ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННОГО УРЯДУВАННЯ / E-GOVERNANCE SECURITY

DOI: 10.18372/2225-5036.30.19211

БЛОКЧЕЙН ЯК ІНСТРУМЕНТ ПРОЗОРОСТІ ТА ЗАХИСТУ ДЕРЖАВНИХ РЕЄСТРІВ

Валерія Балацька, Іван Опірський

Національний університет «Львівська політехніка»

БАЛАЦЬКА Валерія Сергіївна, аспірант
Рік та місце народження: 1996 рік, м. Луцьк, Волинська обл., Україна.
Освіта: Львівський державний університет безпеки життєдіяльності, 2019.
Посада: аспірант кафедри захисту інформації, з 2022 року.
Наукові інтереси: комп'ютерні мережі, операційні системи, захист інформації, комплексні системи захисту інформації, захист персональних даних.
Публікації: більше 25 публікацій серед яких наукові статті, тези та матеріали доповідей на конференціях.
E-mail: valeriia.s.balatska@lpnu.ua.
Orcid ID: 0000-0002-6262-6792.

ОПІРСЬКИЙ Іван Романович, д.т.н., проф.
Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: завідувач кафедри захисту інформації з 2023 рок.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання.
Публікації: більше 120 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

Анотація. *З розвитком цифрових технологій і зростанням вимог до забезпечення прозорості та безпеки даних, державні реєстраційні системи стикаються з низкою викликів, що пов'язані із централізованою архітектурою. Традиційні централізовані системи, що використовуються для зберігання та обробки даних, мають низку проблем, серед яких вразливість до кібератак, ненадійність захисту персональних даних, відсутність контролю користувачів над їхньою інформацією та недотримання міжнародних стандартів, таких як Загальний регламент про захист даних (GDPR). Це породжує потребу у впровадженні нових технологічних рішень, які могли б усунути ці недоліки та забезпечити підвищену надійність державних реєстрів. У цьому дослідженні пропонується впровадження блокчейн-технологій у державні реєстраційні системи як рішення, здатне підвищити безпеку, прозорість і надійність даних, а також надати користувачам більший контроль над своїми персональними даними. Блокчейн дозволяє створювати децентралізовані системи, в яких дані не можуть бути змінені без відповідної аутентифікації та реєстрації всіх транзакцій, що знижує ризики несанкціонованого доступу та шахрайства. Одним із ключових елементів дослідження є розробка математичної моделі для кількісної оцінки ефективності впровадження блокчейн-рішень у державні реєстраційні системи. Модель оцінює показники безпеки, прозорості, надійності та швидкості обробки даних, що дозволяє провести порівняння з традиційними централізованими системами. Аналіз показує, що блокчейн може значно зменшити корупційні ризики, забезпечити повну прозорість державних процесів і покращити рівень довіри громадян до державних установ. Окрім цього, впровадження блокчейн відповідає міжнародним стандартам з безпеки та захисту даних, таким як GDPR, що робить цю технологію перспективною для державного управління. У дослідженні також окреслено ключові напрямки розвитку технології блокчейн, включаючи підвищення масштабованості системи, оптимізацію витрат на обробку даних та інтеграцію з іншими технологіями для державного управління. Отримані результати демонструють значний потенціал блокчейн-рішень для трансформації державних реєстрів, а розроблена модель може бути використана як інструмент для подальших досліджень і впровадження технології в державні установи.*

Ключові слова. *блокчейн, державні реєстри, персональні дані, прозорість, безпека, децентралізація, GDPR, математична модель, управління даними, цифрова трансформація.*

Постановка проблеми

Зростання обсягів цифрових даних і поширення інформаційно-комунікаційних технологій привело до необхідності створення більш ефективних і безпечних механізмів управління інформацією в державному секторі. Державні реєстраційні системи, що зберігають важливі персональні та правові дані громадян, стикаються з численними викликами, пов'язаними з централізацією, вразливістю до кібератак, недостатнім рівнем прозорості та контролю за доступом до даних.

Традиційні централізовані реєстраційні системи, хоч і забезпечують зручний доступ до інформації, мають обмеження у сфері забезпечення надійності, прозорості та відповідності вимогам міжнародних стандартів, зокрема Загального регламенту захисту даних (GDPR) [1]. Однією з перспективних технологій, здатних вирішити ці проблеми, є блокчейн, що забезпечує децентралізоване, незмінне та прозоре зберігання даних. Блокчейн як розподілена система дозволяє зберігати дані в зашифрованому вигляді та відслідковувати всі транзакції, пов’язані з доступом або зміною інформації. Це знижує ймовірність несанкціонованих втручань, а також дозволяє громадянам контролювати, хто і як використовує їхні персональні дані.

Впровадження блокчейн-технологій у державні реєстраційні системи може сприяти підвищенню рівня довіри між громадянами та державою, знизити корупційні ризики, а також забезпечити більшу відповідність міжнародним нормам щодо захисту даних. Однак для повноцінного використання потенціалу блокчейн необхідно проводити ґрунтовний аналіз існуючих систем та розробляти нові моделі оцінки ефективності впровадження цих технологій у державне управління [2].

Метою цього дослідження є оцінка перспектив впровадження блокчейн-рішень у державні реєстраційні системи та розробка математичної моделі для кількісної оцінки їхньої ефективності. У рамках дослідження проводиться порівняння блокчейн-технологій із традиційними централізованими системами, зокрема з точки зору надійності, безпеки, прозорості та швидкості обробки даних. Окрему увагу приділено аналізу ключових переваг і недоліків блокчейн-рішень, а також напрямків їх розвитку в державному управлінні.

Це дослідження також має на меті продемонструвати важливість розробки інноваційних рішень для забезпечення безпеки та прозорості державних процесів, що є особливо актуальним в умовах цифрової трансформації та зростання вимог до захисту даних.

Аналіз останніх досліджень і публікацій

Останні дослідження зосереджуються на використанні блокчейн-технологій для підвищення безпеки та прозорості в управлінні даними. Значна увага приділяється їх потенціалу в контексті державних реєстраційних систем, зокрема питанням децентралізації, прозорості, захисту від несанкціонованого доступу, а також відповідності міжнародним стандартам, як-от GDPR.

Одним з ключових напрямків досліджень є забезпечення безпеки та незмінності даних у розподілених системах. Зокрема, дослідники відзначають, що блокчейн дозволяє створювати незмінні записи, що захищають інформацію від зовнішніх загроз та несанкціонованих змін, роблячи його привабливим рішенням для державних реєстрів. Блокчейн-технологія значно покращує безпеку Інтернету речей (IoT) [3], що можна застосувати й у контексті державних реєстрів, для захисту персональних даних громадян. Інші дослідження зосереджені на ролі блокчейн у підвищенні прозорості та довіри в державних реєстраційних системах. Впровадження блокчейн може суттєво знизити корупційні ризики завдяки незмінності даних та можливості відслідковувати всі транзакції. Також виявлено, що завдяки децентралізованій природі блокчейн можна забезпечити вищий рівень контролю з боку громадян над їхніми персональними даними. Деякі публікації також торкаються питання зниження корупції в процесах державного управління за допомогою блокчейн-рішень, досліджують можливості застосування блокчейн в технологіях єдиного входу (SSO) [4], що може бути використано для підвищення безпеки аутентифікації у державних інформаційних системах. Незважаючи на очевидні переваги, дослідники відзначають і певні обмеження блокчейн. Серед ключових недоліків відзначають високу вартість впровадження, складність масштабування систем, а також повільну швидкість обробки даних у порівнянні з централізованими системами. Крім того, деякі роботи вказують на проблеми з регуляторним середовищем, оскільки впровадження блокчейн-рішень потребує значних змін у правовій базі та нормативних актах [5].

Таким чином, аналіз публікацій свідчить, що блокчейн має значний потенціал для вирішення проблем безпеки, прозорості та контролю за персональними даними в державних реєстраційних системах. Однак для його успішного впровадження необхідно подолати технічні та правові бар'єри, а також розробити ефективні моделі оцінки його ефективності.

Мета та постановка завдання

Метою цього дослідження є розробка та обґрунтування ефективних рішень для впровадження блокчейн-технологій у державні реєстраційні системи з метою підвищення їхньої прозорості, безпеки та надійності. Особлива увага приділяється оцінці можливостей блокчейн щодо забезпечення децентралізації, незмінності даних та дотримання вимог міжнародних стандартів, таких як GDPR.

Основні завдання дослідження:

1. Провести аналіз сучасних централізованих державних реєстраційних систем для виявлення їхніх основних недоліків, таких як вразливість до кібератак, відсутність контролю користувачів над персональними даними, та низька прозорість процесів;

2. Оцінити переваги та недоліки блокчейн-технологій у контексті їхнього використання в державних реєстрах, зокрема щодо прозорості, безпеки та відповідності міжнародним стандартам, таким як GDPR;

3. Розробити математичну модель для кількісної оцінки ефективності впровадження блокчейн-рішень у державні реєстраційні системи, враховуючи показники надійності, швидкості обробки даних, безпеки та прозорості;

4. Запропонувати архітектурну модель блокчейн-системи для державних реєстрів, яка забез-

печить децентралізоване зберігання і обробку даних із підвищеним рівнем захисту;

5. Провести оцінку перспектив впровадження блокчейн-рішень у державні реєстраційні системи та визначити ключові напрями розвитку цієї технології в контексті державного управління.

Виклад основного матеріалу дослідження

Сучасні державні реєстраційні системи стикаються з низкою проблем, пов'язаних із забезпеченням безпеки, прозорості та надійності зберігання і обробки даних [6].

Традиційні централізовані реєстри є вразливими до кібератак, що може призвести до викрадення конфіденційної інформації або зміни даних, зокрема через несанкціонований доступ. Більше того, централізація даних створює залежність від єдиного точки збою, що збільшує ризик втрати або компрометації інформації. Згідно з останніми дослідженнями, центральні системи є привабливими цілями для хакерів, оскільки вони містять велику кількість конфіденційних даних.

Ще однією важливою проблемою є обмежений контроль користувачів над їхніми персональними даними. У централізованих системах громадяни не можуть впливати на те, як і хто використовує їхні дані, що часто суперечить принципам Загального регламенту про захист даних (GDPR) та інших міжнародних стандартів. Це породжує недовіру до державних реєстрів, зокрема у питаннях конфіденційності, прозорості та відповідності чинним нормам захисту даних [7, 8].

Крім того, існує проблема низької прозорості у процесах доступу та використання даних, що може сприяти зловживанням та корупційним схемам. Оскільки зміни та транзакції у централізованих системах не завжди є прозорими, це дозволяє маніпулювати даними без належного контролю.

Ці виклики вимагають впровадження нових технологічних рішень, здатних забезпечити більшу надійність, прозорість і безпеку реєстраційних систем, що використовуються в державному управлінні. Блокчейн-технологія, з її можливостями децентралізації, незмінності та прозорості транзакцій, розглядається як перспективне рішення для вирішення цих проблем, проте її впровадження потребує наукового обґрунтування та детального дослідження.

Аналіз сучасних централізованих державних реєстраційних систем

Аналіз сучасних централізованих державних реєстраційних систем виявляє численні недоліки, які значно обмежують їхню ефективність і безпеку, що особливо критично в умовах зростаючого обсягу даних і підвищених вимог до їх захисту [9].

Однією з основних проблем є вразливість до кібератак, що стає очевидною через численні інциденти, коли великі масиви персональних даних ставали жертвами зловмисників. Оскільки дані зберігаються централізовано, одна успішна атака може поставити під загрозу всю систему, надаючи доступ до значної кількості конфіденційної інформації. Централізовані системи не мають достатньо розподілених механізмів захисту, що робить їх більш вразливими до цільових атак.

Ще однією важливою проблемою є відсутність контролю користувачів над їхніми даними. У централізованих системах громадяни мають обмежений доступ до інформації про те, хто використовує їхні персональні дані і з якою метою [10]. Цей аспект є особливо критичним з точки зору вимог міжнародних стандартів, таких як Загальний регламент про захист даних (GDPR), що передбачає право громадян на доступ до своїх даних і контроль над їхнім використанням. Сучасні централізовані реєстраційні системи не завжди здатні забезпечити цей контроль, що підриває довіру до державних інституцій [11].

Низька прозорість процесів у централізованих системах є ще однією значною проблемою. Дані про транзакції, доступи та зміни в записах часто залишаються недоступними для користувачів, що призводить до зростання корупційних ризиків і можливих зловживань владою. Окрім цього, громадяни не можуть самостійно перевірити, чи їхні дані не використовуються неправомірно, що створює додаткові ризики. Для того, щоб більш наочно продемонструвати різницю між централізованими реєстраційними системами і тими, що базуються на блокчейн-технологіях, розглянемо порівняльну таблицю (табл. 1).

Як видно з наведеної таблиці, блокчейн-технології мають суттєві переваги перед традиційними централізованими системами, зокрема щодо прозорості, безпеки і контролю користувачів над своїми даними.

Таблиця 1

Порівняльний аналіз централізованих систем і блокчейн-технологій у державних реєстрах

Критерій	Централізовані системи	Блокчейн-технології
Безпека	Вразливі до централізованих атак	Високий рівень захисту завдяки децентралізації
Контроль користувачів над даними	Обмежений, переважно залежить від адміністратора системи	Повний контроль над доступом до даних через смарт-контракти
Прозорість процесів	Низька, обмежений доступ до інформації про операції з даними	Висока прозорість, кожна транзакція записується в блокчейн
Ризик корупції	Високий, через закритість системи	Низький, завдяки прозорості і неможливості зміни даних
Вразливість до технічних помилок	Висока, одна помилка може порушити всю систему	Низька, через розподілений характер даних
Швидкість обробки даних	Зазвичай висока, але залежить від потужності серверів	Може бути повільнішою через розподілену природу системи
Витрати на підтримку	Залежить від масштабу і обсягу даних	Вищі початкові витрати, але менші витрати на довгострокову підтримку

Хоча впровадження блокчейн в державні реєстраційні системи може вимагати значних початкових витрат і технічних ресурсів, довгострокові вигоди, такі як зниження корупційних ризиків і забезпечення відповідності міжнародним стандартам, роблять цю технологію перспективною для застосування в державному управлінні. Важливо також зазначити, що технологія блокчейн може вирішити проблеми, пов'язані з централізацією даних, забезпечуючи децентралізовану і прозору архітектуру з підвищеним рівнем захисту інформації [12].

Таким чином, впровадження блокчейн-технологій у державні реєстраційні системи здатне радикально змінити підходи до зберігання і обробки даних, надаючи громадянам більше контролю, а системі — більшу стійкість до зовнішніх атак і внутрішніх зловживань.

Для кращого розуміння відмінностей між блокчейн-технологіями та традиційними централізованими системами у контексті державних реєстрів, важливо порівняти їх за ключовими параметрами. Це дозволить оцінити, наскільки ефективними є обидві системи з точки зору безпеки, прозорості, контролю над даними та витрат. Блокчейн-технології часто позиціонуються як інноваційне рішення для вирішення багатьох проблем, з якими стикаються централізовані системи, проте їх впровадження має як переваги, так і виклики.

На наведеному нижче рисунку 1 представлено порівняння блокчейн-рішень та централізованих систем за чотирма критеріями: безпека, прозорість, контроль користувачів над даними та витрати. Оцінка кожної системи базується на аналізі сучасних досліджень і публікацій у цій сфері (рис. 1).

Рис. 1. Діаграма порівняння блокчейн-технології та централізованих систем

Після аналізу, представленого на діаграмі, можна зробити висновок, що блокчейн-технології мають значні переваги у сфері безпеки та прозорості, що є критично важливим для державних реєстрів. Блокчейн забезпечує незмінність даних і підвищену стійкість до кібератак завдяки децентралізованій природі. Це дозволяє знизити ризик зловживань і несанкціонованого доступу, що є типовими проблемами для централізованих систем. Ще однією важливою перевагою блокчейн є прозорість. Усі транзакції та зміни зберігаються у відкритому реєстрі, що робить їх доступними для перевірки як з боку державних органів, так і з боку громадян. Це значно підвищує рівень довіри до державних установ і сприяє зниженню корупційних ризиків.

Однак, блокчейн має і певні недоліки. Витрати на впровадження блокчейн-рішень можуть бути значно вищими, особливо на початкових етапах, коли необхідно створити нову інфраструктуру та адаптувати існуючі процеси. Крім того, незважаючи на високий рівень безпеки, забезпечення конфіденційності персональних даних у системах на основі блокчейн може бути викликом, оскільки деякі механізми публічного доступу до інформації можуть конфліктувати з нормами, такими як GDPR. Таким чином, блокчейн-технології мають великий потенціал для модернізації державних реєстрів, але їх впровадження потребує ретельного планування, врахування фінансових витрат та правових аспектів [14].

Щоб досягти максимальної ефективності, необхідно розробити стратегії, які дозволять зберегти переваги блокчейн, водночас мінімізуючи його недоліки та забезпечуючи відповідність міжнародним стандартам.

Розробка математичної моделі для кількісної оцінки ефективності впровадження блокчейн-рішень у державні реєстраційні системи

В умовах стрімкого розвитку цифрових технологій і зростання вимог до захисту даних, державні реєстраційні системи стикаються з необхідністю вдосконалення своїх механізмів обробки і зберігання інформації. Традиційні централізовані системи, що широко використовуються в даний час, демонструють обмеження в аспектах прозорості, безпеки і ефективності [15]. Потреба в нових рішеннях для підвищення надійності і захисту даних веде до активного вивчення блокчейн-технологій як можливого інструменту для трансформації цих систем.

Блокчейн, завдяки своїм унікальним властивостям, таким як децентралізація, незмінність і прозорість, обіцяє значні переваги в управлінні державними реєстрами [16]. Проте, для об'єктивної оцінки доцільності впровадження блокчейн-рішень, необхідно розробити математичну модель, яка б дозволяла кількісно оцінити їх ефективність на основі критичних показників. Ця модель повинна враховувати не тільки позитивні аспекти, але й можливі недоліки, які можуть вплинути на загальну ефективність системи.

Наукова новизна даної роботи полягає у створенні комплексної математичної моделі для оцінки ефективності впровадження блокчейн-технологій у державні реєстраційні системи. Модель враховує ключові показники, такі як надійність, безпека, прозорість і швидкість обробки даних, що дозволяє забезпечити всебічний аналіз впливу блокчейн-рішень на ці системи.

У цій роботі пропонується новий підхід до інтеграції блокчейн-технологій у державні реєстри, який включає врахування специфічних характеристик блокчейн-архітектури і їхній вплив на основні функціональні аспекти реєстраційних систем. Модель також враховує можливі сценарії впровадження і експлуатації систем, що дозволяє оцінити ефективність на різних етапах життєвого циклу системи.

Опис деталей моделі

Математична модель, розроблена для оцінки ефективності впровадження блокчейн-рішень, включає наступні етапи і компоненти:

– надійність (R): надійність системи визначається як ймовірність безвідмовної роботи. Вона розраховується як відношення часу без збоїв до загального часу роботи системи. Висока надійність блокується через децентралізовану природу блокчейн-технологій, яка знижує ймовірність одночасного збою всіх вузлів. Розраховується наступним чином:

$$R = \frac{T_{operational} - F}{T_{operational}},$$

де $T_{operational}$ — загальний час роботи системи, а F — кількість збоїв або помилок;

– безпека (S): оцінка безпеки базується на аналізі уразливостей і ймовірності їх реалізації. Блокчейн забезпечує високий рівень безпеки завдяки криптографічному захисту і розподіленій природі, що робить атаки на всю мережу малоймовірними:

$$S = \frac{1}{1 + NV}$$

де NV — кількість відомих уразливостей у системі;

– прозорість (T): прозорість визначається як кількість доступних для перевірки транзакцій або записів у реєстрі. Блокчейн забезпечує високу прозорість, оскільки всі транзакції видимі для всіх учасників і неможливо змінити інформацію без відома всієї мережі:

$$T = \frac{V}{N}$$

де V — кількість видимих або перевірених транзакцій або записів, а N — загальна кількість транзакцій або записів у системі;

– швидкість обробки даних (P): швидкість обробки даних вимірюється як час, необхідний для завершення транзакцій. Хоча блокчейн може мати повільнішу обробку через необхідність консенсусу, технологічні інновації, такі як шардінг і рівень 2 рішення, можуть значно підвищити швидкість:

$$P = \frac{1}{T_{processing}}$$

де $T_{processing}$ — середній час обробки транзакції або запиту.

Формулювання комплексної моделі

Для інтеграції всіх показників у єдину метрику ефективності, ми використовуємо зважене середнє. Кожен показник оцінюється з урахуванням його ваги, що відображає важливість цього аспекту для загальної ефективності системи. Математична формула для розрахунку загальної ефективності E має вигляд:

$$E = w_R \cdot R + w_S \cdot S + w_T \cdot T + w_P \cdot P$$

де E – загальна ефективність системи, w_R, w_S, w_T, w_P – вагові коефіцієнти для кожного з показників (надійність, безпека, прозорість, швидкість обробки), R, S, T, P – значення відповідних показників.

Визначення вагових коефіцієнтів

Вагові коефіцієнти w_R, w_S, w_T, w_P можна визначити на основі пріоритетів конкретної системи. Наприклад, у системах, де безпека є критично важливою, ваговий коефіцієнт w_S може бути вищим. Вагові коефіцієнти мають відповідати сумі 1, щоб забезпечити правильну нормалізацію:

$$w_R + w_S + w_T + w_P = 1$$

Приклад розрахунків

Припустимо, що для конкретної системи вагові коефіцієнти та значення показників є такими:

1) Надійність R= 0.95;
2) Безпека S=0.85;
3) Прозорість T=0.90;
4) Швидкість обробки P=0.80.

Вагові коефіцієнти:

1. W_R=0.25
2. W_S =0.30
3. W_T =0.20
4. W_P =0.25

Тоді загальна ефективність E розраховується як:

$$E = 0.25 \cdot 0.95 + 0.30 \cdot 0.85 + 0.20 \cdot 0.90 + 0.25 \cdot 0.80$$

$$E = 0.2375 + 0.255 + 0.18 + 0.20$$

$$E = 0.8725$$

Використання вагових коефіцієнтів у моделі дозволяє налаштувати акценти відповідно до специфічних потреб і пріоритетів системи. Це дає змогу ефективно оцінити переваги і недоліки блокчейн-рішень у контексті конкретних завдань, таких як управління реєстраціями, та забезпечити обґрунтовану підтримку рішень про їх впровадження.

Модель підтверджується сучасними науковими дослідженнями, які демонструють, що блокчейн-технології здатні значно поліпшити надійність і безпеку систем у порівнянні з традиційними централізованими рішеннями. Дослідження також вказують на можливість зменшення корупційних ризиків і підвищення прозорості процесів завдяки децентралізації та можливості відкритого моніторингу транзакцій.

Таким чином, розроблена модель є корисним інструментом для оцінки і порівняння ефективності технологій у контексті конкретних прикладів застосування.

Після аналізу та розробки математичної моделі для кількісної оцінки ефективності впровадження блокчейн-рішень у державні реєстраційні системи, важливо перейти до практичного аспекту реалізації цих рішень. Математична модель дозволяє оцінити потенційні вигоди та визначити ключові показники для успішного впровадження технологій, проте для реального застосування необхідно розробити чітку архітектуру системи.

Варто зосередитись на основах розробки архітектури блокчейн-системи для державних реєстрів.

Розробка архітектурної моделі блокчейн-системи у державних реєстрах

Для забезпечення децентралізованого зберігання та обробки даних з підвищеним рівнем захисту пропонується архітектура блокчейн-системи, що включає декілька важливих компонентів, які дозволять вирішити основні проблеми централізованих реєстраційних систем, такі як вразливість до кібератак, низька прозорість і недостатній контроль з боку користувачів над їхніми даними.

Основні компоненти архітектури

1. Користувацький інтерфейс (UI Layer). Це рівень, з яким взаємодіють кінцеві користувачі, такі як громадяни, державні установи або органи управління. Користувачі отримують доступ до реєстраційних даних, можуть виконувати операції, такі як реєстрація, оновлення даних або перевірка записів. Цей інтерфейс має бути зручним та безпечним, забезпечуючи автентифікацію та авторизацію користувачів.

Ключові функції:

5) інтерфейси веб-додатків або мобільних додатків;

6) доступ до даних через особисті кабінети з двофакторною автентифікацією (2FA);

7) підтримка смарт-контрактів для автоматизації операцій;

2. API-шар (API Layer). Цей шар забезпечує комунікацію між користувацьким інтерфейсом і блокчейн-мережею. Він виступає проміжним компонентом, через який дані і запити передаються між фронтендом і основною блокчейн-інфраструктурою. API відповідає за захищену передачу даних, їхнє шифрування та декодування.

Ключові функції:

8) аутентифікація та авторизація запитів;

9) шифрування даних перед відправкою у блокчейн;

10) інтеграція зі сторонніми системами та реєстрами.

3. Блокчейн-шар (Blockchain Layer). Основний компонент системи, який зберігає всі транзакції та реєстраційні дані в незмінному та децентралізованому вигляді. Всі дані записуються у блоки, що формують ланцюг. Цей ланцюг є незмінним і прозорим, що дозволяє забезпечити перевірюваність і контроль за операціями в системі. Використовуються смарт-контракти для автоматизації перевірки транзакцій, що підвищує швидкість і точність обробки даних.

Ключові функції:

11) децентралізоване зберігання даних;

12) використання смарт-контрактів для автоматизації операцій (наприклад, підтвердження прав власності або доступу до даних);

13) консенсусний механізм (Proof of Stake або інші енергоефективні механізми) для перевірки транзакцій.

4. Механізм консенсусу (Consensus Mechanism). Цей компонент відповідає за узгодження даних у мережі. Оскільки система є децентралізованою, дані повинні бути узгоджені між усіма вузлами мережі для забезпечення їхньої незмінності. Використання механізму Proof of Stake (PoS) або іншого механізму консенсусу дозволяє досягти консенсусу щодо нових транзакцій із мінімальними витратами ресурсів.

Ключові функції:

14) узгодження транзакцій між усіма вузлами мережі;

15) забезпечення стійкості до атак через децентралізацію;

16) мінімізація енергетичних витрат порівняно з Proof of Work (PoW).

5. Система децентралізованого зберігання (Decentralized Storage System). Для зберігання великих обсягів даних, таких як документи або файли, використовуються децентралізовані файлові системи, наприклад, IPFS (InterPlanetary File System). Це дозволяє ефективно зберігати великі файли, при цьому забезпечуючи їхню доступність через блокчейн-запити.

Ключові функції:

17) зберігання файлів та документів у децентралізованій системі з можливістю доступу через хеші, записані в блокчейн;

18) забезпечення доступності даних, навіть якщо один або кілька вузлів вийдуть з ладу;

19) захист від втрати даних через реплікацію на різних вузлах.

6. Система безпеки і конфіденційності (Security and Privacy Layer). Цей компонент відповідає за шифрування даних і забезпечення конфіденційності. Особисті дані користувачів повинні бути зашифровані перед зберіганням у блокчейн для дотримання вимог таких стандартів, як GDPR. Крім того, система повинна підтримувати функції децентралізованого

управління ключами для забезпечення конфіденційності даних.

Ключові функції:

20) шифрування персональних даних користувачів;

21) децентралізоване управління ключами;

22) відповідність GDPR та іншим міжнародним стандартам конфіденційності.

7. Система аудиту та моніторингу (Audit and Monitoring System). Ця система забезпечує контроль за всіма операціями в реєстрі. Вона дозволяє проводити аудит будь-якої транзакції, забезпечуючи прозорість операцій для відповідальних органів і користувачів. Всі транзакції можуть бути легко перевірені, а результати доступні в реальному часі.

Ключові функції:

23) можливість перегляду історії транзакцій для аудиту;

24) система сповіщень про підозрілі операції;

25) звіти в реальному часі для державних органів.

Нижче зображено основні компоненти блокчейн-системи, які забезпечують ефективне зберігання, управління та захист державних реєстрів (рис. 2). Користувацький інтерфейс взаємодіє з API-шаром, який передає дані до блокчейн-шару для децентралізованого зберігання. У свою чергу, дані реєстрів зберігаються у Державному реєстрі та захищені системою безпеки, яка відповідає за шифрування та управління ключами.

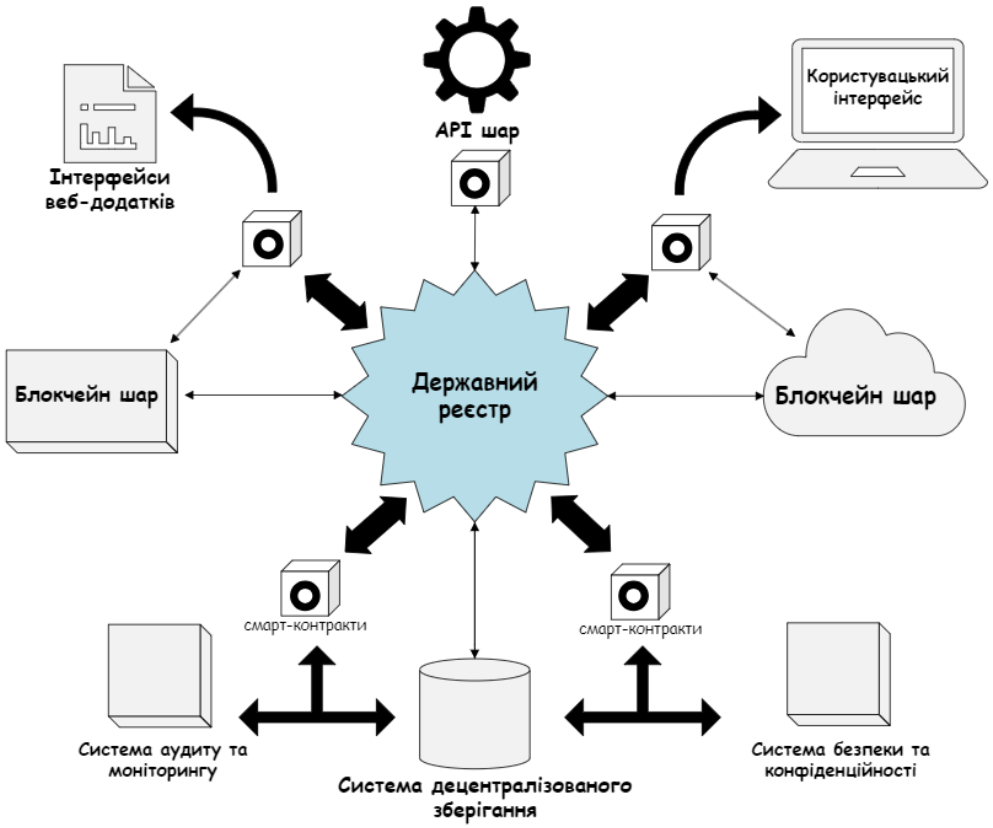

Рис. 2. Архітектурна схема блокчейн-системи для державних реєстрів України

Запропонована архітектурна модель блокчейн-системи для державних реєстрів забезпечує децентралізоване зберігання та обробку даних з високим рівнем захисту, прозорістю та стійкістю до атак. Вона також гарантує відповідність вимогам міжнародних стандартів, таких як GDPR, і надає користувачам більше контролю над їхніми даними.

Оцінка перспектив та ключові напрями розвитку блокчейн-технологій у державних реєстраційних системах

Оцінка перспектив впровадження блокчейн-технологій у державні реєстраційні системи показує значний потенціал цієї технології для підвищення ефективності, прозорості та безпеки державного управління [17]. Традиційні централізовані системи стикаються з численними викликами, такими як вразливість до кібератак, складність забезпечення прозорості та контролю над даними, а також необхідність відповідати міжнародним стандартам, як-от GDPR. Блокчейн пропонує вирішення багатьох з цих проблем завдяки своїй децентралізованій і незмінній природі, що робить його ефективним інструментом для управління державними реєстрами.

Блокчейн може забезпечити значне підвищення прозорості процесів у державних реєстраційних системах, оскільки кожна транзакція фіксується в реєстрі, який доступний для перевірки всіма учасниками системи [18].

Це сприяє зниженню корупційних ризиків, адже маніпуляції з даними стають практично неможливими.

Крім того, високий рівень безпеки забезпечується завдяки децентралізованому зберіганню інформації: дані розміщуються на багатьох вузлах, що унеможливлює їх компрометацію в разі атаки на один із серверів.

Однією з найбільших переваг блокчейн є можливість автоматизації процесів за допомогою смарт-контрактів. Це дає змогу автоматично виконувати певні дії, як-от реєстрацію прав власності або видачу дозволів, без

участі посередників, що знижує рівень бюрократії і пришвидшує обробку заявок. Блокчейн також дає змогу користувачам самостійно керувати своїми персональними даними, надаючи або відкликаючи доступ до них відповідно до встановлених правил. Це відповідає вимогам міжнародних стандартів захисту даних і підвищує рівень довіри громадян до державних установ.

Застосування блокчейн-рішень також може суттєво скоротити витрати на адміністрування державних реєстрів, адже автоматизація та децентралізоване зберігання інформації знижують потребу в значних ресурсах для їх підтримки. Однак впровадження блокчейн потребує значних початкових інвестицій, що може стати викликом для багатьох державних органів. Крім того, проблеми масштабованості блокчейн залишаються відкритими: чим більше транзакцій обробляє система, тим більше ресурсів вона вимагає.

Однак головною перешкодою для впровадження блокчейн можуть бути правові та регуляторні обмеження. Необхідність розробки нових законодавчих і регуляторних механізмів для контролю за блокчейн-рішеннями є важливим елементом процесу впровадження. Успіх технології залежить від створення відповідної законодавчої бази, яка буде забезпечувати захист даних і відповідність міжнародним стандартам.

Для успішного впровадження блокчейн-рішень важливо забезпечити інтеграцію технології з уже існуючими державними системами. Розвиток механізмів консенсусу, таких як Proof of Stake, може допомогти вирішити проблеми масштабованості і знизити енергетичні витратиv [19]. Блокчейн також може сприяти підвищенню довіри до державних установ, забезпечуючи прозорість і незмінність даних, що є критично важливим для довіри громадян до державних процесів [20].

Отже, блокчейн-технології мають великий потенціал для трансформації державних реєстраційних систем, але для успішного впровадження необхідно враховувати чинні виклики. Розвиток законодавчої бази, адаптація існуючих процесів та вирішення технічних питань є ключовими умовами для інтеграції блокчейн в державне управління. У довгостроковій перспективі блокчейн може стати основною технологією, яка сприятиме модернізації державних систем і підвищенню довіри громадян до державних інституцій.

Висновки. Висновки по дослідженню впровадження блокчейн-технологій у державні реєстраційні системи підтверджують їхній значний потенціал для підвищення прозорості, безпеки та ефективності управління. Традиційні централізовані системи державних реєстрів мають низку суттєвих недоліків, таких як вразливість до кібератак, відсутність належного контролю користувачів над їхніми даними та складність дотримання міжнародних стандартів конфіденційності, таких як GDPR. Блокчейн-технології надають нові можливості для вирішення цих проблем, забезпечуючи децентралізоване зберігання даних, яке є стійким до несанкціонованого втручання.

Використання смарт-контрактів дозволяє автоматизувати ключові процеси, такі як реєстрація прав власності або управління дозволами, що значно знижує рівень бюрократії та пришвидшує процеси в державних органах. Основними перевагами блокчейн-систем є прозорість, безпека, контроль користувачів над своїми даними та скорочення витрат на адміністрування реєстрів. Прозорість забезпечується завдяки незмінній природі блокчейн, який фіксує кожну транзакцію, що дозволяє відстежувати зміни в реєстрах та перевіряти їхню автентичність. Безпека підвищується за рахунок децентралізованого зберігання даних у багатьох вузлах мережі, що мінімізує ризик компрометації даних. Користувачі отримують більше контролю над доступом до своїх даних, що відповідає міжнародним вимогам захисту персональної інформації.

Однак, дослідження також виявило ряд викликів і обмежень для впровадження блокчейн-рішень у державних реєстрах. Серед них – високі початкові витрати на впровадження та необхідність адаптації існуючих систем до нових умов. Проблеми масштабованості технології та правові аспекти, пов'язані з її використанням, також потребують уваги з боку урядових органів і регуляторів.

Для успішного впровадження блокчейн в державних реєстраційних системах важливо розвивати відповідну законодавчу базу, яка забезпечить дотримання міжнародних стандартів і прав користувачів. Крім того, важливо забезпечити ефективну інтеграцію блокчейн-систем з існуючими державними системами для уникнення збоїв у їх роботі.

У цілому, блокчейн-технології мають великий потенціал для модернізації державного управління, і їхнє впровадження може сприяти підвищенню довіри до державних інституцій з боку громадян. У довгостроковій перспективі блокчейн може стати ключовою технологією, яка сприятиме підвищенню ефективності та безпеки державних реєстраційних систем.

Список літератури

[1]. Dong, M., Wang, X., Niyato, D., & Han, Z. (2021). "Blockchain for Secure and Trustworthy IoT: A Survey." IEEE Access, 9, pp. 4955-4971. https://doi. org/10.1109 /JIOT.2019.2920987.

[2]. Poberezhnyk, V., Balatska, V., & Opirskyy, I. (2023). Development of the Learning Management System Concept based on Blockchain Technology. Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, 3550, pp. 143-156. https://doi.org/ 10.28925/2663-4023.2023.20.619.

[3]. Balatska, V., Poberezhnyk, V., Petriv, P., & Opirskyy, I. (2024). Blockchain Application Concept in SSO Technology Context. CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, Kyiv, Ukraine, pp. 38-49. /https://doi.org/10. 28925/ 2663-4023. 2024. 24. 99114.

[4]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

[5]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." IEEE International Congress on Big Data, pp. 557-564. https: //doi.org/ 10.1109/BigDataCongress.2017.85.

[6]. Pilkington, M. (2016). "Blockchain Technology: Principles and Applications." In Research Handbook on Digital Transformations, pp. 225-253. Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00014

[7]. Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley. https: // www.wiley.com /en-us/ The+Business+Blockchain%3A+Promise%2C+Practice%

2C+and+Application+of+the+Next+Internet+Technology-p-9781119300311.

[8]. Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. https:// github.com/ethereum/wiki/wiki/White-Paper.

[9]. Zyskind, G., Nathan, O., & Pentland, A. (2015). "Decentralizing Privacy: Using Blockchain to Protect Personal Data." 2015 IEEE Security and Privacy Workshops, 180-184. https://doi.org/10.1109/SPW.2015.27.

[10]. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin. https: // www.penguinrandomhouse.com / books/ 248181/blockchain-revolution-by-don-tapscott-and-alex-tapscott/.

[11]. Bălăcescu, P., Frățilă, D., & Simion, D. (2020). "Blockchain technology applied in the public sector: opportunities and challenges." Proceedings of the International Conference on Informatics in Economy, 101-107. https://doi.org/10.1109/ICIE50452.2020.9254596.

[12]. Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K. L. (2018). "Blockbench: A Framework for Analyzing Private Blockchains." Proceedings of the 2017 ACM International Conference on Management of Data, 1085-1100. https://doi.org/10.1145/3035918.3064033.

[13]. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). "Blockchain Technology Overview." NIST, U.S. Department of Commerce. https://doi.org/10.6028/ NIST.IR.8202.

[14]. Kshetri, N. (2017). "Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy." Telecommunications Policy, 41(10), 1027-1038. https://doi.org/10. 1016/j.telpol.2017.09.003.

[15]. Балацька, В. С., Опірський, І. Р. (2023). Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. Кібербезпека: освіта, наука, техніка, 4 (20), 6-19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619.

[16]. Балацька, В., Побережник, В., Опірський, І. (2024). Використання Non-Fungible Tokens та блокчейн для розмежування доступу до державних реєстрів. Кібербезпека: освіта, наука, техніка, 4(24), 99–114. DOI: https: // doi.org/10.28925/2663-4023.2024.24. 99114.

[17]. Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D., & Wattenhofer, R. (2016). "On Scaling Decentralized Blockchains." Proceedings of the 2016 International Conference on Financial Cryptography and Data Security, 106-125. https://doi.org/10.1007/978-3-662-53357-4_8.

[18]. Christidis, K., & Devetsikiotis, M. (2016). "Blockchains and Smart Contracts for the Internet of Things." IEEE Access, 4, 2292-2303. https://doi.org /10.1109/ACCESS.2016.2566339.

[19]. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). "Blockchain Technology: Beyond Bitcoin." Applied Innovation Review, 2, 6-19. https:// j2capital.com / wp-content / uploads / 2017/11/ AIR-2016-Blockchain.pdf.

[20]. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues." Telecommunications Systems, 171-190. https:// doi.org/10.1007/s11235-018-0481-5.

УДК 004.065

Balatska V., Opirskyy I. Blockchain as a Tool for Transparency and Protection of Government Registries

Abstract. *With the advancement of digital technologies and the growing demand for transparency and data security, government registration systems face several challenges associated with their centralized architecture. Traditional centralized systems used for storing and processing data exhibit various problems, including vulnerability to cyberattacks, insufficient protection of personal data, lack of user control over their information, and non-compliance with international standards, such as the General Data Protection Regulation (GDPR). This creates the need for the adoption of new technological solutions capable of addressing these shortcomings and ensuring enhanced reliability for government registries. This research proposes the implementation of blockchain technologies in government registration systems as a solution capable of improving data security, transparency, and reliability while providing users with greater control over their personal information. Blockchain enables the creation of decentralized systems where data cannot be altered without proper authentication, and all transactions are recorded, reducing the risk of unauthorized access and fraud. A key element of this study is the development of a mathematical model for quantitatively assessing the effectiveness of blockchain adoption in government registration systems. The model evaluates security, transparency, reliability, and data processing speed indicators, allowing for a comparison with traditional centralized systems. The analysis shows that blockchain can significantly reduce corruption risks, ensure full transparency of government processes, and improve citizens' trust in public institutions. Moreover, blockchain implementation complies with international data security and protection standards, such as GDPR, making this technology a promising tool for public administration. The study also highlights key directions for blockchain development, including improving system scalability, optimizing data processing costs, and integrating with other technologies for public governance.*

The findings demonstrate the significant potential of blockchain solutions to transform government registries, and the developed model can be used as a tool for further research and implementation of the technology in public institutions.

Keywords*: blockchain, government registries, personal data, transparency, security, decentralization, GDPR, mathematical model, data management, digital transformation.*

Балацька Валерія Сергіївна, аспірант, кафедра захисту інформації, Національного університету «Львівська політехніка».
Valeriia Balatska, PhD Students of Information Security Department, Lviv Polytechnic National University.

Опірський Іван Романович, доктор технічних наук, професор, кафедра захисту інформації, Національного університету «Львівська політехніка».
Ivan Opirskyy, doctor of Technical Sciences, professor, Department of Information Security, Lviv Polytechnic National University.

Отримано *23 травня 2024 року*, затверджено редколегією *26 червня 2024 року*