УДК 004.056.52

АНАЛІЗ ПІДХОДІВ ДО РОЗМЕЖУВАННЯ ДОСТУПУ ДО ОБЛАДНАННЯ В ІНФОРМАЦІЙНІЙ СИСТЕМІ МАГАЗИНУ ЛАНДШАФТНОГО ДЕКОРУ

Ткачук Д. В.[1]; Шаріпова І. В.[2]
[1,2] Одеський національний університет імені І. І. Мечникова
[1,2] Україна, Одеса
[1] tkachuk.dariia@stud.onu.edu.ua; [2] iln.sharipova@onu.edu.ua

Анотація. *Розглянуто основні підходи до розмежування доступу до ресурсів інформаційних систем. Порівняно дискреційний, мандатний, рольовий та атрибутивний підходи, визначено їхні переваги й обмеження та можливості застосування в інформаційній системі магазину ландшафтного декору.*
Ключові слова: *розмежування доступу; інформаційна система; RBAC; ABAC; інформаційна безпека.*

Вступна частина. У сучасних умовах використання інформаційних технологій на підприємствах особливого значення набуває питання захисту ресурсів та регулювання прав користувачів. Інформаційні системи забезпечують обробку, зберігання та обмін даними, а також підтримують виконання різноманітних організаційних і виробничих процесів. Водночас використання спільних ресурсів різними категоріями працівників зумовлює необхідність визначення чітких правил доступу до них.

Актуальність проблеми - для підприємств, діяльність яких пов'язана з використанням багатоцільового обладнання: торговельні, складські та адміністративні ресурси, використання яких залежить від посадових обов'язків працівників. Відсутність належного розмежування прав може призвести до несанкціонованого використання обладнання, зміни інформаційної складової або виконання операцій особами, які не мають відповідних повноважень.

Одним із засобів розв'язання цієї проблеми є застосування моделей управління доступом, які визначають умови надання або заборони доступу користувачам до певних ресурсів інформаційної системи.

Мета роботи. Проаналізувати основні моделі розмежування доступу, визначити їхні особливості, переваги й обмеження та оцінити можливості застосування відповідних підходів для організації доступу до обладнання в інформаційній системі магазину ландшафтного декору.

Основна частина. Розмежування доступу є складовою забезпечення інформаційної безпеки, яка передбачає надання або заборону користувачам виконувати певні дії щодо визначених ресурсів. Процес управління доступом пов'язаний з ідентифікацією користувача, його автентифікацією та авторизацією. Ідентифікація дозволяє встановити особу користувача, автентифікація забезпечує перевірку його заявленої особи, а авторизація визначає перелік дозволених операцій [1]. Основними моделями є дискреційна (DAC), мандатна (MAC), рольова (RBAC) та атрибутивна (ABAC) [1].

Дискреційна модель (DAC) дозволяє власнику ресурсу або уповноваженій особі самостійно визначати права користувачів. Вона є гнучкою, однак децентралізоване надання дозволів може ускладнювати загальний контроль [1].

Мандатна модель (MAC) ґрунтується на централізованих правилах і рівнях безпеки. Користувач не може самостійно змінювати призначені права. Такий підхід забезпечує суворіший контроль, але потребує централізованого адміністрування [1].

Рольова модель (RBAC) передбачає призначення дозволів ролям, що відповідають функціональним обов'язкам працівників. Користувач отримує права відповідно до призначеної йому ролі, що спрощує адміністрування доступу [1].

Атрибутивна модель (ABAC) визначає доступ на основі атрибутів користувача, ресурсу, запитуваної дії та умов середовища. Вона дає змогу враховувати додаткові обставини, наприклад, підрозділ працівника або час виконання операції, проте потребує налаштування відповідних політик [1; 2].

Основні відмінності моделей узагальнено в таблиці 1.

Таблиця 1 – Порівняльна характеристика моделей управління доступом

Модель	Основний принцип	Переваги	Обмеження
DAC	Власник ресурсу надає права	Гнучкість, делегування прав	Обмежені можливості централізованого контролю
MAC	Централізовані правила та рівні безпеки	Суворий контроль	Складність адміністрування
RBAC	Права пов'язані з ролями	Централізований розподіл прав через ролі	Необхідність підтримання актуальності ролей
ABAC	Аналіз атрибутів і контексту	Гнучкість, контекстні умови	Складність політик доступу

Важливим принципом під час організації доступу є принцип мінімальних привілеїв, відповідно до якого користувачам надаються лише ті права, які необхідні для виконання службових завдань [3]. Дотримання цього принципу дає змогу зменшити кількість необґрунтовано наданих дозволів та обмежити можливі наслідки помилкових або несанкціонованих дій.

Таким чином, попередній аналіз показує, що для проєктування інформаційної системи магазину ландшафтного декору доцільно розглянути рольову модель як основу розподілу повноважень між працівниками, а атрибутивний підхід – як можливість додаткового врахування умов доступу.

Висновки. Розглянуто основні підходи до розмежування доступу та проаналізовано особливості моделей DAC, MAC, RBAC і ABAC. Визначено, що кожна з них має власні переваги й обмеження, які необхідно враховувати під час вибору механізмів управління доступом.

Встановлено, що рольова модель RBAC дає змогу структурувати повноваження відповідно до функціональних обов'язків працівників, тоді як атрибутивна модель ABAC дає змогу враховувати додаткові характеристики користувачів, ресурсів та умов виконання операцій.

За результатами аналізу визначено доцільність подальшого дослідження можливостей застосування рольового та атрибутивного підходів для організації розмежування доступу до обладнання в інформаційній системі магазину ландшафтного декору.

Використання інструментів ШІ. Дослідження виконано без застосування інструментів ШІ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Aftab, M. U., Hamza, A., Oluwasanmi, A., Nie, X., Sarfraz, M. S., Shehzad, D., Qin, Z., & Rafiq, A. (2022). Traditional and hybrid access control models: A detailed survey. *Security and Communication Networks*, *2022*(1), Article 1560885. https://doi.org/10.1155/2022/1560885

[2] Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2019). *Guide to attribute based access control (ABAC) definition and considerations* (NIST Special Publication 800-162, updated 2019). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-162

[3] Joint Task Force. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Tkachuk D. V., Sharipova I. V.

Analysis of approaches to controlling access to equipment in the information system of a landscape décor store

Abstract. *The main approaches to access control for information system resources are examined. The discretionary, mandatory, role-based, and attribute-based approaches are compared, their advantages and limitations are identified, and their potential applications in the information system of a landscape décor store are considered.*

Keywords: *access control; information system; RBAC; ABAC; information security.*