МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

НАЦІОНАЛЬНА АКАДЕМІЯ ПРАВОВИХ НАУК УКРАЇНИ

Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів

Тези доповідей
Всеукраїнської науково-практичної конференції
(м. Вінниця, 21 червня 2024 року)

Вінниця 2024

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ПОЛІЦІЇ. СТВОРЕННЯ ЗАСОБІВ ТА КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. КІБЕРБЕЗПЕКА

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ПОЛІЦІЇ. СТВОРЕННЯ ЗАСОБІВ ТА КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. КІБЕРБЕЗПЕКА

Валерія Сергіївна БАЛАЦЬКА,
аспірантка кафедри захисту інформації
Національного університету «Львівська політехніка»;
ORCID: https://orcid.org/0000-0002-6262-6792;
Іван Романович ОПІРСЬКИЙ,
завідувач кафедри захисту інформації
Національного університету «Львівська Політехніка»,
доктор технічних наук, професор;
ORCID: https://orcid.org/0000-0002-8461-8996

ПІДВИЩЕННЯ БЕЗПЕКИ ДЕРЖАВНИХ РЕЄСТРІВ УКРАЇНИ ЗА ДОПОМОГОЮ ТРЬОХФАКТОРНОЇ АУТЕНТИФІКАЦІЇ НА ОСНОВІ БЛОКЧЕЙН

У сучасному світі безпека даних є однією з найважливіших проблем, з якими стикаються державні установи. Особливо це стосується державних реєстрів, які містять критично важливу інформацію про громадян, власність, правові документи та інші важливі дані. Будь-яка несанкціонована зміна чи доступ до цих даних може призвести до серйозних наслідків, таких як шахрайство, крадіжка особистих даних або компрометація державних процесів.

Традиційні методи аутентифікації, такі як паролі або однофакторні рішення, стають все менш ефективними у боротьбі з сучасними загрозами. Тому все більше уваги приділяється багатофакторній аутентифікації, яка використовує кілька рівнів захисту для перевірки особи користувача. Трьохфакторна аутентифікація (3FA), яка включає комбінацію знань (пароль), володіння (смарт-карта або мобільний телефон) та біометричних даних (відбитки пальців, розпізнавання обличчя), є одним із найефективніших методів захисту.

Блокчейн-технологія, яка спочатку з'явилася як основа для криптовалют, таких як Bitcoin, все частіше розглядається як інноваційне рішення для забезпечення безпеки даних. Її основні характеристики – децентралізованість, незмінність записів та прозорість – роблять її ідеальним кандидатом для інтеграції з трьохфакторною аутентифікацією.

Для оцінки доцільності впровадження трьохфакторної аутентифікації на основі блокчейн в державних реєстрах України важливо

розглянути як переваги, так і потенційні недоліки такого рішення. Нижче представлена таблиця 1 з порівнянням основних переваг та недоліків, що дає змогу оцінити всі аспекти впровадження даної технології.

З одного боку, блокчейн-технології забезпечують високий рівень безпеки завдяки децентралізованій структурі, незмінності записів та можливості аудиту. Вони також дозволяють автоматизувати процеси управління доступом через смарт-контракти, що може значно підвищити ефективність і надійність системи. Особливу увагу слід звернути на захист біометричних даних, які можуть бути збережені у вигляді хешів, що забезпечує їх конфіденційність.

З іншого боку, впровадження блокчейн-рішень вимагає значних фінансових та технічних ресурсів. Це пов'язано з високими початковими витратами на розробку та інтеграцію, а також з необхідністю залучення висококваліфікованих фахівців. Крім того, блокчейн-системи можуть стикатися з проблемами продуктивності та масштабованості, особливо при обробці великої кількості транзакцій. Не менш важливими є правові та регуляторні питання, які можуть потребувати додаткових зусиль для адаптації законодавства до нових технологій.

Таким чином, таблиця нижче дає змогу детально розглянути всі переваги та недоліки трьохфакторної аутентифікації на основі блокчейн, що є необхідним для прийняття обґрунтованого рішення щодо її впровадження у державних реєстрах України.

Таблиця 1

Переваги та недоліки трьохфакторної аутентифікації на основі блокчейн для державних реєстрів України

№	Переваги	Недоліки
1.	Високий рівень безпеки. Використання трьох незалежних факторів значно знижує ризик несанкціонованого доступу до даних.	Впровадження блокчейн-технологій вимагає значних фінансових ресурсів для розробки, впровадження та підтримки.
2.	Дані, збережені в блокчейн, не можуть бути змінені або видалені, що забезпечує їх цілісність і достовірність.	Розробка та підтримка системи вимагають високого рівня технічної експертизи і кваліфікованих фахівців.
3.	Усі дії аутентифікації записуються в блокчейн, що забезпечує прозорість і можливість проведення повного аудиту.	Блокчейн-системи можуть бути повільнішими і менш масштабованими порівняно з традиційними базами даних.

4.	Відсутність центрального органу знижує ризик компрометації даних у разі атаки на один із вузлів системи.	Впровадження нових технологій може зустріти опір з боку користувачів і організацій, звиклих до традиційних методів.
5.	Смарт-контракти дозволяють автоматизувати управління доступом і виконання умов аутентифікації, що підвищує ефективність системи.	Використання блокчейн-технологій може вимагати змін у правовому та регуляторному полі, що потребує додаткового часу та ресурсів.
6.	Зберігання біометричних даних у вигляді хешів у блокчейн забезпечує їх конфіденційність та захист від зловживань.	Ефективна робота системи залежить від надійної мережевої інфраструктури та доступності вузлів блокчейн-мережі.

Для впровадження трьохфакторної аутентифікації на основі блокчейн у державних реєстрах України потрібно розглянути широкий спектр аспектів. Одним із головних переваг такого підходу є високий рівень безпеки, що забезпечується децентралізованою структурою, незмінністю записів та можливістю автоматизації через смарт-контракти. Крім того, блокчейн дозволяє ефективно захищати біометричні дані, зберігаючи їх у вигляді хешів і забезпечуючи конфіденційність.

З іншого боку, впровадження таких технологій вимагає значних витрат на розробку і інтеграцію, а також компетентних фахівців для підтримки системи. Існують також проблеми з продуктивністю і масштабованістю блокчейн-систем, які потребують вирішення перед їхнім впровадженням. Правові та регуляторні аспекти також є важливими, оскільки вони вимагають адаптації законодавства до нових технологій та забезпечення відповідності з існуючими нормативними вимогами.

Крім того, важливо враховувати інтеграцію з існуючими інформаційними системами, організаційні аспекти впровадження, участь громадськості та міжнародний досвід. Ці аспекти доповнюють технічні та фінансові вимоги і відображають складність процесу впровадження нових технологій у державних структурах.

Отже, вирішення всіх цих викликів та оптимізація процесів є ключовим для успішного впровадження трьохфакторної аутентифікації на основі блокчейн у державних реєстрах України. Такий підхід дозволить забезпечити високий рівень захисту даних і забезпечити

ефективне функціонування системи, враховуючи інтереси користувачів та вимоги сучасного інформаційного середовища.

В даній роботі було проаналізовано переваги та виклики впровадження трьохфакторної аутентифікації на основі блокчейн у державних реєстрах України. Дослідження показало, що блокчейн-технології мають значний потенціал для підвищення рівня безпеки та надійності систем управління даними, завдяки їхній децентралізованій природі, незмінності записів і можливості автоматизації через смарт-контракти. Особлива увага приділялася захисту біометричних даних, що є критично важливими для запобігання шахрайства та недозволеним доступам.

Інтеграція нових технологій з існуючими інформаційними системами, участь громадськості та використання міжнародного досвіду є важливими складовими для успішного впровадження блокчейн-рішень у державному секторі України. Врахування всіх цих аспектів дозволить максимізувати переваги нових технологій і забезпечити стійкий і безпечний розвиток державних інформаційних систем у майбутньому.

Список бібліографічних посилань

1. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2019). Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services.

2. Opirskyy I., Balatska V., Poberezhnyk V. Modern possibilities of use blockchain technology in the education system// Ukrainian Scientific Journal of Information Security, 2023, vol. 29, issue 3, pp. 138-146. DOI: https://doi.org/10.18372/2225-5036.29.18073

3. Балацька, В., Опірський, І. (2023). Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 4(20), 6–19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619

Одержано 18.06.2024