УДК 004.056.5

А. В. Грицак

М. В. Римаренко

Використання штучного інтелекту та технології блокчейн для підвищення безпеки системи управління доступом

Вінницький національний технічний університет

Анотація. *У даній роботі досліджуються перспективи використання штучного інтелекту та блокчейн-технологій для підвищення ефективності систем контролю та управління доступом. Проаналізовано сучасні підходи до впровадження методів машинного навчання та нейронних мереж у процеси ідентифікації, автентифікації та моніторингу доступу, а також розглянуто інтеграцію блокчейну для забезпечення прозорості та незмінності даних. Визначено основні переваги застосування штучного інтелекту для адаптивного контролю доступу, виявлення аномальної поведінки та зниження ризиків несанкціонованого проникнення, тоді як блокчейн сприяє децентралізованому зберіганню інформації та автоматизації процесів за допомогою смарт-контрактів. Виокремлено основні виклики впровадження інтелектуальних технологій та блокчейну у системи безпеки, а також окреслено перспективи їх подальшого розвитку з метою створення надійних і стійких до зовнішніх загроз систем управління доступом.*

Ключові слова: контроль доступу, управління доступом, штучний інтелект, аналіз поведінки, інформаційна безпека, виявлення аномалій, кіберзагрози, блокчейн, смарт-контракт.

Abstract*. This paper explores the prospects of using artificial intelligence and blockchain technologies to enhance the efficiency of access control and management systems. Modern approaches to implementing machine learning methods and neural networks in identification, authentication, and access monitoring processes are analyzed, along with the integration of blockchain to ensure data transparency and immutability. The key advantages of applying artificial intelligence for adaptive access control, anomaly detection, and reducing the risks of unauthorized intrusion are identified, while blockchain facilitates decentralized data storage and process automation through smart contracts. The main challenges of integrating intelligent technologies and blockchain into security systems are highlighted, and the prospects for their further development are outlined to create reliable and resilient access management systems capable of withstanding external threats.*

Keywords: access control, access management, artificial intelligence, behavioural analysis, information security, anomaly detection, cyber threats, blockchain, smart contracts.

Вступ

У наш час, коли зростання кіберзагроз вимагає підвищення рівня безпеки, традиційні системи контролю та управління доступом потребують вдосконалення. Штучний інтелект відкриває нові можливості для автоматичного аналізу поведінки користувачів, виявлення аномалій і гнучкого управління доступом. Важливо оцінити переваги впровадження інтелектуальних алгоритмів у системи безпеки, а також визначити основні виклики та перспективи їх розвитку.

Результати дослідження

Система контролю і управління доступом - сукупність програмно-апаратних технічних засобів безпеки, призначених для обмеження та реєстрації входу- виходу об'єктів (людей, транспорту) на об'єкті. Системи контролю доступу та управління доступом (СКУД) дають можливість забезпечити безпеку підприємства шляхом обмеження доступу в різні зони об'єкта або на весь об'єкт в цілому. Основне завдання СКУД - управління доступом на задану територію, включаючи так само обмеження доступу на задану територію ідентифікація особи, яка має доступ на задану територію. На об'єктах СКУД виконується фізично незв'язаної з іншими інформаційними мережами, а також може інтегруватися в чинні системи [1].

На сьогодні системи контролю та управління доступом (СКУД) є ефективним інструментом забезпечення безпеки, оскільки більшість сучасних пристроїв виконують покладені на них функції з високою точністю. Однак суттєвим недоліком таких систем є їхня статичність, що обмежує можливість адаптації до змінних умов експлуатації та виникнення аномальних ситуацій.

Більшість традиційних СКУД розроблені для виконання фіксованого набору функцій і не здатні самостійно аналізувати нові загрози або реагувати на нетипову поведінку користувачів. Відсутність гнучкості та адаптивності таких систем створює ризики для інформаційної безпеки, особливо в умовах зростаючої складності кібератак та розширення спектра потенційних загроз. Це зумовлює необхідність розробки інтелектуальних підходів до контролю доступу, здатних до самонавчання та динамічної зміни параметрів відповідно до поточної ситуації.

Автоматизація процесів мінімізує людський фактор: системи можуть самостійно ухвалювати рішення щодо доступу, інтегруватися з іншими системами безпеки та адаптувати рівні доступу в реальному часі. Крім того, аналітика на базі ШІ надає керівництву цінну інформацію про переміщення персоналу й загальний стан безпеки об'єкта.

Особливо важливим є те, що такі системи здатні протистояти сучасним загрозам, включно з кібератаками та електромагнітними впливами, застосовуючи адаптивні методи захисту. У підсумку, інтеграція ШІ в СКУД створює більш розумні, стійкі й ефективні рішення для захисту критичних об'єктів.

У 2024 році кількість підприємств, що використовують біометричні технології контролю доступу, зросла з 30% до 39%. Основними чинниками цього зростання є зручність і точність безконтактних рішень, зокрема розпізнавання облич, сканування відбитків пальців, долоні та райдужної оболонки ока. Близько 23% опитаних вважають, що біометрія суттєво вплине на розвиток галузі, а дві з п'яти організацій уже застосовують мобільні пристрої для безконтактного доступу. Інтеграція штучного інтелекту є ще одним ключовим трендом – 38% компаній зацікавлені у його впровадженні. ШІ підвищує безпеку, дозволяючи системам аналізувати поведінкові моделі та ухвалювати рішення в реальному часі. Також розвиваються рішення з інтеграції розпізнавання облич із відеоспостереженням, що дає змогу відстежувати переміщення персоналу та обмежувати доступ неавторизованих осіб. Дедалі популярнішими стають мобільні платформи, які використовують ШІ для безпечного управління доступом без потреби в картках чи ключах [2].

Штучний інтелект (ШІ) активно впроваджується в системи контролю доступу, підвищуючи їхню точність, ефективність та безпеку. Одним із ключових застосувань є розпізнавання облич, що дозволяє ідентифікувати особу без використання фізичних носіїв (карток, ключів).

Основні переваги ШІ у контролі доступу:

– точність та безпека, алгоритми ШІ швидко аналізують біометричні дані, запобігаючи спуфінгу та знижуючи кількість помилкових спрацьовувань;

– автоматизація, ШІ може керувати реєстрацією користувачів, налаштуванням рівнів доступу та виявленням аномальної поведінки;

– швидкість реагування, системи аналізують великі обсяги даних у реальному часі, оперативно повідомляючи про загрози;

– інтеграція, поєднання з відеоспостереженням та системами виявлення вторгнень покращує комплексну безпеку.

Проблеми та виклики:

– конфіденційність. Використання біометричних даних потребує суворих заходів захисту та відповідності законодавству;

– упередженість алгоритмів. Навчання на нерепрезентативних даних може призводити до дискримінаційних результатів, що вимагає регулярного тестування та коригування;

– прозорість та етичність. Організації повинні інформувати користувачів про збір даних та надавати можливість відмови [3].

У сфері комерції провідні китайські компанії, такі як Alibaba та Jingdong, впровадили системи електронних платежів на основі розпізнавання облич. Ці системи пов'язують біометричні дані клієнтів з їхніми банківськими рахунками, забезпечуючи швидкі та безпечні транзакції без необхідності використання фізичних карток або готівки.

Крім того, технологічна компанія Baidu співпрацює з China Southern Airlines для впровадження розпізнавання облич в аеропорту Наньян Цзяньїн у провінції Хенань. Ця технологія використовується для автоматизації процесу посадки на літак, що прискорює процедури та знижує навантаження на персонал аеропорту [4].

Однією з головних проблем безпеки Інтернету речей є відсутність стандартизації пристроїв. Багато пристроїв IoT виробляються різними компаніями та працюють на різних операційних системах, що ускладнює реалізацію єдиних протоколів та процесів безпеки. Технологія блокчейн пропонує вирішення цієї проблеми, надаючи загальну платформу для роботи всіх пристроїв IoT.

Використовуючи технологію блокчейн, IoT-пристроям можна надати унікальні цифрові ідентифікатори, які зберігаються в блокчейні. Ці ідентифікатори можна використовувати для аутентифікації пристроїв і забезпечення підключення до мережі лише санкціонованим пристроям. Це допомагає запобігти зловмисному доступу та гарантує, що всі пристрої в мережі є надійними.

Ще одна перевага використання технології блокчейн для безпеки IoT полягає в тому, що вона може допомогти запобігти фальсифікації даних. Незмінний характер записів блокчейну означає, що будь-яка спроба змінити дані буде негайно виявлена та позначена як шахрайська. Це значно ускладнює хакерам маніпулювання даними або впровадження шкідливих програм у систему.

Одним із прикладів того, як технологію блокчейн можна використовувати для захисту

пристроїв Інтернету речей, є сфера розумних будинків. Розумні будинки стають дедалі популярнішими, коли власники будинків використовують підключені пристрої для керування всім – від освітлення до опалення та кондиціонування повітря. Однак ці пристрої часто вразливі до кібератак, що створює для власників будинків ризик викрадення особистої інформації або злому будинків [5].

Інтеграція блокчейну в СКУД дозволяє підвищити рівень безпеки та захисту даних. Блокчейн-технології мають значний потенціал для вдосконалення процесів зберігання та обробки даних, зокрема у державних цифрових системах, що оперують персональною інформацією. Однією з ключових переваг блокчейну є його децентралізована природа, яка усуває єдину точку відмови, характерну для централізованих систем, та мінімізує ризики компрометації даних. Інформація розподіляється між вузлами мережі, а будь-яка зміна вимагає консенсусу більшості учасників, що забезпечує цілісність даних і запобігає несанкціонованим модифікаціям.

Незмінність блокчейну гарантує, що кожна транзакція фіксується у незмінному реєстрі, створюючи прозорий механізм контролю за всіма діями з інформацією. Смарт-контракти автоматизують управління доступом до персональних даних, знижуючи вплив людського фактору та підвищуючи точність виконання процесів, таких як надання або відкликання згоди на обробку даних. Ці механізми сприяють дотриманню вимог Загального регламенту про захист даних (GDPR), оскільки забезпечують прозорість операцій та гарантують контроль користувача над власною інформацією.

Додаткову безпеку забезпечує використання децентралізованих файлових систем, зокрема InterPlanetary File System (IPFS), що дозволяють зберігати великі обсяги даних у розподіленому середовищі. IPFS застосовує механізм хешування для збереження цілісності інформації та захисту від модифікацій, створюючи надійний інструмент для забезпечення доступності та безпеки даних.

Методи обробки даних, такі як маскування, псевдоанонімізація та тасування, у поєднанні з блокчейном дозволяють зберігати корисність даних для аналітики, водночас знижуючи ризик розкриття конфіденційної інформації. З огляду на особливості зберігання, доцільним є застосування комбінованого підходу: on-chain для важливих даних, що вимагають максимальної цілісності, та off-chain для великих масивів інформації із збереженням у блокчейні лише їхніх криптографічних хешів.

Оптимальним рішенням для державних цифрових платформ є впровадження гібридної моделі блокчейну, що поєднує переваги відкритих та приватних мереж. Такий підхід забезпечує прозорість у відстеженні доступу до даних при одночасному захисті персональної інформації від несанкціонованого розголошення. Інтеграція блокчейну, смарт-контрактів та IPFS створює комплексний механізм, що відповідає міжнародним стандартам безпеки, підвищує рівень довіри користувачів до цифрових сервісів та сприяє мінімізації ризиків, пов’язаних із порушенням конфіденційності даних [6].

Таким чином, інтеграція блокчейну в системи контролю доступу є перспективним напрямком, що дозволяє підвищити безпеку, ефективність та гнучкість таких рішень.

Висновки

Інтеграція штучного інтелекту та блокчейн-технологій у системи контролю та управління доступом (СКУД) створює передумови для підвищення рівня безпеки, адаптивності та прозорості таких систем. Штучний інтелект забезпечує швидке ухвалення рішень у реальному часі, автоматизацію процесів і виявлення аномальної поведінки, тоді як блокчейн гарантує незмінність та надійність даних про доступ, мінімізуючи ризики зовнішнього втручання. Поєднання цих технологій сприяє створенню динамічних, самонавчальних систем, здатних оперативно реагувати на нові загрози та забезпечувати високий рівень захисту критичної інфраструктури в умовах постійних кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ТЗІ.UA – СКУД - інформаційна безпека та захист інформації [Електронний ресурс]. Режим доступу: https://tzi.ua/ua/skud.html (дата звернення: 19.03.2025).
2. GreenVision – Технологічні тренди в контролі фізичного доступу: розвиток біометрії, штучного інтелекту та мобільних рішень [Електронний ресурс]. Режим доступу: https://greenvision.ua (дата звернення: 20.03.2025).
3. PC-Security – The Rise of AI in Access Control: What You Need to Know [Електронний ресурс]. Режим доступу: https://fpc-security.com/blogs/articles/artificial-intelligence-ai-in-access-control#:~:text=One%20key%20use%20of%20AI,physical%20keys%20or%20key%20cards (дата звернення: 18.03.2025).
4. Главком – Китай змінює підходи до технології розпізнавання облич. Якою буде ідентифікація [Електронний ресурс]. Режим доступу: https://glavcom.ua/techno/hitech/kitaj-zminjuje-pidkhodi-do-tekhnolohiji-rozpiznavannja-oblich-jakoju-bude-inditifikatsija (дата звернення: 18.03.2025).
5. H-X Technology – Як захистити Інтернет речей за допомогою Blockchain [Електронний ресурс]. Режим доступу: https://www.h-x.technology/ua/blog-ua/how-secure-internet-of-things-with-blockchain-ua (дата звернення: 19.03.2025).
6. CSecurity – Концепція застосування блокчейн-технологій для підвищення захищеності персональних даних платформи «Дія»: відповідність вимогам GDPR та українському законодавству [Електронний ресурс]. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/681/564 (дата звернення: 20.03.2025).

Римаренко Микола Вікторович – студент групи УБ-21б, факультет менеджменту і інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: craaaashbaaashl@gmail.com

Науковий керівник: Грицак Анатолій Васильович – доцент каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: grytsak.a.v@gmail.com

Rymarenko Mykola V. – student of the UB-21b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: craaaashbaaashl@gmail.com

Supervisor: Hrytsak Anatolii Vasyliovych – docent of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: grytsak.a.v@gmail.com