацію розподілу запитів REST API між вузлами з найвищою енергоефективністю. Можна розробити прототип системи «енергоефективної авторизації» з відкритим вихідним кодом, яка може стати основою для впровадження в українських фінансових та енергетичних IT-системах у межах концепції «цифрового енергозбереження».

Висновки. Розроблена динамічна модель авторизації доступу до ресурсів REST API поєднує принципи інформаційної безпеки та енергоефективності цифрових систем. Її особливістю є використання контексту середовища (у тому числі енергетичного) для прийняття рішень про доступ у реальному часі. Це дозволяє: підвищити рівень кіберзахисту; знизити навантаження на обчислювальні потужності; забезпечити сталий розвиток енергетичних і фінансових IT-платформ. Таким чином, запропонований підхід сприяє не лише безпечній інтеграції банківських REST API у цифрову економіку, але й реалізує концепцію «енергоефективної безпеки» у сучасних IT-інфраструктурах.

Список використаних джерел:

1. Дашко І. М., Крилов Д. В. Енергоефективність: проблеми оцінки та наявний стан / І. М. Дашко, Д. В. Крилов. – «Вісник Хмельницького національного університету», 2021, № 3. - Режим доступу: https://journals.khnu.km.ua/vestnik/wp-content/uploads/2022/03/2021-en-3-17.pdf
2. Як правильно працювати з REST API / Zell Liew. – ITVDN.ua, 15.05.2018. – Режим доступу: https://itvdn.com/ua/blog/article/rest-api-18
3. Scheneider Electric: сучасні дата-центри як запорука сталого розвитку та стабільного майбутнього / Ukrinform, 27.02.2024. – Режим доступу: https://www.ukrinform.ua/rubric-technology/3832821-schneider-electric-sucasni-datacentri-ak-zaporuka-stalogo-rozvitku-ta-stabilnogo-majbutnogo.html
4. Kiselev E. A., Telegin P. N., Shabanov B. M. An energy-efficient scheduling algorithm for shared facility supercomputer centers / E. A. Kiselev, P. N. Telegin, B. M. Shabanov. – arXiv preprint, 2021. – Режим доступу: https://arxiv.org/abs/2111.08978