DOI: 10.35681/1560-9189.2019.21.4.199370

УДК 004.056.55

**О. Ю. Волинець, Д. В. Куліш, А. В. Приймак, Я. Ю. Яремчук**
Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

# Удосконалення моделі керування доступом на основі ролей у приватних хмарних середовищах

*Розроблено гібридну модель авторизації на основі виразів і RBAC, яка складається з 9 кроків і динамічно дає рішення про доступ до ресурсу чи операції залежно від поточного налаштування, а також проведено порівняння запропонованої моделі з існуючими. Отримані результати показали, що запропонована модель має вищий коефіцієнт правильності надання доступу користувачеві в середньому на 1,5–11,5 %.*

***Ключові слова:*** *захист інформації, приватні хмарні середовища, моделі керування доступом, ролі.*

## Вступ

На даний час усе більшої популярності набувають хмарні технології. Це пов'язано зі стрімким розвитком Інтернету та супутніх технологій. На багатьох підприємствах люди працюють у віддаленому режимі, передаючи всю необхідну інформацію через Інтернет [1]. Хмарні технології надають споживачам рішення, повністю готові до роботи. Достатньо володіти будь-яким пристроєм, здатним з'єднатися з Інтернетом, і можна отримати доступ до віддаленої бази, яка розташовується на віддаленому сервері. Крім того, користувачеві хмарних сервісів не потрібно піклуватися про інфраструктуру, яка забезпечує працездатність сервісів, що надаються йому. Усі завдання з налаштування, усунення несправностей, розширення інфраструктури тощо бере на себе сервіс-провайдер [2].

Наразі існує декілька типів хмар — загальна, публічна, приватна і гібридна, кожна з яких виконує різні завдання та підходить під різні вимоги. Зазвичай організації обирають використання приватної хмари. Приватна хмара може знаходитися у власності, управлінні і експлуатації як самої організації, так і третьої сторони (чи яких-небудь їхніх комбінацій), і вона може фізично існувати як усередині, так і поза юрисдикцією власника [2]. Оскільки в одній такій хмарі може зберігатись інформація одразу декількох підрозділів організації, то питання розмежування доступу та безпеки даних є дуже важливим. Однією з відповідних моделей контролю доступу для хмарних середовищ є рольова модель управління доступом через простоту управління авторизацією.

Модель керування доступом на основі ролей (RBAC — role based access control) — це метод регулювання доступу до комп'ютерних або мережевих ресурсів на основі ролей окремих користувачів у межах підприємства [3]. У цьому контексті доступ є здатністю окремих користувачів виконувати певне завдання, наприклад, переглядати, створювати або змінювати файл. Ролі визначаються відповідно до компетенції, повноважень та відповідальності в межах підприємства. Після належного впровадження, RBAC дозволяє користувачам здійснювати широке коло авторизованих завдань шляхом динамічного регулювання їхніх дій відповідно до гнучких функцій, взаємозв’язків та обмежень [4].

Класична модель процедури авторизації на основі ролей має етапи співвідношення користувача ролям і перевірки чи є у користувача роль, яка має дозвіл на виконання певної операції (рис. 1).


Рис. 1. Схема роботи моделі авторизації RBAC

Слід зазначити, що у приватних хмарних середовищах, зв’язок між ресурсами і користувачами є більш специфічним і динамічним. Постачальники ресурсів для однієї послуги неоднорідні та розподілені в різних областях, тому проблеми контролю доступу у хмарних середовищах значно складніші, ніж у загальних мережевих середовищах і вимагають використовувати деякі нові елементи при застосуванні моделі RBAC.

Використання оригінальної моделі RBAC значно утруднює процес модифікації уже налаштованої хмарної системи, оскільки при створенні ще одного типу користувача, для нього потрібно також генерувати і нову роль, те ж саме відбуває-

ться при необхідності зміни однієї з наявних ролей, тому виникає завдання вирішення таких недоліків, як гнучкість і нескладність модифікацій моделі авторизації.

## Постановка задачі та методика дослідження

Провести аналіз можливості покращення моделі RBAC та розробити модель авторизації, яка буде гнучка в налаштуванні, не буде містити в собі вимог до визначення політики доступу при проектуванні та буде нескладна для модифікацій. Також провести порівняння запропонованої моделі авторизації з існуючими.

## Аналіз можливості покращення моделі авторизації RBAC

На сьогодні відомо багато модифікацій моделі RBAC. Найбільш поширеними та відомими є MT-RBAC, CAACM, GEO-RBAC, SAT-RBAC та ABAC. Для порівняння вищеперерахованих модифікацій доцільно провести аналіз кожної з них.

У своїй роботі Bo Tang, Qi Li та Ravi Sandhu, запропонували сімейство моделей MT-RBAC [5], розширивши модель RBAC, додавши компоненти орендарів (організацій-клієнтів) та емітентів для вирішення питань багаторазового дозволу на спільні хмарні послуги. MT-RBAC має на меті забезпечити тонкодоступний перехресний доступ до ресурсів, будуючи деталізацію довірчих відносин на рівні орендарів. MT-RBAC була спроектована використовуючи бібліотеку XACML SUN для впровадження авторизації як служби (AaaS) у хмарі. Щоб продемонструвати життєздатність прототипної системи, її продуктивність була оцінена та масштабована у хмарі Joyent. Результати показують, що платформа AaaS з MT-RBAC має прийнятні витрати та є масштабованою для служби хмарного зберігання, а коефіцієнт правильності наданого доступу для користувачів лежить у межах 75–92 %.

Результатом спільної роботи Zhenji Zhou, Lifa Wu та Zheng Hong стала запропонована модель управління доступом Context-Aware на основі ARBAC97 для хмарних обчислень (CAACM) [6]. Модель не тільки успадковує переваги ARBAC97, але й захищає конфіденційність та безпеку даних користувачів, додаючи контекст і ролі менеджера. Крім того, вони формально довели безпеку CAACM, щоб гарантувати, що зловмисні інсайдери не зможуть порушити безпеку даних користувачів. При наявності багатьох переваг, у даної моделі присутні і недоліки. Так однією з найбільших проблем є те, як забезпечити цілісність платформи CAACM. Рівень довіри платформи втратить свою надійність, якщо цілісність буде порушена. Експериментальні дослідження показали, що результати правильності роботи моделі знаходяться в межах від 78 % до 96 %.

Іншим прикладом застосування моделі керування доступом на основі ролей у хмарних середовищах є GEO-RBAC [7] — розширення моделі RBAC, що стосується просторової інформації та інформації про місцезнаходження користувача. На відміну від інших геолокаційних моделей контролю доступу, GEO-RBAC побудований на просторовій моделі OGC для моделювання просторових об’єктів, геолокації користувача та географічно обмежених ролей, що робить підхід досить гнучким. У свою чергу, коефіцієнт правильності наданого доступу для користувачів даної моделі лежить у межах 72–94 %.

У роботі Jun Luo, Hongjun Wang, Xun Gong, Tianrui Li пропонується модель SAT-RBAC [8], яка інтегрує безпеку хостів і доступність мережі в традиційну модель RBAC для вирішення складних проблем управління доступом у хмарних середовищах. Те, чи призначена роль користувачеві, у моделі SAT-RBAC, визначається декількома елементами, які включають стан безпеки та доступність мережі для хоста, що використовується користувачем, стан захисту постачальників послуг, пов'язаних з роллю. Результат експериментів у симуляційній системі показує очевидну перевагу моделі SAT-RBAC (90–96 % правильності наданого доступу) над RBAC.

Xin Jin, Ram Krishnan та Ravi Sandhu запропонували модель ABAC [9], яка має достатньо функцій, щоб бути легко та природно налаштовано для роботи з DAC, MAC і RBAC. Вони зазначили, що в їхньому випадку DAC означає списки контролю доступу, контрольовані власником. MAC — це контроль доступу на основі решітки, а RBAC — це рівна та ієрархічна модель RBAC. Їм вдалося налаштувати формальні зв'язки між трьома успішними класичними моделями та бажаними моделями ABAC, у зв'язку з чим, отримані результати коефіцієнта правильності наданого доступу для користувачів мали значення 78–95 %.

Результати порівняння коефіцієнту правильності наданого доступу користувачам різними модифікаціями моделі RBAC представлено в табл. 1.

Таблиця 1. Порівняльна характеристика існуючих модифікацій моделі RBAC

| **Назва моделі** | **Правильність надання доступу, %** |
|---|---|
| MT-RBAC | 75-92 |
| CAACM | 78-96 |
| GEO-RBAC | 72-94 |
| SAT-RBAC | 90-96 |
| ABAC | 78-95 |

Виходячи з аналізу існуючих модифікацій, видно, що правильність надання доступу знаходиться в межах від 72 % до 96 %, крім того, також можна виділити такі недоліки як мала гнучкість налаштування, необхідність попереднього визначення політики доступу та при її модифікації необхідність модифікації самого продукту, а тому залишається актуальним підвищення даного коефіцієнта та розробки відповідної моделі, яка усуне вищеперераховані недоліки.

## Модель керування доступом на основі виразів

Пропонується модель авторизації на основі виразів (умов), яка динамічно дає рішення про доступ до ресурсу чи операції, в залежності від поточного налаштування. Гнучкість досягнута шляхом використання виразів (набору певних умов), які можна змінити під час експлуатації додатку. Вирази можна комбінувати між собою, що дає змогу утворювати будь-які комбінації в залежності від потреб підприємства. Таким чином захист є більш стійким та процес авторизації більш гнучким, і відкритим до модифікації. Кожному користувачу присвоєний

певний набір параметрів, а операції чи ресурсу набір виразів. Під час виконання авторизації, дані користувача використовуються у якості параметрів виразу і при успішному проходженні дозволяють доступ.

Адміністратор підприємства має змогу керувати доступом користувачів, тобто визначати певні умови, при яких користувач матиме доступ до ресурсу чи операції.

Наприклад, користувач матиме змогу завантажувати файл у папку, якщо час його перебування в системі більший ніж один рік, він має найвищий рівень доступу та має змогу завантажити більше десяти файлів. Таким чином, деякі з виразів будуть виконуватися через певний час, і адміністратор матиме змогу задати їх наперед, а не кожен раз оновлювати роль чи інформацію про користувача. Також буде зменшена можливість помилки при налаштуванні, оскільки критеріїв може бути багато, але вони не можуть бути розділеними. Оскільки вирази можуть комбінуватися, то дана модель авторизації є досить гнучкою, щоб задовольнити потреби підприємства.

В адмінпанелі адміністратор матиме змогу додати для користувачів ролі: вибрати якусь з існуючих (рис. 2) чи перейти на вікно створення умов і додати нову (рис. 3).

При переході на вікно «створення умови», користувач матиме змогу вибрати дані для умови чи обрати статичні дані (рис. 3).

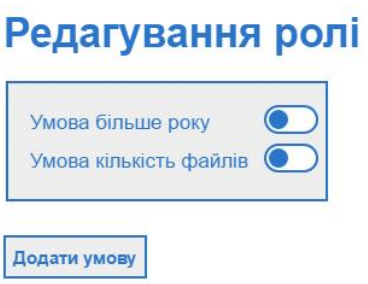


Рис. 2. Робота з існуючими ролями

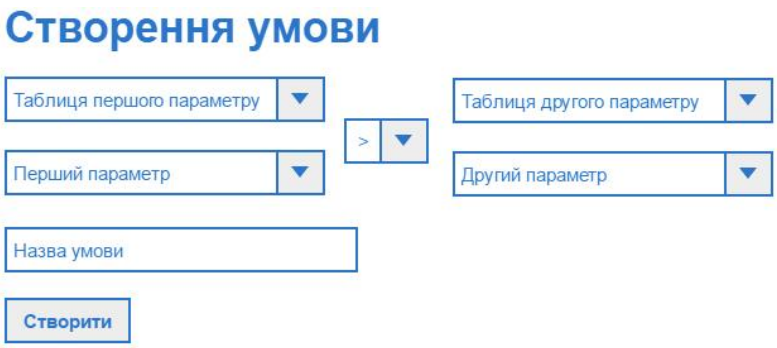


Рис. 3. Вікно створення умови-виразу

До існуючого інтерфейсу хмарного сховища слід додати нові пункти меню, які будуть доступні тільки для адміністратора, такі як Ролі, Умови, Користувачі. Впровадження нових вікон для адміністрування полегшить керування процедурами авторизації.

Запропонована модель авторизації складається з наступних кроків.

1. Початок процедури авторизації користувача в системі.

2. Отримання виразів для певного користувача (попередньо внесеними до системи адміністратором).

3. Перевірка виразу.

4. У разі виконання виразу система перевіряє інші вирази, після чого формується рішення щодо надання доступу.

5. У разі невиконання якогось із виразів, система одразу формує негативне рішення щодо надання доступу користувачу, без подальшої перевірки виразів.

Додаток з використанням моделі авторизації на основі виразів буде повністю захищеним, оскільки при відсутності даних, необхідних для проходження виразу (умови), запит на ресурс чи операцію буде відхилено.

Схема роботи моделі авторизації на основі виразів представлена на рис. 4.

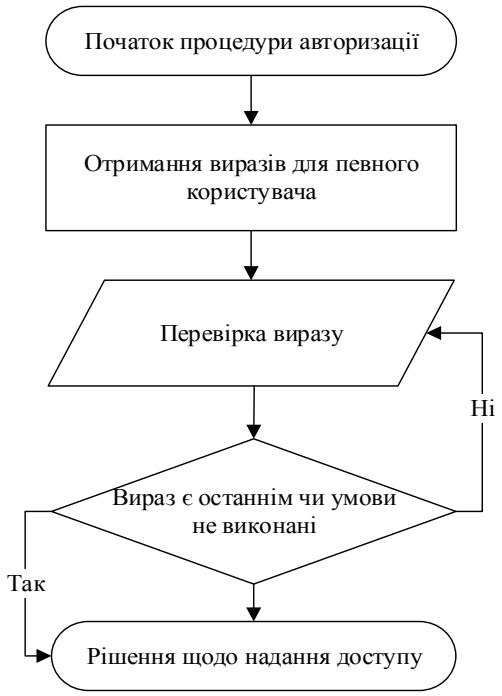


Рис. 4. Схема роботи моделі авторизації на основі виразів

Користувач має перелік умов у вигляді виразів, які він повинен успішно пройти, у разі невиконання умов хоча б одного виразу користувач не отримає доступ до ресурсу чи операції. Якщо кожна з умов буде виконана, користувач матиме змогу виконати операцію. Немає сенсу перевіряти усі вирази, якщо один не виконаний і такою оптимізацією перевірка займатиме менше часу.

Хоча даний підхід і надає необхідний захист та гнучкість, але час на адміністрування можна покращити об’єднавши моделі авторизації на основі виразів з RBAC. Об’єднання з RBAC також надає простоту модифікації під час експлуатації, оскільки для виконання певної операції користувач має мати роль, якій відповідають певні вирази, тобто роль може змінювати своє значення під час роботи додатку, без необхідності зміни програмного коду. З об’єднанням, певний набір виразів можна буде надавати певній ролі або одразу декільком ролям, таким чином буде легше оперувати групами користувачів і одночасно редагувати умови доступу.

На рис. 5 представлено схему роботи моделі авторизації на основі виразів у поєднані з RBAC.


Рис. 5. Схема роботи моделі авторизації на основі виразів із RBAC

Модифіковану модель авторизації можна поєднувати з іншими, не маючи потреби в модифікації бібліотеки. Тобто, іноді буде доцільним поєднати дану перевірку з перевіркою на основі претензій, хоча при правильному налаштуванні виразів даний тип перевірки буде надлишковим.

Експериментальні дослідження запропонованої моделі були проведені у приватній хмарній інфраструктурі з відкритим кодом Joyent. На рис. 6 представлено результати правильності надання доступу запропонованою моделлю для чо-

тирьох різних видів роботи користувача в системі (доступ до файлів, аналіз даних, пошук документів і листування).

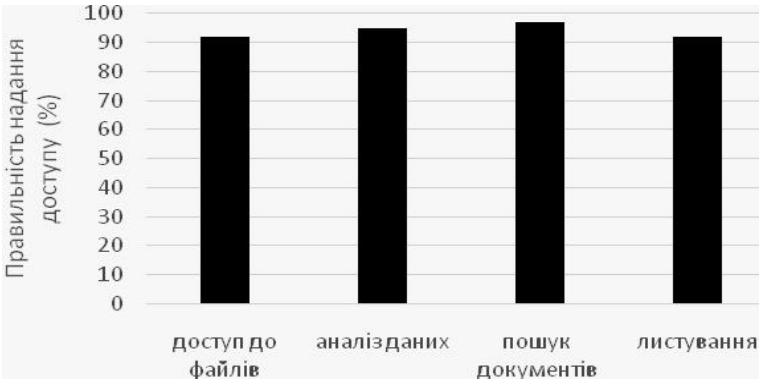


Рис. 6. Результати правильності надання доступу запропонованою моделлю

Як видно з рис. 6, запропонована модель авторизації на основі виразів показала високі результати правильності надання доступу (92–97 %), що показує високу точність і надійність її роботи.

Порівняльну характеристику правильності надання доступу існуючих модифікацій моделі RBAC із запропонованою моделлю керування доступу на основі виразів представлено в табл. 2.

Таблиця 2. Порівняльна характеристика існуючих модифікацій моделі RBAC із запропонованою моделлю

| **Назва моделі** | **Правильність надання доступу, %** |
|---|---|
| MT-RBAC | 75–92 |
| CAACM | 78–96 |
| GEO-RBAC | 72–94 |
| SAT-RBAC | 90–96 |
| ABAC | 78–95 |
| Запропонована модель керування доступу на основі виразів | 92–97 |

Виходячи з результатів, наведених у табл. 2, можна зробити висновок, що запропонована модель керування доступу на основі виразів має вищі показники правильності надання доступу користувачам в приватному хмарному середовищі. Так, запропонована модель показала вищі показники в середньому на 11 % ніж модель MT-RBAC, на 7,5 % вищі ніж CAACM, на 11,5 % вищі ніж GEO-RBAC, а також на 1,5 % та 8 % вищі ніж моделі SAT-RBAC і ABAC відповідно.

## Висновки

Проведено аналіз і порівняння існуючих найбільш поширених і відомих модифікацій моделі RBAC — MT-RBAC, CAACM, GEO-RBAC, SAT-RBAC та ABAC. Детально описані їхні переваги та недоліки, а також складено їхню порів-

няльну характеристику за коефіцієнтом правильності надання доступу користувачеві. Дослідження показало, що існуючі моделі не є ідеальними, а тому підвищення захищеності приватних хмарних середовищ є дійсно актуальним.

Було запропоновано гібридну модель авторизації на основі виразів та RBAC, яка складається з 9 кроків і динамічно дає рішення про доступ до ресурсу чи операції, в залежності від поточного налаштування. Гнучкість була досягнута шляхом використання виразів, які можна змінити під час експлуатації додатку. У свою чергу об'єднання з RBAC додало простоту модифікації при застосуванні додатку, оскільки під час його роботи роль користувача може змінюватись адміністратором без необхідності корегування програмного коду.

Тестування роботи запропонованої моделі проводилось у приватній хмарній інфраструктурі Joyent, дослідження показників правильності надання доступу показало вищі результати порівняно з аналогами у середньому на 1,5–11,5 %, що підтверджує високу точність, надійність її роботи та перевагу над конкурентами.

1. Данилюк І.І., Карпінець В.В., Приймак А.В., Яремчук Ю.Є., Костюченко О.І. Метод ідентифікації користувача за клавіатурним почерком на основі нейромереж. *Реєстрація, зберігання і оброб. даних*. 2018. Т. 20. № 2. С. 68–76. URL: http://nbuv.gov.ua/UJRN/rzod_2018_20_2_10

2. Sedighi A., Jacobson D. Forensic Analysis of Cloud Virtual Environments. 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC). New York, USA. 2019. P. 323–329. URL: https://ieeexplore.ieee.org/abstract/document/8919540

3. Mundbrod N., Reichert M. Object-Specific Role-Based Access Control. *International Journal of Cooperative Information Systems*. 2019. Vol. 28. No 1. URL: http://dbis.eprints.uni-ulm.de/1743/

4. Mitra B., Sural S., Vaidya J., Atluri V. Migrating from RBAC to temporal RBAC. *IET Information Security.* 2017. Vol. 11. No 5. P. 294–300. URL: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2016.0258

5. Tang B., Li Q., Sandhu R. A Multi-Tenant RBAC Model for Collaborative Cloud Services. 2013 Eleventh Annual Conference on Privacy, Security and Trust. IEEE, 2013. P. 229–238. URL: https://www.profsandhu.com/cs6393_s16/Tang-etal-2013b.pdf

6. Zhou Zh., Wu L., HongZh. Context-aware access control model for cloud computing. *International Journal of Grid and Distributed Computing*. 2013. Vol. 6. No 6. P. 1–12. URL: https://pdfs.semanticscholar.org/15fa/ced667554216990aa034a9c6e57928a53ef6.pdf)

7. Damiani M., Bertino E., Catania B. Geo-rbac: A spatially aware RBAC. ACM Transactions on Information and System Security (TISSEC). 2007. Vol. 10. No 1. P. 1–42. URL: https://dl.acm.org/doi/abs/10.1145/1210263.1210265)

8. Luo J., Wang H., Gong X., Li T. A novel role-based access control model in cloud environments. *International Journal of Computational Intelligence Systems*. 2016. Vol. 9. No 1. P. 1–9.

9. Jin X., Krishnan R., Sandhu R. A unified attribute-based access control model covering DAC, MAC and RBAC. IFIP Annual Conference on Data and Applications Security and Privacy. Springer, Berlin, Heidelberg, 2012. P. 41–55. URL: https://link.springer.com/content/pdf/10.1007%2F978-3-642-31540-4_4.pdf

Надійшла до редакції 20.11.2019