ЗАСТОСУВАННЯ МЕТОДУ АНР ДЛЯ ВИБОРУ МОДЕЛІ КОНТРОЛЮ ДОСТУПУ В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

[1]Дудля Роман Дмитрович, студент
[2]Маслова Наталія Олександрівна, к.т.н., доц., доц. каф. ШІК
[3]Любименко Олена Миколаївна, к.ф-м.н., доц., доц. каф. ШІК
ДВНЗ «Донецький національний технічний університет»
[1]roman.dudlia.kita@donntu.edu.ua, [2]nataliia.maslova@donntu.edu.ua,
[3]olena.liubymenko@donntu.edu.ua

У сучасних інформаційних системах контроль доступу є одним із базових механізмів забезпечення конфіденційності, цілісності й доступності інформації. Вибір відповідної моделі контролю доступу залежить від призначення системи, рівня критичності інформаційних активів, складності бізнес-процесів, нормативних вимог та можливостей адміністрування.

Метод аналізу ієрархій (Analytic Hierarchy Process, AHP) – це метод підтримки прийняття рішень, який використовується для вибору найкращої альтернативи за наявності кількох критеріїв оцінювання. Метод базується на побудові ієрархічної структури задачі, де на верхньому рівні розташовується мета, на середньому – критерії оцінювання, а на нижньому – можливі альтернативи (рис.1).

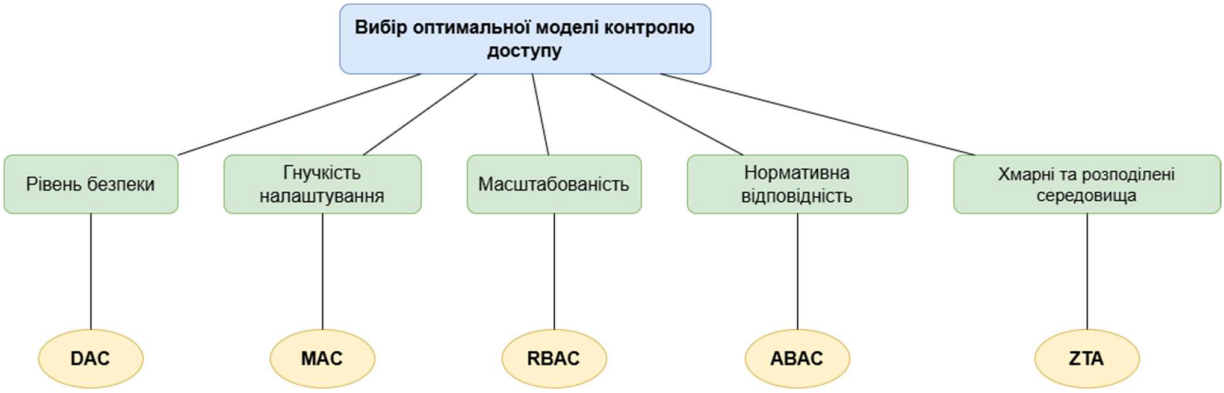

Рисунок 1 – Структура вибору моделі контролю доступу методом АНР

Метою дослідження є вибір оптимальної моделі контролю доступу для інформаційної системи на основі багатокритеріального оцінювання з використанням методу аналізу ієрархій (АНР)/

Критерії оцінювання моделей контролю доступу визначаються особливостями функціонування інформаційної системи та вимогами до забезпечення інформаційної безпеки. Одним із ключових критеріїв є рівень безпеки, який характеризує здатність моделі запобігати несанкціонованому доступу, витоку інформації та порушенню цілісності даних. Важливим критерієм також є гнучкість налаштування, що визначає можливість адаптації моделі до змін бізнес-процесів, політик безпеки та структури організації.

Не менш важливою характеристикою є складність адміністрування, оскільки деякі моделі потребують значних ресурсів для підтримки, керування правами доступу та супроводу політик безпеки. Критерій масштабованості відображає здатність моделі ефективно функціонувати при збільшенні кількості користувачів, ресурсів та інформаційних сервісів.

Окреме значення має відповідність нормативним вимогам, що визначає можливість використання моделі для реалізації вимог міжнародних стандартів і регуляторних актів, таких як ISO/IEC 27001, GDPR, HIPAA або PCI DSS. Крім того, сучасні інформаційні системи потребують оцінювання придатності для хмарних і розподілених середовищ, де контроль доступу повинен враховувати динамічний характер інфраструктури, контекст доступу, багатофакторну автентифікацію та постійний моніторинг активності користувачів.

Для порівняння моделей контролю доступу за основними критеріями оцінювання сформовано таблицю 1.

Таблиця 1 – Порівняння моделей контролю доступу за критеріями оцінювання

Модель	Рівень безпеки	Гнучкість	Масштабованість	Нормативна відповідність	Хмарні середовища
DAC	Низький	Середня	Низька	Часткова	Низька
MAC	Високий	Низька	Середня	Висока	Обмежена
RBAC	Високий	Середня	Висока	Висока	Висока
ABAC	Високий	Висока	Висока	Висока	Висока
ZTA	Дуже високий	Висока	Висока	Висока	Дуже висока

Застосування AHP передбачає попарне порівняння критеріїв і моделей доступу. Наприклад, якщо для організації найважливішими є нормативна відповідність і централізований контроль, вищі пріоритети можуть отримати MAC або RBAC. Якщо система є хмарною, динамічною та потребує врахування контексту доступу, перевагу доцільно надати ABAC або ZTA. Якщо ж система є невеликою і потребує простої реалізації, прийнятним варіантом може бути DAC.

Результати порівняльного оцінювання моделей контролю доступу за основними критеріями наведено на рисунку 2. Значення на рисунку 2 отримані на основі узагальненого експертного оцінювання критеріїв методом AHP.

Моделі DAC та MAC, незважаючи на важливе історичне значення та широке використання у класичних системах захисту інформації, характеризуються меншою гнучкістю та обмеженими можливостями масштабування у динамічних середовищах. Водночас RBAC демонструє компроміс між рівнем безпеки, централізованим адмініструванням та практичною реалізацією в корпоративних інформаційних системах.

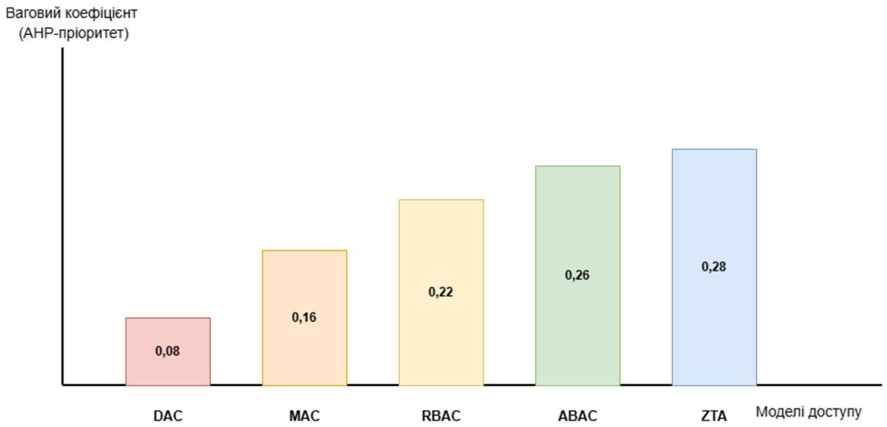

Рисунок 2 – Порівняльна оцінка моделей контролю доступу за методом AHP

Згідно з проведеним аналізом, найбільш високі інтегральні оцінки отримали моделі ABAC та Zero Trust Architecture (ZTA), що пояснюється їх здатністю реалізовувати адаптивний і контекстно-орієнтований контроль доступу в умовах хмарних та розподілених інфраструктур.

Науковою новизною роботи є формалізація процесу вибору моделей контролю доступу на основі багатокритеріального оцінювання із врахуванням сучасних вимог хмарних та розподілених інформаційних систем.

Отримані результати підтверджують доцільність застосування методу аналізу ієрархій для підтримки прийняття рішень у сфері управління інформаційною безпекою, оскільки метод дозволяє формалізувати процес вибору моделі контролю доступу та врахувати як технічні, так і організаційні фактори функціонування інформаційної системи.

ЛІТЕРАТУРА

1. Saaty T. L. Decision Making with the Analytic Hierarchy Process. *International Journal of Services Sciences*. 2008. Vol. 1, No. 1. P. 83–98. DOI: 10.1504/IJSSCI.2008.017590

2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : ISO, 2022.

3. NIST SP 800-207 Zero Trust Architecture. National Institute of Standards and Technology, 2020.

4. Role-Based Access Control Models / R. Sandhu et al. *IEEE Computer*. 1996. Vol. 29, No. 2. P. 38–47. DOI: 10.1109/2.48584.

5. Hu V., Ferraiolo D., Kuhn R. Assessment of Access Control Systems. *NIST Interagency Report 7316*. 2006. DOI: 10.6028/NIST.IR.7316.

6. Любименко О. М., Штепа О. А., Маслова Н. О., Стаценко О. А. Оцінювання якості web-застосунків управління проєктами на IT-ринку з використанням методу аналізу ієрархій // *Науковий вісник Донецького національного технічного університету*. 2026. № 2. С. 99–106/ DOI: 10.31474/2415-7902-2026-2-17-99-106.