

## ПІДТРИМКА КОНТРОЛЮ ДОСТУПУ У ПРОГРАМНИХ ПЛАТФОРМАХ ДЛЯ ВОЛОНТЕРІВ

*Д.А. Супрун<sup>1</sup>, М.С. Широкопетлева<sup>2</sup>*

*<sup>1</sup> здобувачка, кафедра програмної інженерії, ХНУРЕ, Харків, Україна*

*<sup>2</sup> старший викладач, кафедра програмної інженерії, ХНУРЕ, Харків, Україна  
[daryna.suprun@nure.ua](mailto:daryna.suprun@nure.ua)*

У сучасних волонтерських платформах, де одночасно взаємодіють тисячі користувачів із різним рівнем відповідальності, питання правильного контролю доступу набуває ключового значення. Такі системи поєднують у собі елементи соціальної взаємодії, управління подіями, збору даних і фінансової звітності, що потребує чіткої організації прав користувачів [1]. Відсутність продуманої ієрархії ролей може призвести до порушень безпеки, несанкціонованого доступу, дублювання функцій або, навпаки, надмірного обмеження можливостей активних учасників.

Волонтерські ініціативи мають динамічну структуру — ролі користувачів часто змінюються залежно від активності, довіри та досвіду. Тому традиційні підходи до розподілу прав доступу, такі як класична рольова модель (RBAC), виявляються недостатньо гнучкими [2]. Необхідна система, що поєднує стабільність ієрархічного управління з адаптивністю до контексту діяльності користувача.

Таким чином, актуальність теми полягає у пошуку моделі контролю доступу, яка враховує специфіку волонтерських платформ — відкритість, колективність та постійне оновлення ролей. Ефективне управління правами користувачів забезпечує не лише інформаційну безпеку, а й підвищує довіру до платформи, покращує координацію дій та спрощує адміністрування [3].

Метою дослідження є створення гібридної моделі контролю доступу, що поєднує структурованість RBAC із гнучкістю атрибутивної моделі доступу (ABAC) і забезпечує збалансоване керування правами, безпеку та адаптивність системи до змінних умов волонтерської діяльності.

Для вивчення сучасних підходів до контролю доступу проаналізовано дві волонтерські платформи, що мають різні організаційні моделі.

Платформа PatronBadge використовує змішану модель, де права користувача залежать не лише від ролі, а й від параметрів активності та репутації [4]. Цей підхід частково реалізує ABAC, що дозволяє більш точно налаштовувати взаємодію з системою. Недоліком є висока складність адміністрування: із зростанням кількості користувачів збільшується кількість атрибутів, які потрібно обробляти.

Платформа GlobalGiving пропонує гнучку систему партнерських ролей, де організації, волонтери й донори мають різні рівні доступу до аналітики, звітності та управління кампаніями [5]. Модель побудована на принципах RBAC, однак розширена контекстними параметрами — наприклад, ролі активуються лише під час участі в певному проекті. Це дозволяє підвищити точність контролю, але потребує складної внутрішньої логіки обробки запитів.

В більшості інших платформ застосовуються класичні моделі контролю доступу, однак RBAC часто є надто статичною, тоді як ABAC — складною для впровадження та підтримки. Узагальнюючи результати аналізу, можна зробити висновок, що жодна з розглянутих платформ не пропонує повністю збалансованої моделі, яка б одночасно забезпечувала ієрархічну структуру, гнучке налаштування прав та врахування контексту взаємодії користувачів. Тому виникає потреба у розробленні гібридної моделі

контролю доступу, яка поєднує структурованість RBAC і динамічність ABAC, з урахуванням специфіки волонтерських платформ. Основна проблема полягає у виборі оптимальної моделі розподілу ролей, здатної враховувати динамічну структуру волонтерських спільнот, різні рівні довіри та контекст взаємодії користувачів.

Пропонується підхід, що базується на поєднанні рольового та атрибутивного підходів, що дозволяє формувати чітку ієрархію доступів, але водночас динамічно адаптувати її до характеристик користувача. На підставі аналізу вимог для програмної системи визначено два рівні ролей - системний і контекстний. Системні ролі визначають загальний рівень прав користувача в межах усїєї платформи, охоплюючи такі статуси, як SuperAdmin, Admin, Moderator, User та Guest. Контекстні ролі застосовуються в межах конкретних організацій, проєктів, подій або завдань. Наприклад, організатор організації має повний контроль над усіма її елементами, тоді як менеджер проєкту відповідає лише за власний проєкт, а волонтер — за виконання своїх завдань. Ієрархія побудована за принципом наслідування, де вищі рівні мають розширений набір прав і впливають на нижчі, що забезпечує логічну послідовність та уникнення дублювання функцій.

Важливим елементом моделі є атрибутивний рівень, який додає гнучкості. Кожен користувач має набір параметрів — досвід, кількість успішних проєктів, відпрацьовані години, рейтинг чи рівень довіри. Ці атрибути визначають можливість розширення його доступу або підвищення ролі. Наприклад, на підставі інформації про досвід та рейтинг можливо автоматичне формування запиту на зміну ролі волонтера та роль менеджера, який може бути відхилено або підтверджено користувачем. Такі запити мають перевірятися як автоматично, так і модераторами, що забезпечує баланс між автономністю процесів і контролем безпеки.

Запропонований підхід було застосовано при реалізації волонтерської платформи. Додатково запроваджений механізм делегування та відкликання ролей. Адміністратор або координатор може тимчасово передавати свої повноваження іншому користувачу без зміни загальної структури прав. Це важливо для волонтерських спільнот, де учасники часто змінюють свої обов'язки або беруть участь у кількох проєктах одночасно.

Отже, запропонована гібридна модель об'єднує чітку ієрархію управління з динамічними політиками доступу, забезпечуючи належний рівень безпеки, масштабованості та зручності адміністрування. Вона формує прозорий механізм контролю, у якому рішення про надання прав базуються не лише на ролі користувача, а й на контексті його взаємодії та рівні довіри. Реалізація двошарової системи — системних і контекстних ролей — сприяє підтриманню балансу між організованістю системи й гнучкістю адаптації до потреб волонтерського середовища, підвищуючи безпеку, прозорість процесів і зручність адміністрування. Запропоноване рішення може слугувати основою для побудови масштабованих волонтерських платформ, що ефективно поєднують організаційний порядок із динамічною природою волонтерської діяльності.

### Список літератури:

1. Sandhu, R., Coyne, E., Feinstein, H., Youman, C. Role-Based Access Control Models / R. Sandhu, E. Coyne, H. Feinstein, C. Youman // IEEE Computer. – 1996. – Т. 29, №2. – DOI: 10.1109/2.485845.
2. Hu, V. C., Kuhn, D. R., Ferraiolo, D. F. Attribute-Based Access Control / V. C. Hu, D. R. Kuhn, D. F. Ferraiolo // NIST Special Publication 800-162. – 2014. – DOI: 10.1109/SP.2015.33
3. Cram, W. A., Brohman, M. K., Gallupe, R. B. Addressing the control challenges of volunteer-based virtual organizations / W. A. Cram, M. K. Brohman, R. B. Gallupe // Information Systems Journal. – 2016. – Т. 26, №3. – DOI: 10.17705/1jais.00427
4. PatronBadge. Lead by Example. Multiply your Impact [Електрон. ресурс]. – Режим доступу: <https://patronbadge.com/> – Назва з титул. екрану.
5. GlobalGiving. Connecting Donors with Grassroots Projects Around the World [Електрон. ресурс]. – Режим доступу: <https://www.globalgiving.org/> – Назва з титул. екрану.