УДК 004.056

Палій О.М.

ВИКОРИСТАННЯ ГІБРИДНОЇ МОДЕЛІ РОЗМЕЖУВАННЯ ПРАВ ДОСТУПУ У ЗАСТОСУНКАХ ОБМІНУ КОРПОРАТИВНОЮ ІНФОРМАЦІЄЮ

Анотація

Доповідь аналізує переваги гібридної моделі розмежування прав доступу у сучасних корпоративних застосунках обміну інформацією, зосереджуючись на гнучкості, принципах найменших привілеїв та адаптації до змін. Зазначаються перспективи її розвитку, зокрема інтеграція з іншими технологіями безпеки та використання штучного інтелекту для покращення моніторингу та аналізу безпекових аспектів. Доповідь акцентує на важливості цієї моделі у забезпеченні ефективного та безпечного обміну корпоративною інформацією

Ключові слова: *гібридна модель, розмежування прав доступу, корпоративна інформація, інформаційна безпека, управління доступом, дискреційна модель, рольова модель.*

Abstract

The paper analyses the advantages of a hybrid model of access rights differentiation in modern corporate information exchange applications, focusing on flexibility, least privilege principles and adaptation to changes. The prospects for its development, including integration with other security technologies and the use of artificial intelligence to improve monitoring and analysis of security aspects, are outlined. The report emphasizes the importance of this model in ensuring efficient and secure exchange of corporate information.

Key words: *hybrid model, demarcation of access rights, corporate information, information security, access management, discretionary model, role model.*

Вступ

У сучасному бізнес-середовищі, де безпека та ефективність обміну корпоративною інформацією є визначальними факторами, використання відповідних стратегій управління доступом стає пріоритетним завданням. Мета даної доповіді - полягає в покращенні гнучкості управління розмежуванням прав доступу у застосунках обміну корпоративною інформацією шляхом імплементації гібридної моделі розмежування прав доступу [1]. Задачі включають розгляд основних принципів цієї моделі, дослідження її гнучкості та ефективності, а також визначення перспектив розвитку у контексті забезпечення безпеки даних та моніторингу прав доступу.

Результати дослідження

Гібридна модель розмежування прав доступу є дискреційною системою, яка має риси рольової моделі. Це означає, що не тільки статус користувача визначає доступ до ресурсів [1], але й посада користувача в організації [2]. В основі цієї моделі лежать такі принципи:

– гнучкість у визначенні прав доступу: гібридна модель, які і модель дискреційного розмежування прав доступу зберігає можливість змінювати права доступу відповідно до особливостей кожного користувача та ролі, яку він відіграє в організації. Це враховує особливості кожного працівника та забезпечує гнучкість у управлінні доступом.

– принцип найменших привілеїв: принцип найменших привілеїв використовується в гібридній моделі, що дозволяє користувачеві отримувати тільки права, необхідні для виконання своїх робочих обов'язків. Це зменшує ризики та загрози безпеці.

Проведений аналіз інформаційної діяльності підприємств дозволив виявити, що гібридна модель розмежування прав доступу особливо ефективна та адаптивна в умовах корпоративного середовища:

– адаптація до змін організаційної структури: у сучасному світі компанії часто стикаються зі змінами як у структурі, так і в процесах, які вони виконують. Гібридна модель дозволяє легко адаптуватися до таких змін, не перебудовуючи систему управління [3].

– забезпечення конфіденційності та цілісності даних: гібридна модель дозволяє точно налаштувати права доступу до різних типів даних, що гарантує, що корпоративна інформація зберігається в секреті. Крім того, вона запобігає потенційним порушенням безпеки, виявляючи небажані дії користувачів [4].

Переваги гібридної моделі в майбутньому:

– інтеграція з іншими технологіями безпеки: гібридна модель добре працює з системами моніторингу та двофакторною автентифікацією. Це сприятиме створенню складних систем захисту даних.

– використання штучного інтелекту для аналізу поведінки користувачів: використання гібридної моделі з штучним інтелектом дозволить автоматично реагувати на потенційні загрози безпеці, виявляючи аномальну поведінку користувачів.

Висновок

Гібридна модель розмежування прав доступу є корисним інструментом для забезпечення безпеки даних і оптимізації управління доступом у застосунках обміну корпоративною інформацією. Інтеграція гібридної моделі з використанням штучного інтелекту дозволить покращити моніторинг процесів розмежування прав доступу та дозволить звертати увагу працівників служби управління інформаційної безпеки на аномалії щодо запів доступу у поведінці працівників.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Баришев Ю. В. Дискреційна модель та метод розмежування прав доступу до розподілених інформаційних ресурсів / Ю.В. Баришев, В.А. Каплун, К.В. Неуйміна // Наукові праці ВНТУ, 2017, № 2. – Вінниця, 2017
2. A revised model for role-based access control. Gaithersburg, MD : U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 1998. 20 p.
3. Zarowin P. Estimation of Discretionary Accruals and the Detection of Earnings Management. Oxford University Press, 2015. URL: https://doi.org/10.1093/oxfordhb/9780199935406.013.20 (date of access: 26.11.2023).
4. Pietro R. D., Colantonio A., Ocello A. Role Mining in Business: Taming Role-Based Access Control Administration. World Scientific Publishing Co Pte Ltd, 2011. 274 p.

Палій Олексій Миколайович *– студент групи 2БС-22м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: alexey.paliy1337@gmail.com*

Науковий керівник: ***Баришев Юрій Володимирович*** *– кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет*

Oleksii Palii *- student of group 2BS-22m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail:* alexey.paliy1337@gmail.com

Supervisor: ***Yurii Baryshev*** *— PhD (Eng), Associated Professor of the Department of Information Protection, Faculty of Information Technologies and Computer Engineering. Vinnytsia National Technical University.*