DOI 10.31891/2307-5732-2024-343-6-56
УДК 004.056

ЯМНИЧ АНДРІЙ
Національний університет «Львівська політехніка»
https://orcid.org/0009-0005-7226-1896
e-mail: andrii.b.yamnych@lpnu.ua
КОРОБЕЙНІКОВА ТЕТЯНА
Національний університет «Львівська політехніка»
https://orcid.org/0000-0003-2487-8742
e-mail: tetianakorobeinikova@gmail.com

МОДЕЛЬ КОНТРОЛЮ ДОСТУПУ ПЕРСОНАЛУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВ НА ОСНОВІ RBAC ТА ТЕХНОЛОГІЇ BLOCKCHAIN

У статті досліджується інтеграція контролю доступу на основі ролей (Role-Based Access Control – RBAC) з технологією блокчейн для покращення контролю доступу та інформаційної безпеки на підприємстві. Запропонована модель використовує смарт-контракти, написані в середовищі Solidity, для керування призначенням ролей, правами доступу та журналювання подій. Інтеграція включає такі функції, як делегування ролей, відкликання та нормалізація ієрархії ролей, що забезпечує динамічну та адаптовану структуру контролю доступу. Модель RBAC визначає ролі користувачів, дозволи та обмеження доступу, гарантуючи, що рівень доступу кожного користувача відповідає його визначеним обов'язкам у межах підприємства. Застосування запропонованої моделі у виробничому середовищі на основі блокчейну значно підвищує безпеку та прозорість політик контролю доступу. Незмінний характер технології блокчейн запобігає несанкціонованим змінам записів контролю доступу і гарантує, що всі дії, пов'язані з доступом, можна відстежити та перевірити.

Ключові слова: RBAC, blockchain, кібербезпека, контроль доступу, персонал, модель контролю доступу.

YAMNYCH ANDRII, KOROBEINIKOVA TETIANA
Lviv Polytechnic National University

A MODEL FOR PERSONNEL ACCESS CONTROL TO INFORMATION RESOURCES OF INDUSTRIAL ENTERPRISES BASED ON RBAC AND BLOCKCHAIN TECHNOLOGY

The article investigates the integration of Role-Based Access Control (RBAC) with blockchain technology to enhance access control and information security within an enterprise. The proposed model uses smart contracts written in the Solidity environment to manage role assignments, access rights, and event logging. The integration includes features such as role delegation, revocation, and normalization of the role hierarchy, ensuring a dynamic and adaptable access control structure. The RBAC model defines user roles, permissions, and access constraints, ensuring that each user's access level aligns with their designated responsibilities within the enterprise.

The smart contract was divided into three main parts. The first part established the RBAC initialization and role assignment (where user roles were mapped to addresses), and access rights were defined. Functions like assignRole and setAccessRight allowed administrators to assign roles to users and configure access rights. The second part handled access management and event logging (specific functions like initiateAccess and confirmAccess regulated access to enterprise resources based on predefined roles). These functions checked whether the user's role met the necessary criteria before granting or confirming access, and all actions were logged through events (AccessInitiated and AccessConfirmed).

The third part extended the functionality by introducing delegation, revocation, and normalization. The delegateRole function allowed the temporary transfer of role permissions between users (important for scenarios where a user could not fulfill their duties). The revokeRole function ensured the immediate revocation of roles when they were no longer valid, while maintaining the integrity of the access control system. The normalizeRoles function regulated the establishment of hierarchical relationships between roles, optimizing role management and reducing the storage space required for access policies.

The application of the proposed model within a blockchain-based environment significantly enhances the security and transparency of access control policies. The immutable nature of blockchain technology prevents unauthorized changes to access control records and ensures that all access-related actions are traceable and verifiable.

Keywords: RBAC, blockchain, cybersecurity, access control, personnel, access control model.

Постановка проблеми

У контексті підприємства оцінка персоналу та контроль доступу до інформаційних ресурсів вимагають більш тонкого підходу через складність і масштабність операцій. Співробітники в таких умовах часто взаємодіють із дуже конфіденційними даними, починаючи від власних виробничих технологій і закінчуючи логістикою ланцюга поставок, що робить їх потенційними переносниками інформаційних порушень, якщо вони не контролюються та не оцінюються належним чином. Таким чином, аналіз персоналу повинен враховувати унікальні вимоги виробничих процесів, де доступ до даних у реальному часі, засобів керування обладнанням та інструментів оптимізації процесів може мати прямий вплив як на ефективність, так і на безпеку.

Підприємства оперують людськими ресурсами, і кожен його тип має різні рівні взаємодії з критично важливими інформаційними системами. Оцінка персоналу в цьому середовищі виходить за рамки загальних компетенцій і має враховувати їхню здатність обробляти оперативні дані, адаптуватися до технологічних інтерфейсів і дотримуватися строгих протоколів безпеки. Наприклад, критерії оцінки оператора обладнання будуть суттєво відрізнятися від тих, які застосовуються до IT-фахівця, який керує базою даних підприємства. Проте обидві ролі необхідно досконало перевірити на предмет їх потенційного впливу на цілісність виробничого процесу, особливо коли йдеться про доступ до ключових інформаційних ресурсів.

Розробка критеріїв оцінки персоналу в контексті виробництва вимагає наголосу на технічних

навичках, досвіді роботи з галузевим програмним забезпеченням і розумінні робочих процесів виробництва. Крім того, співробітники повинні продемонструвати здатність обробляти конфіденційні дані, пов'язані зі специфікаціями продукту, угодами з постачальниками та показниками контролю якості. Ці фактори сприяють створенню всебічного профілю кожного працівника, що дозволяє підприємству узгодити їхні права доступу з точним характером їхніх обов'язків. Таке узгодження має вирішальне значення для запобігання несанкціонованому доступу до конфіденційних даних, який може порушити графіки виробництва, погіршити якість продукту або призвести до погіршення конкурентоспроможності.

Аналіз останніх джерел

У науково-дослідницькому просторі сьогодення з'являються роботи, присвячені огляду ризиків інформаційної безпеки для персоналу під час розмежування доступу до інформаційних ресурсів підприємства.

У роботі [1] проаналізовано існуючі підходи та принципи побудови типової інформаційної структури комп'ютерної лабораторії та запропоновано кілька технічних рішень для організації віддаленого доступу до внутрішніх інформаційних ресурсів такої лабораторії. Серед потенційних рішень для розробки інформаційної системи з віддаленим доступом було окреслено три реалізації. У дослідженні аналізуються різні способи організації віддаленого доступу до комп'ютерних лабораторій за допомогою технології переадресації портів, яка може використовуватися для одного або кількох вузлів локальної мережі, включаючи сервери віддаленого робочого столу та веб-сервери з унікальними IP-адресами. Стаття також розглядає основні компоненти системи віддаленого доступу, побудованої на основі VPN, надаючи рекомендації щодо налаштування VPN. Запропонований підхід дозволив реорганізувати комп'ютерну лабораторію та створити нові можливості для студентів і викладачів, особливо під час віддаленої роботи. Загалом, використання VPN на маршрутизаторі MikroTik RB750Gr3 забезпечив надійний та безпечний доступ до ресурсів комп'ютерної лабораторії, представляючи собою гнучке та масштабоване рішення для навчальних закладів, які прагнуть поліпшити дистанційне навчання.

У роботі [2] обговорюється ACS-IoT, смарт-контракт та структура на основі блокчейну, розроблені для децентралізованого контролю доступу в корпоративному середовищі IoT. Відрізняючись від існуючих токенізованих підходів, ACS-IoT інтегрує пристрої IoT з обмеженими ресурсами безпосередньо в блокчейн-мережу, що дозволяє їм отримувати доступ до дозволених ресурсів без централізованого адміністрування чи перевірки з боку керуючих центрів. Використовуючи смарт-контракти та блокчейн Ethereum, розроблений фреймворк автоматизує реалізацію політик контролю доступу, функціонуючи як автономний агент, що виконує попередньо визначене програмування, що підвищує безпеку та ефективність управління доступом у IoT-мережах. Фреймворк ACS-IoT пройшов строгі випробування, включаючи перевірку концепції, і був реалізований у тестовій мережі Ethereum. Експериментальні результати свідчать про те, що інтеграція блокчейну та смарт-контрактів спрощує управління доступом у корпоративних середовищах IoT, пропонуючи безпечне, масштабоване та децентралізоване рішення, яке відповідає специфічним вимогам IoT-мереж. Це підкреслює потенціал блокчейн-технології як надійного механізму управління доступом, що забезпечує більшу прозорість, зменшену залежність від посередників і підвищену безпеку для пристроїв Інтернету речей у корпоративних умовах.

Крім того, варто зазначити праці таких вітчизняних науковців: Бучик С. С. та Мельник С. В. дослідили підходи до оцінки інформаційних ризиків в автоматизованих системах, розробивши методику, що спрямована на мінімізацію ризиків та підвищення рівня захисту даних [3]; Шульга М. Д. дослідив ризики інформаційної безпеки віртуальних середовищ, зокрема, розглянув аспекти захисту в умовах хмарних обчислень та віртуалізованих інфраструктур [4]; Опірський І. дослідив проблеми та виклики, що виникають під час забезпечення кібербезпеки в хмарних обчислювальних системах, приділяючи увагу ключовим загрозам та шляхам їх мінімізації [5]; Дудикевич В. Б., Микитин Г. В. та Ребець А. І. дослідили питання управління безпекою кіберфізичних систем, звертаючи увагу на комплексні підходи до захисту в умовах зростання кіберзагроз [6]; Машталяр Я. Р., Козачок В. А., Бржевська З. М. та Богданов О. М. вивчали інноваційні підходи до забезпечення кібербезпеки на об'єктах критичної інфраструктури, зосереджуючись на новітніх методах захисту таких об'єктів [7].

Серед закордонних вчених ми дослідили такі здобутки: Аарелла С. Г., Моганті С. П., Кугіанос Е. та Путал Д., які запропонували механізм аутентифікації для периферійних центрів обробки даних, що підвищує рівень захисту в спільних обчислювальних середовищах [8]; Бутун І. та Естерберг П. провели огляд систем розподіленого контролю доступу для блокчейн-систем, звернувши увагу на безпеку таких систем у контексті IoT [9]; Круз Ж. П., Каджі Ю. та Янаї Н. дослідили застосування смарт-контрактів для ролеорієнтованого контролю доступу, що дозволяє більш ефективно управляти доступом до ресурсів у блокчейн-середовищах [10]; Хан Д., Чжу Ю., Лі Д., Лян В., Сурі А. та Лі К. С. розробили систему аудиту на основі блокчейну для управління приватними даними, що значно підвищує прозорість і контроль над доступом до даних у середовищах IoT [11]; Лі Ю. та Лі К. М. запропонували модель анонімної автентифікації користувачів на основі блокчейну, що забезпечує безпечну ідентифікацію з використанням ролеорієнтованого контролю доступу [12]; Путал Д., Малик Н., Моганті С. П., Кугіанос Е. та Дас Г. розглянули основні аспекти роботи блокчейну, його компоненти та проблеми, з якими стикаються під час його використання [13]; Альмансорі С., Альзаабі М., Альрейссі М., Путал Д., Дутта Дж. та Шехі А. розробили адаптивний механізм управління доступом на основі машинного навчання для приватного зберігання даних у блокчейні [14]; Красс С., Лакнер А., Бегіч Н., Мірхоссейні С. А. М. та Кірхмайр Н. дослідили спільне адміністрування ролеорієнтованого

контролю доступу за допомогою смарт-контрактів [15]; Дутта Дж., Путал Д. та Даміані Е. дослідили використання штучного інтелекту для ідентифікації та класифікації блоків у блокчейн-інтегрованих середовищах Інтернету речей [16]; Камбодж П., Харе С. та Пал С. дослідили автентифікацію користувачів із використанням смарт-контрактів на основі блокчейну в системах ролеорієнтованого контролю доступу [17]; Ліу Д., Донг А., Янь Б. та Юй Дж. розробили динамічну та детальну систему ролеорієнтованого контролю доступу на основі смарт-контрактів [18]; Свайн С., Путал Д. та Бертіно Е. дослідили використання граф-теоретичних криптографічних методів для захисту блокчейн-систем [19].

Водночас, зважаючи на значний доробок та зазначену наукову документацію, досі питання, що пов'язане з розробкою моделей контролю доступу персоналу до інформаційних ресурсів підприємства є недостатньо дослідженим та потребує подальшого опрацювання [20, 21].

Метою роботи є: розробка моделі контролю доступу персоналу до інформаційних ресурсів підприємства на основі RBAC та технології Blockchain.

Виклад основного матеріалу

З методологічної точки зору, процеси оцінювання на реальному виробництві мають перевагу, оскільки є доступ до передових аналітичних інструментів, таких як прогнозне моделювання та аналітика поведінки. Такі інструменти дозволяють виявляти аномалії в шаблонах доступу, які можуть вказувати на потенційні порушення безпеки або неефективність. Наприклад, доступ працівника до систем управління виробництвом у неробочий час або спроба отримати дані, не пов'язані з його роллю, може означати або загрозу безпеці, або необхідність подальшого дослідження його обов'язків. Такий підхід дозволяє підприємствам передбачати ризики та реагувати на них до того, як вони переростуть у більш серйозні інциденти.

Диференціація доступу повинна бути тісно пов'язана з ієрархічною структурою організації. Наприклад, операторам може знадобитися доступ до інтерфейсів обладнання та налаштувань процесу, тоді як менеджерам може бути необхідний доступ до аналітики виробництва і інформації про запаси. Запровадження контролю доступу на основі ролей, що відображає цю ієрархію, дозволяє організаціям забезпечити, щоб лише уповноважені співробітники мали доступ до важливих систем і даних. Ця диференціація стає особливо важливою в умовах впровадження сучасних виробничих технологій, таких як Інтернет речей і автоматизація, коли збільшується кількість точок доступу та підвищується ризик несанкціонованих дій.

Зв'язок між процесами оцінювання персоналу та диференціацією доступу на виробництві полягає в обмеженні доступу та оптимізації ефективності роботи під час збереження безпеки. Цей баланс досягається завдяки постійному аналізу профілів співробітників, що дозволяє коригувати дозволи на доступ відповідно до змін у ролях, навичках та вимогах організації. Наприклад, якщо технік отримує додатковий досвід і демонструє надійність, його доступ до складніших налаштувань обладнання або аналітичних інструментів може бути розширений, і це збільшить його внесок у покращення процесів без загрози для безпеки.

У цьому контексті контроль доступу на основі ролей (відомою технологією RBAC [22, 23]) може бути ефективно інтегрований із блокчейн-технологією для покращення управління доступом і безпеки в організації. Поєднання RBAC з блокчейном пропонує децентралізований, прозорий і захищений метод контролю доступу. У системі RBAC, що базується на блокчейні, дозволи на доступ зберігаються в розподіленій книзі, що гарантує незмінний запис усіх змін у правах доступу. Цей підхід забезпечує чіткий облік того, кому було надано доступ, коли і ким були внесені зміни, і це підвищує підзвітність та зменшує ризик несанкціонованих змін. Оскільки блокчейн по своїй природі запобігає підробці даних, він гарантує, що політики контролю доступу не можуть бути змінені без відповідної авторизації, і це робить процес управління доступом більш безпечним.

Процес інтеграції передбачає кодування політик RBAC у смарт-контракти, які є самовиконуваними угодами з попередньо визначеними правилами, записаними в код. Ці смарт-контракти автоматично забезпечують виконання правил контролю доступу, надаючи або скасовуючи дозволи на основі ролей, посад або поточних завдань працівника на підприємстві. Наприклад, якщо роль працівника змінюється або він отримує додаткові обов'язки, смарт-контракт може налаштувати його права доступу в режимі реального часу, не вимагаючи ручного втручання. Цей рівень автоматизації підвищує ефективність і зменшує ризик людської помилки.

Використовуючи блокчейн, RBAC також може сприяти безпечній співпраці між відділами або навіть організаціями в межах мережі постачання. Кожна організація може мати власний набір правил доступу, записаних у блокчейні, гарантуючи, що лише авторизований персонал кожного відділу чи партнерської організації може отримати доступ до певних даних або ресурсів. Це особливо важливо на виробництві, де існує потреба передавати конфіденційну інформацію (технології виробництва, дані про контроль якості, рівень запасів тощо) зовнішнім партнерам, і це вимагає суворого контролю доступу для запобігання витоку даних або промисловому шпигунству.

Основною функцією RBAC є визначення та керування дозволами доступу на основі ролей користувачів в організації. У поєднанні з блокчейном, така система використовує незмінну та децентралізовану природу блокчейну з метою створення прозорого та захищеного від втручання середовища, де всі дії контролю доступу постійно записуються. Кожному співробітнику призначаються певні ролі з попередньо визначеними рівнями доступу до інформаційних ресурсів, гарантуючи, що лише авторизований персонал може виконувати дії, які відповідають їхнім обов'язкам.

У запропонованій комбінованій моделі RBAC-блокчейн смарт-контракти діють як автоматизовані контролери, які забезпечують виконання політик RBAC і водночас не вимагають ручного втручання. Ці смарт-контракти визначають правила для дозволів доступу, і це унеможливлює неавторизованим особам змінити або обійти ці елементи керування без виявлення. Таке автоматизування гарантує, що доступ узгоджений із політикою організації, і при цьому цілісність системи є збереженою. Втілення запропонованої моделі реалізована мовою програмування Solidity. Solidity – це мовою програмування для розробки смарт-контрактів на Ethereum і використовується для написання, тестування та розгортання смарт-контрактів RBAC.

Конфігурація ролей в запропонованій моделі RBAC базується на блокчейні і передбачає створення та призначення пар ключів для ідентифікації та підтвердження особи користувача («ключ»-«особа»). На рисунку 1 наведено діаграму комбінованої моделі RBAC-блокчейн.

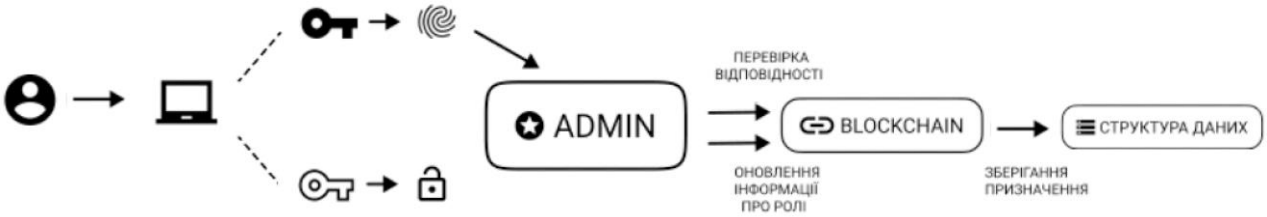

Рис. 1. Діаграма комбінованої моделі RBAC-блокчейн

Кожен користувач генерує пару ключів (закритий і відкритий) на локальному пристрої, де закритий ключ підтверджує доступ, а відкритий ключ використовується для ідентифікації в системі блокчейн. Після генерації ключів користувач відправляє свій відкритий ключ разом із запитом на відповідну роль адміністратору даних. Адміністратор перевіряє відповідність користувача до запитуваної ролі, гарантуючи, що це призначення відповідає принципу розмежування обов'язків (SoD), який зберігається в блокчейні. Після успішної перевірки інформація про ролі користувача оновлюється в блокчейні, і це призначення зберігається у структурі даних відображення, де відкритий ключ слугує ключем, а масив призначених ролей виступає значенням. На рисунку 2 наведено фрагмент програмної реалізації алгоритму ініціалізації RBAC та призначення ролей.

RBAC реалізується завдяки явному порівнянню адрес користувачів із ролями та визначенню прав доступу для кожної ролі. Функція assignRole дозволяє адміністратору призначати користувачам ролі, наприклад «менеджер» або «співробітник», гарантуючи, що рівень доступу кожного користувача відповідає його обов'язкам. Функція setAccessRight дозволяє адміністратору вказати, чи має роль необхідні дозволи для доступу до певних ресурсів, таким чином гарантуючи, що політику доступу можна налаштувати відповідно до змінних вимог підприємства.

На рисунку 3 наведено фрагмент програмної реалізації взаємодії процесу керування доступом та журналу подій.

```
contract EnterpriseRBACControl {
    address public admin;
    mapping(address => string) public roles; // Mapping user addresses to their roles
    mapping(string => bool) public accessRights; // Defining access rights per role

    uint256 public resourceID;
    uint256 public accessTimestamp;
    bool public accessConfirmed;

    constructor(uint256 _resourceID) {
        admin = msg.sender;
        resourceID = _resourceID;
        accessConfirmed = false;
    }

    modifier onlyAdmin() {
        require(msg.sender == admin, "Access restricted to admin only");
        _;
    }

    modifier roleCheck(string memory role) {
        require(keccak256(bytes(roles[msg.sender])) == keccak256(bytes(role)),
"Access restricted based on role");
        _;
    }

    function assignRole(address _user, string memory _role) public onlyAdmin {
        roles[_user] = _role;
        emit RoleAssigned(_user, _role);
    }

    function setAccessRight(string memory role, bool hasAccess) public onlyAdmin {
        accessRights[role] = hasAccess;
        emit AccessRightsUpdated(role, hasAccess);
    }
```

Рис. 2. Ініціалізація RBAC та присвоювання ролей

```
function initiateAccess() public roleCheck("manager") {
        require(accessConfirmed == false, "Access already initiated");
        require(accessRights["manager"] == true, "Manager does not have access rights");

        accessTimestamp = block.timestamp;
        accessConfirmed = true;

        emit AccessInitiated(msg.sender, resourceID);
    }

    function confirmAccess() public roleCheck("employee") {
        require(accessConfirmed == true, "Access not yet initiated");
        require(block.timestamp >= accessTimestamp,
"Cannot confirm access before initiation");
        require(accessRights["employee"] == true,
"Employee does not have access rights");

        emit AccessConfirmed(msg.sender, resourceID);
    }

    event RoleAssigned(address indexed user, string role);
    event AccessRightsUpdated(string role, bool accessGranted);
    event AccessInitiated(address indexed user, uint256 resourceID);
    event AccessConfirmed(address indexed user, uint256 resourceID);
}
```

Рис. 3. Керування доступом та журнал подій

Наприклад, лише користувач, якому надано роль «менеджер», може ініціювати доступ до ресурсу, викликавши функцію initiateAccess, і лише користувач із роллю «співробітник» може підтвердити доступ через функцію confirmAccess за умови, що права доступу для його ролі були надані. Ці функції захищені модифікатором roleCheck, гарантуючи, що користувачі можуть виконувати дії, лише якщо їхня роль відповідає необхідному рівню повноважень.

На рисунку 4 наведено фрагмент програмної реалізації управління ролями в моделі. Тут передбачено функції делегування, відкликання та нормалізація ієрархії ролей. Це гарантує, що політики контролю доступу залишаються динамічними та адаптованими. Функція делегування дозволяє користувачу тимчасово передавати частину своїх ролей іншому користувачу. Функція відкликання працює таким чином, що користувачі не можуть утримувати призначені ролі безстроково, оскільки автоматичне відкликання відбувається після завершення визначеного терміну (тайм-ауту). Функція нормалізації ієрархії ролей підвищує ефективність управління ролями завдяки ієрархічній структурі ролей на основі призначень і дозволів, і це полегшує адміністрування і водночас зменшує необхідний обсяг пам'яті для політик контролю доступу.

```
    struct Delegation {
        address delegator;
        address delegatee;
        string role;
        uint256 expirationTime;
    }


    mapping(address => Delegation) public delegations;
    mapping(address => uint256) public roleValidUntil;

    function delegateRole(address _delegatee, string memory _role,
uint256 _duration) public roleCheck(_role) {
        require(_duration > 0, "Invalid duration");
        delegations[_delegatee] =
Delegation(msg.sender, _delegatee, _role, block.timestamp + _duration);
        emit RoleDelegated(msg.sender, _delegatee, _role, block.timestamp + _duration);
    }

    function revokeRole(address _user) public onlyAdmin {
        require(bytes(roles[_user]).length != 0, "No role assigned");
        emit RoleRevoked(_user, roles[_user]);
        delete roles[_user];
        delete roleValidUntil[_user];
    }

    function normalizeRoles(address _parent, address _child) public onlyAdmin {
        emit RoleHierarchyNormalized(_parent, roles[_parent], _child, roles[_child]);
    }

    event RoleDelegated(address indexed delegator, address indexed delegatee, string role,
    event RoleRevoked(address indexed user, string role);
    event RoleHierarchyNormalized(address indexed parent, string parentRole,
address indexed child, string childRole);
}
```

Рис. 4. Управління ролями у запропонованій моделі

Функція delegateRole дозволяє користувачеві тимчасово передати свою роль іншому користувачеві, при цьому ця дія реєструється через подію RoleDelegated. Функція revokeRole дозволяє адміністратору відкликати роль користувача, гарантуючи, що ролі, термін дії яких закінчився, не зберігаються. Функція normalizeRoles визначає ієрархічні зв’язки між ролями, а подія RoleHierarchyNormalized забезпечує прозорість цих змін. Ці вдосконалення забезпечують динамічне керування ролями, зберігаючи безпечний, незмінний контроль доступу в межах блокчейну.

Висновки

Загалом, інтеграція технології блокчейн з RBAC забезпечує високий рівень безпеки і водночас запобігає несанкціонованому доступу. Також забезпечує прозорість і можливість перевірки. Кожен запит на доступ, запит на призначення ролі чи зміну політики логуються і це унеможливлює підміну політики контролю доступу або втручання в логи для зловмисників. Запропонований рівень безпеки є особливо корисним у закладах, установах та підприємствах, де цілісність інформації є вирішальним фактором, оскільки він забезпечує стійкий до втручання механізм для керування доступом до корпоративних ресурсів. Комбінована RBAC-блокчейн модель спроможна обробляти динамічні зміни щодо призначення ролей і дозволів, і такий підхід робить її гнучким і масштабованим рішенням для підприємств, які прагнуть покращити свої методи захисту інформації.

У загальному підсумку в цій науковій статті відображена ідея інтеграції RBAC із технологією блокчейн. Це дає надійну та адаптовану структуру для керування доступом до інформаційних ресурсів підприємства. Запропонована комбінована RBAC-блокчейн модель гарантує суворе дотримання дозволів доступу відповідно до попередньо визначених ролей та забезпечує прозорість і незмінність, що властиві технології блокчейн. Комбінована RBAC-блокчейн модель значно знижує ризики, пов'язані з несанкціонованим доступом, фальсифікацією даних і зміною політики, що робить її важливим рішенням для сучасних підприємств, які прагнуть підтримувати цілісність і конфіденційність своїх інформаційних ресурсів.

Література

1. Могильний Г. (2024). Впровадження системи віддаленого доступу до інформаційних ресурсів комп'ютерних лабораторій. https://journals.snu.edu.ua/index.php/VisnikSNU/article/download/412/409

2. Rashid, A., Masood, A., & Khan, A. U. R. (2024). ACS-IoT: Smart contract and blockchain assisted framework for access control systems in IoT enterprise environment. *Wireless Personal Communications*, 1–22. https://doi.org/10.1007/s11277-024-11266-1

3. Бучик, С. С., & Мельник, С. В. (2015). Методика оцінювання інформаційних ризиків в автоматизованій системі. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*, (11), 33–43.

4. Шульга, М. Д. (2023). Оцінювання ризиків інформаційної безпеки віртуальної інфраструктури.

5. Опірський, І. (2023). Дослідження та аналіз проблем та викликів, що виникають у забезпеченні кібербезпеки в хмарних обчисленнях. *Ukrainian Information Security Research Journal*, 26(1), 76–88.

6. Дудикевич, В. Б., Микитин, Г. В., & Ребець, А. І. (2018). До проблеми управління комплексною системою безпеки кіберфізичних систем. *Вісник Національного університету "Львівська політехніка". Серія: Інформаційні системи та мережі*, (901), 10–21.

7. Машталяр, Я. Р., Козачок, В. А., Бржевська, З. М., & Богданов, О. М. (2023). Дослідження розвитку та інновацій кіберзахисту на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, (2(22)), 156–167.

8. Aarella, S. G., Mohanty, S. P., Kougianos, E., & Puthal, D. (2023). Fortified-edge: Secure PUF certificate authentication mechanism for edge data centers in collaborative edge computing. *Proceedings of the Great Lakes Symposium on VLSI 2023*, 249–254.

9. Butun, I., & Österberg, P. (2021). A review of distributed access control for blockchain systems towards securing the Internet of Things. *IEEE Access*, 5428–5441. https://doi.org/10.1109/ACCESS.2020.3047902

10. Cruz, J. P., Kaji, Y., & Yanai, N. (2018). RBAC-SC: Role-based access control using smart contract. *IEEE Access*, 12240–12251. https://doi.org/10.1109/ACCESS.2018.2812844

11. Han, D., Zhu, Y., Li, D., Liang, W., Souri, A., & Li, K. C. (2022). A blockchain-based auditable access control system for private data in service-centric IoT environments. *IEEE Transactions on Industrial Informatics*, 3530–3540. https://doi.org/10.1109/TII.2021.3114621

12. Lee, Y., & Lee, K. M. (2019). Blockchain-based RBAC for user authentication with anonymity. *Proceedings of the Conference on Research in Adaptive and Convergent Systems*, ACM. https://doi.org/10.1145/3338840.3355673

13. Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine*, 6–14. https://doi.org/10.1109/MCE.2018.2816299

14. Almansoori, S., Alzaabi, M., Alrayssi, M., Puthal, D., Dutta, J., & Shehhi, A. (2023). Machine learning-based adaptive access control mechanism for private blockchain storage. *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*. https://doi.org/10.1109/COMPSAC57700.2023.00188

15. Craß, S., Lackner, A., Begic, N., Mirhosseini, S. A. M., & Kirchmayr, N. (2022). Collaborative administration of role-based access control in smart contracts. *2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 87–94. https://doi.org/10.1109/BRAINS55737.2022.9909116

16. Dutta, J., Puthal, D., & Damiani, E. (2022). AI-based block identification and classification in the blockchain integrated IoT. *2022 OITS International Conference on Information Technology (OCIT)*, 415–421. https://doi.org/10.1109/OCIT56763.2022.00084

17. Kamboj, P., Khare, S., & Pal, S. (2021). User authentication using blockchain-based smart contract in role-based access control. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-021-01150-1

18. Liu, D., Dong, A., Yan, B., & Yu, J. (2021). DF-RBAC: Dynamic and fine-grained role-based access control scheme with smart contract. *Procedia Computer Science*, 359–364. https://doi.org/10.1016/j.procs.2021.04.074

19. Swain, S., Puthal, D., & Bertino, E. (2021). CryptoCliqIn: Graph-theoretic cryptography using clique injection. *IEEE Intelligent Systems*, 59–65.

20. Коробейнікова, Т. І., Ямнич, А. Б. (2023). Оцінка ризиків інформаційної безпеки для персоналу. *International periodical scientific journal «SWorldJournal»*, 20(1), 43–51. https://doi.org/10.30888/2663-5712.2023-20-01-024

21. Коробейнікова, Т. І., Ямнич, А. Б. (2023). Огляд питання оцінки ризиків інформаційної безпеки для персоналу. *International scientific integration 2023: Міжнародна наукова конференція, 11 липня 2023 р.: тези доповідей*, Сіетл, США: ProConference, 18–25. https://doi.org/10.30888/2709-2267.2023-19-01-008

22. Трояновська, Т. І., Захарченко, С. М., & Бойко, О. В. (2017). Побудова захищених мереж на базі обладнання компанії Cisco. Вінниця: ВНТУ.

23. Коробейнікова, Т. І., Захарченко, С. М. (2021). Технології захисту локальних мереж на основі обладнання CISCO: навч. посібник. Львів: Видавництво Львівської політехніки.

References

1. Mohylnyi, H. (2024). Vprovadzhennia systemy viddalenoho dostupu do informatsiinykh resursiv kompiuternykh laboratorii https://journals.snu.edu.ua/index.php/VisnikSNU/article/download/412/409.

2. Rashid, A., Masood, A., & Khan, A. U. R. (2024). ACS-IoT: Smart contract and blockchain assisted framework for access control systems in IoT enterprise environment. *Wireless Personal Communications*, 1–22. https://doi.org/10.1007/s11277-024-11266-1

3. Buchyk, S. S., & Melnyk, S. V. (2015). Metodyka otsiniuvannia informatsiinykh ryzykiv v avtomatyzovanii systemi [Methodology for assessing information risks in an automated system]. *Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system*, (11), 33–43.

4. Shulha, M. D. (2023). Otsiniuvannia ryzykiv informatsiinoi bezpeky virtualnoi infrastruktury [Risk assessment of information security in virtual infrastructure].

5. Opirskyi, I. (2023). Doslidzhennia ta analiz problem ta vyklykiv, shcho vynykaiut u zabezpechenni kiberbezpeky v khmarnykh obchyslenniakh [Research and analysis of challenges in ensuring cybersecurity in cloud computing]. *Ukrainian Information Security Research Journal*, 26(1), 76–88.

6. Dudykevych, V. B., Mykytyn, H. V., & Rebets, A. I. (2018). Do problemy upravlinnia kompleksnoiu systemoiu bezpeky kiberfizychnykh system [On the problem of managing a complex security system of cyber-physical systems]. *Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Seriia: Informatsiini systemy ta merezhi*, (901), 10–21.

7. Mashtaliar, Ya. R., Kozachok, V. A., Brzhevska, Z. M., & Bohdanov, O. M. (2023). Doslidzhennia rozvytku ta innovatsii kiberzakhystu na ob'iektakh krytychnoi infrastruktury [Research on the development and innovation of cybersecurity at critical infrastructure facilities]. *Kiberbezpeka: osvita, nauka, tekhnika*, (2(22)), 156–167.

8. Aarella, S. G., Mohanty, S. P., Kougianos, E., & Puthal, D. (2023). Fortified-edge: Secure PUF certificate authentication mechanism for edge data centers in collaborative edge computing. *Proceedings of the Great Lakes Symposium on VLSI 2023*, 249–254.

9. Butun, I., & Österberg, P. (2021). A review of distributed access control for blockchain systems towards securing the Internet of Things. *IEEE Access*, 5428–5441. https://doi.org/10.1109/ACCESS.2020.3047902

10. Cruz, J. P., Kaji, Y., & Yanai, N. (2018). RBAC-SC: Role-based access control using smart contract. *IEEE Access*, 12240–12251. https://doi.org/10.1109/ACCESS.2018.2812844

11. Han, D., Zhu, Y., Li, D., Liang, W., Souri, A., & Li, K. C. (2022). A blockchain-based auditable access control system for private data in service-centric IoT environments. *IEEE Transactions on Industrial Informatics*, 3530–3540. https://doi.org/10.1109/TII.2021.3114621

12. Lee, Y., & Lee, K. M. (2019). Blockchain-based RBAC for user authentication with anonymity. *Proceedings of the Conference on Research in Adaptive and Convergent Systems*, ACM. https://doi.org/10.1145/3338840.3355673

13. Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine*, 6–14. https://doi.org/10.1109/MCE.2018.2816299

14. Almansoori, S., Alzaabi, M., Alrayssi, M., Puthal, D., Dutta, J., & Shehhi, A. (2023). Machine learning-based adaptive access control mechanism for private blockchain storage. *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*. https://doi.org/10.1109/COMPSAC57700.2023.00188

15. Craß, S., Lackner, A., Begic, N., Mirhosseini, S. A. M., & Kirchmayr, N. (2022). Collaborative administration of role-based access control in smart contracts. *2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 87–94. https://doi.org/10.1109/BRAINS55737.2022.9909116

16. Dutta, J., Puthal, D., & Damiani, E. (2022). AI-based block identification and classification in the blockchain integrated IoT. *2022 OITS International Conference on Information Technology (OCIT)*, 415–421. https://doi.org/10.1109/OCIT56763.2022.00084

17. Kamboj, P., Khare, S., & Pal, S. (2021). User authentication using blockchain-based smart contract in role-based access control. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-021-01150-1

18. Liu, D., Dong, A., Yan, B., & Yu, J. (2021). DF-RBAC: Dynamic and fine-grained role-based access control scheme with smart contract. *Procedia Computer Science*, 359–364. https://doi.org/10.1016/j.procs.2021.04.074

19. Swain, S., Puthal, D., & Bertino, E. (2021). CryptoCliqIn: Graph-theoretic cryptography using clique injection. *IEEE Intelligent Systems*, 59–65.

20. Korobeinykova, T. I., & Yamnych, A. B. (2023). Otsinka ryzykiv informatsiinoi bezpeky dlia personalu [Risk assessment of information security for personnel]. *International Periodical Scientific Journal "SWorldJournal"*, 20(1), 43–51. https://doi.org/10.30888/2663-5712.2023-20-01-024

21. Korobeinykova, T. I., & Yamnych, A. B. (2023). Ohliad pytannia otsinky ryzykiv informatsiinoi bezpeky dlia personalu [Review of information security risk assessment for personnel]. *International Scientific Integration 2023: Proceedings of the International Scientific Conference*, Seattle, USA: ProConference, 18–25. https://doi.org/10.30888/2709-2267.2023-19-01-008

22. Troianovska, T. I., Zakharchenko, S. M., & Boiko, O. V. (2017). Pobudova zakhyshchenykh merezh na bazi obladnannia kompanii Cisco [Building secure networks based on Cisco equipment]. Vinnitsa: VNTU.

23. Korobeinykova, T. I., & Zakharchenko, S. M. (2021). Tekhnolohii zakhystu lokalnykh merezh na osnovi obladnannia Cisco [Technologies for protecting local networks based on Cisco equipment]. Lviv: Vydavnytstvo Lvivskoi politekhniky.