КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.681
УДК 004.056

Балацька Валерія Сергіївна
аспірант кафедри «Захист інформації»
Національний Університет «Львівська Політехніка», Львів, Україна
викладач кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID ID: 0000-0002-6262-6792
valeriia.s.balatska@lpnu.ua, lera31505@gmail.com

Побережник Василь Олегович
аспірант кафедри «Захист інформації»
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-7523-2557
vasyl.poberezhnyk@gmail.com

КОНЦЕПЦІЯ ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ ПЛАТФОРМИ «ДІЯ»: ВІДПОВІДНІСТЬ ВИМОГАМ GDPR ТА УКРАЇНСЬКОМУ ЗАКОНОДАВСТВУ

Анотація. З розвитком цифрових державних сервісів і проєкту «Дія» в Україні, питання захисту персональних даних стає одним з найважливіших викликів, особливо в контексті дотримання вимог Загального регламенту про захист даних (GDPR) і національного законодавства. Сучасні цифрові рішення повинні забезпечувати прозорість, безпеку та відповідність правовим нормам щодо обробки та зберігання персональної інформації громадян. У даному дослідженні пропонується інтеграція блокчейн-технологій у проєкт «Дія» як ефективного засобу для підвищення конфіденційності та безпеки персональних даних. Використання блокчейн забезпечує незмінність і прозорість даних у державних реєстрах, дозволяючи відстежувати всі операції з інформацією та фіксувати кожен запит на доступ. Це особливо важливо для дотримання принципів GDPR, таких як прозорість обробки даних, право на інформацію та право на забуття. Запропонована система включає ключові технологічні компоненти, такі як смарт-контракти для автоматизації управління згодою на обробку даних і розмежування доступу до них. Смарт-контракти дозволяють забезпечити автоматичне та безпечне виконання угод між користувачем і системою, значно знижуючи ризики людських помилок або зловживань. Крім того, використання децентралізованої файлової системи IPFS гарантує надійне зберігання файлів, що виключає можливість централізованих атак або втрати інформації. Методи захисту даних, такі як маскування, псевдоанонімізація та пертурбація, допомагають знизити ризик несанкціонованого розкриття інформації навіть у випадку витоку даних. Це особливо актуально для державних реєстрів, які містять чутливу інформацію про громадян, і забезпечує високий рівень захисту відповідно до стандартів GDPR. Реалізація даної концепції в рамках проєкту «Дія» не тільки підвищить довіру громадян до державних цифрових послуг, але й створить умови для інтеграції України в європейський правовий простір з точки зору захисту персональних даних. Запропоноване рішення може стати фундаментом для подальшого розвитку державних реєстрів та інших цифрових сервісів, орієнтованих на захист даних у рамках новітніх технологій. Метою дослідження є аналіз і розробка інноваційної системи для захисту персональних даних у державних реєстрах України на основі блокчейн-технологій, що відповідає вимогам GDPR та національного законодавства. Такий підхід забезпечить надійність, безпеку та прозорість обробки даних, що сприятиме цифровій трансформації державного управління.

Ключові слова: захист персональних даних; блокчейн; «Дія»; смарт-контракти; GDPR; українське законодавство; IPFS; децентралізовані системи зберігання; державні реєстри; конфіденційність; управління згодами; децентралізація.

ВСТУП

Зі стрімким розвитком інформаційних технологій, уряди різних країн світу зосереджують свої зусилля на впровадженні цифрових рішень для надання державних послуг громадянам. В Україні цей процес набув нового рівня завдяки проєкту «Дія» — цифровій платформі, яка об'єднує низку державних послуг в одному зручному інтерфейсі. Мільйони українців тепер можуть отримувати державні послуги онлайн, використовуючи цифрові документи, реєструвати майно, сплачувати податки, подавати запити на соціальні послуги та інше. Це підвищує ефективність, зручність і прозорість роботи державних органів, але також створює нові виклики, пов'язані з безпекою та конфіденційністю персональних даних [1]. Питання потенційних загроз кібербезпеки платформи «Дія» неодноразово піднімалося в експертних колах. Наприклад, у січні 2022 року в інтернеті з'явилися повідомлення про нібито продаж персональних даних українських користувачів цього сервісу. Попри те, що Міністерство цифрової трансформації заперечило злам і назвало його інформаційною провокацією, вказуючи, що дані у додатку лише підтягуються з державних реєстрів, це питання залишилося дискусійним та не отримало остаточного спростування або підтвердження [2].

Однією з ключових загроз цифровізації є ризики несанкціонованого доступу до персональних даних, маніпуляцій з ними та можливих витоків інформації. Ці питання є особливо важливими в контексті вимог Загального регламенту про захист даних (GDPR), який встановлює суворі правила щодо обробки персональних даних громадян Європейського Союзу. Для країн, які прагнуть інтеграції в європейський простір, таких як Україна, необхідно забезпечити відповідність своїх цифрових систем міжнародним стандартам у сфері захисту даних.

GDPR вимагає забезпечення прозорості обробки даних, згоди користувачів на їх обробку, права на доступ, виправлення та видалення даних, а також звітності щодо використання персональних даних. Невиконання цих вимог може призвести до серйозних юридичних наслідків і втрати довіри з боку громадян. У той же час, українське законодавство, зокрема Закон України «Про захист персональних даних», також передбачає ряд правил щодо обробки та захисту даних, які мають бути інтегровані в національні цифрові сервіси [3].

З огляду на це, необхідно впроваджувати інноваційні технологічні рішення, які можуть забезпечити належний рівень безпеки та відповідності вимогам законодавства. Одним з перспективних напрямків є використання блокчейн-технологій, що можуть забезпечити незмінність записів, прозорість транзакцій та захищений контроль доступу до інформації. Блокчейн-технології пропонують децентралізовану, захищену систему, яка мінімізує ризики втрати або модифікації даних і створює можливість чітко відстежувати всі операції з інформацією.

Крім того, важливим аспектом є використання смарт-контрактів, які дозволяють автоматизувати управління правами доступу та обробкою персональних даних. Смарт-контракти можуть виступати засобом контролю за згодами користувачів, визначаючи умови і дозволи на обробку інформації, що мінімізує людські помилки та підвищує ефективність захисту даних. Ще одним важливим елементом є застосування децентралізованої файлової системи IPFS, яка забезпечує надійне та розподілене зберігання даних без єдиної точки відмови, що робить її більш захищеною від кібератак і втрати даних.

Метою даної роботи є розробити концепції використання блокчейн-технологій, смарт-контрактів і IPFS у проєкті «Дія» для забезпечення конфіденційності та безпеки

персональних даних. У рамках дослідження буде проаналізовано можливість інтеграції блокчейн з українськими державними реєстрами, забезпечення відповідності вимогам GDPR і національного законодавства, а також розглянуто технічні й організаційні аспекти впровадження цієї концепції. Передбачається, що запропоноване рішення сприятиме підвищенню безпеки персональних даних, зниженню ризиків несанкціонованого доступу та створенню нових можливостей для розвитку цифрових державних сервісів в Україні.

Таким чином, дане дослідження дозволяє науково обґрунтувати необхідність впровадження блокчейн-технологій у державні реєстри та цифрові сервіси як «Дія» з метою підвищення рівня захисту персональних даних і відповідності законодавчим вимогам, таким як GDPR.

Постановка проблеми. З розвитком цифрових технологій в Україні спостерігається стрімке зростання обсягу даних, що обробляються та зберігаються державними структурами. Проєкт «Дія» став важливим кроком у напрямку цифровізації державних послуг, надаючи громадянам зручний доступ до своїх персональних даних і спрощуючи взаємодію з державними установами. Однак це породжує ряд нових викликів у сфері захисту інформації, зокрема конфіденційності та безпеки персональних даних, які зберігаються та обробляються в рамках цієї платформи.

Однією з основних проблем є високий ризик несанкціонованого доступу до персональних даних через централізовані системи зберігання. Централізація даних створює вразливі місця для кіберзлочинців, що може призвести до масштабних витоків інформації або маніпуляцій з даними користувачів. Це, у свою чергу, може призвести до втрати довіри громадян до державних цифрових сервісів, що є критично важливим у період зростання обсягу оброблюваних даних та масштабів цифровізації.

Крім того, Україна, як країна, що прагне до європейської інтеграції, повинна дотримуватися міжнародних стандартів захисту персональних даних, таких як Загальний регламент про захист даних (GDPR). GDPR висуває жорсткі вимоги до обробки, зберігання і доступу до персональної інформації, включаючи право на видалення даних, прозорість операцій з даними, забезпечення належного рівня безпеки і збереження конфіденційності. Поточні державні системи, такі як «Дія», потребують вдосконалення механізмів контролю доступу до даних та інструментів для ефективного управління згодами користувачів на обробку їхніх даних.

На додаток до цього, актуальною є проблема забезпечення незмінності даних у державних реєстрах, що зберігають інформацію про громадян, їхнє майно, реєстраційні записи та інші важливі дані. Маніпуляції з цими даними можуть мати серйозні правові та соціальні наслідки, тому забезпечення їхньої цілісності є ключовим завданням для держави.

Таким чином, постає проблема необхідності впровадження новітніх технологій, таких як блокчейн, для забезпечення прозорості, безпеки та відповідності міжнародним стандартам у роботі з персональними даними. Блокчейн-технології здатні забезпечити незмінність записів, прозорість доступу до даних та захист від несанкціонованого доступу. Крім того, інтеграція смарт-контрактів дозволить автоматизувати процеси управління згодами користувачів та надання доступу до даних, що мінімізує людські помилки та зловживання.

Отже, основна проблема полягає в необхідності розробки та впровадження надійної системи для захисту персональних даних у рамках державних цифрових сервісів, таких як «Дія», що відповідатиме вимогам GDPR та національного

законодавства, з використанням інноваційних блокчейн-технологій та децентралізованих систем зберігання даних.

Аналіз останніх досліджень і публікацій. Останні дослідження та публікації у сфері захисту персональних даних свідчать про зростаючий інтерес до використання блокчейн-технологій для забезпечення конфіденційності та безпеки інформації [4]. Фахівці активно досліджують можливості застосування блокчейн для створення децентралізованих систем зберігання даних, які здатні забезпечити високу ступінь захисту від несанкціонованого доступу та витоків інформації. Однією з ключових переваг блокчейн є його незмінність і прозорість, що дозволяє відстежувати всі дії з даними та гарантувати їхню цілісність. Блокчейн забезпечує незмінність даних, що робить їх недоступними для несанкціонованих змін, а також дозволяє використовувати смарт-контракти для автоматизації процесів управління доступом до даних [5].

Смарт-контракти можуть виконувати роль автоматизованих механізмів для контролю доступу до персональних даних відповідно до встановлених правил і згод користувачів, що підвищує безпеку обробки інформації та зменшує вплив людського фактору [6]. Ці автоматизовані процеси дозволяють точніше й ефективніше керувати доступом до даних, мінімізуючи ризики помилок або зловживань.

Значну увагу в дослідженнях приділяють децентралізованим файловим системам, таким як IPFS (InterPlanetary File System), які дозволяють зберігати великі обсяги даних у розподіленому середовищі. IPFS забезпечує підвищену доступність і захист від атак, оскільки розподіляє дані між різними вузлами мережі, зберігаючи їхню цілісність за допомогою хешування [7]. Це важливий аспект для відповідності вимогам GDPR, оскільки IPFS надає механізм зберігання, який забезпечує як прозорість, так і безпеку даних.

Ключовими характеристиками блокчейн є незмінність та прозорість. Незмінність забезпечується механізмом консенсусу, де кожен учасник мережі має копію всіх транзакцій, а будь-яка зміна даних вимагає узгодження більшості вузлів [8]. Такий механізм робить дані в блокчейн практично неможливими для зміни без схвалення інших учасників, що гарантує їхню захищеність та незмінність. Прозорість забезпечується доступом до всіх даних у мережі, що дозволяє кожному учаснику відстежувати всі транзакції або стани рахунків. Ці властивості роблять блокчейн ідеальним інструментом для захисту персональних даних та інших конфіденційних інформаційних активів [9].

Методи обробки даних, такі як маскування, псевдоанонімізація, тасування та пертурбація, активно досліджуються як додаткові способи забезпечення конфіденційності даних. Ці методи дозволяють зберігати корисність даних для аналітики, знижуючи ризик розкриття чутливої інформації [10]. Використання таких методів, разом із блокчейн-технологіями, може забезпечити високий рівень захисту персональних даних і відповідність вимогам GDPR.

Останні дослідження підкреслюють значний потенціал блокчейн-технологій для створення безпечних і прозорих систем зберігання та обробки персональних даних. Поєднання блокчейн, смарт-контрактів, IPFS та сучасних методів обробки даних може стати надійним інструментом для досягнення відповідності GDPR і підвищення рівня безпеки в цифровому середовищі [11]. Це відкриває нові можливості для інтеграції блокчейн-технологій у державні цифрові платформи, такі як «Дія», забезпечуючи безпеку та конфіденційність даних громадян на високому рівні.

Метою статті є розробка концепції інноваційного сервісу для збору, зберігання та управління персональними даними, який відповідає вимогам Загального регламенту про захист даних (GDPR) та українського законодавства.

Основними завданнями статті виступають:

1. Аналіз сучасних викликів у сфері захисту персональних даних в контексті впровадження цифрових державних сервісів, таких як проєкт «Дія».
2. Дослідження можливостей застосування блокчейн-технологій для забезпечення незмінності та прозорості обробки персональних даних у державних реєстрах.
3. Розробка концепції інтеграції смарт-контрактів для автоматизації процесів управління доступом до даних і згод користувачів.
4. Оцінка ефективності використання децентралізованих систем зберігання даних, таких як IPFS, для підвищення рівня захисту та доступності персональних даних.
5. Визначення ключових переваг та можливих викликів впровадження блокчейн-технологій у державних цифрових платформах з точки зору відповідності вимогам GDPR та українського законодавства.

Ці завдання спрямовані на створення інноваційного сервісу, який забезпечить високий рівень захисту персональних даних відповідно до вимог GDPR, використовуючи сучасні технології для підвищення безпеки, прозорості та ефективності обробки даних. Використання блокчейн-технологій, смарт-контрактів та децентралізованих систем зберігання даних дозволить мінімізувати ризики несанкціонованого доступу і маніпуляцій з даними, а також автоматизувати процеси управління згодами та правами доступу, що відповідає міжнародним стандартам захисту інформації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Аналіз викликів у сфері захисту персональних даних в цифрових державних сервісах

Захист персональних даних є однією з ключових проблем у розвитку цифрових державних сервісів, таких як проєкт «Дія», який активно впроваджується в Україні. Мільйони користувачів отримують доступ до державних послуг через цифровий інтерфейс, що значно спрощує процеси взаємодії з державою, але одночасно створює нові загрози для безпеки персональних даних. Ці виклики стосуються не тільки технологічних аспектів, але й відповідності законодавчим вимогам, зокрема Загальному регламенту про захист даних (GDPR).

Основні виклики в цифрових державних системах:

1. Централізація даних — більшість державних платформ для надання послуг, таких як «Дія», використовують централізовані моделі зберігання даних. Це створює єдину точку вразливості, яка може стати об’єктом хакерських атак або призвести до внутрішніх порушень безпеки. У випадку успішного злому система може втратити великі обсяги персональних даних громадян, що призведе до серйозних наслідків, включаючи втрату довіри з боку користувачів.
2. Недостатня прозорість процесів обробки даних — сучасні цифрові платформи часто не мають механізмів для прозорого відстеження всіх дій з даними. Це ускладнює контроль за обробкою персональних даних як з боку користувачів, так і з боку державних органів. Відсутність такого механізму

знижує довіру до системи і може ускладнити виконання вимог GDPR щодо права на доступ і контроль над персональними даними.

3. GDPR накладає жорсткі вимоги до обробки, зберігання та захисту персональних даних, включаючи забезпечення прозорості, права на доступ і виправлення даних, а також контроль за згодою користувачів на обробку їхньої інформації. Україна, як держава, що прагне європейської інтеграції, повинна адаптувати свої цифрові системи відповідно до цих стандартів.

Ризик несанкціонованого доступу — персональні дані є мішенню для кіберзлочинців, і навіть наявність внутрішніх зловживань може створити додаткові загрози безпеці. Недостатній контроль доступу до даних і відсутність автоматизованих систем для управління правами доступу створюють ризик витоку інформації.

Організації, які обробляють великі обсяги персональних даних, зокрема через державні платформи, повинні впроваджувати сучасні технології для їх захисту [12]. Основні методи, що використовуються для забезпечення конфіденційності та безпеки даних, включають:

- Шифрування — використовується для захисту даних під час зберігання та передачі. Це один з найефективніших методів для захисту від несанкціонованого доступу.
- Псевдоанонімізація — цей метод дозволяє замінювати особисті дані на штучні ідентифікатори, що значно ускладнює ідентифікацію користувачів.
- Смарт-контракти — технологія, що використовується для автоматизації процесів управління доступом до даних. Смарт-контракти дозволяють забезпечити дотримання згоди на обробку даних і запобігти несанкціонованим діям з даними.
- Моніторинг і аудит — забезпечує прозорість дій з даними, що дозволяє вчасно виявляти порушення та реагувати на них.

У табл. 1 наведено короткий опис основних методів захисту персональних даних, їхні переваги та недоліки.

Таблиця 1

Методи захисту персональних даних у державних цифрових системах

Метод захисту	Опис	Переваги	Недоліки
Шифрування	Перетворення даних для захисту від доступу	Високий рівень безпеки	Високі вимоги до управління ключами
Псевдоанонімізація	Замінює ідентифікуючі дані штучними	Забезпечує конфіденційність	Можливість відновлення ідентифікаторів
Смарт-контракти	Автоматизація управління доступом	Автоматизація, прозорість	Складність реалізації та впровадження
Моніторинг і аудит	Відстеження дій з даними	Прозорість, можливість швидкого реагування	Висока вартість впровадження
Децентралізоване зберігання	Розподіл даних між вузлами мережі	Відсутність єдиної точки відмови	Висока складність управління та підтримки

Аналіз методів захисту персональних даних, наведених у табл.1, дозволяє зробити висновки щодо доцільності їх впровадження у державних цифрових платформах, таких як «Дія». Використання шифрування та смарт-контрактів забезпечує високий рівень безпеки, тоді як децентралізоване зберігання даних зменшує ризик витоків, що робить ці методи важливими для захисту персональних даних та відповідності вимогам GDPR.

Використання блокчейн-технологій у державних платформах, таких як «Дія», може вирішити більшість вищеописаних проблем. Блокчейн забезпечує децентралізацію зберігання даних, що мінімізує ризик централізованих атак і втрати даних. Крім того, блокчейн гарантує незмінність записів та прозорість усіх транзакцій, що дозволяє повністю контролювати обробку даних і виконувати вимоги GDPR щодо прозорості та контролю згод.

- **Прозорість обробки**: усі транзакції, що стосуються обробки персональних даних, фіксуються в незмінному реєстрі, що дозволяє відстежувати будь-які зміни або дії з даними.
- **Контроль згод**: смарт-контракти дозволяють автоматизувати процес управління згодами користувачів, що підвищує точність і зменшує ризик порушень.

Аналіз викликів у сфері захисту персональних даних в рамках цифрових державних платформ вказує на необхідність модернізації підходів до обробки даних. Впровадження блокчейн-технологій та децентралізованих моделей зберігання, таких як IPFS, може значно підвищити рівень безпеки персональних даних та забезпечити відповідність державних платформ вимогам GDPR.

Розробка концепції застосування технології блокчейн та смарт-контрактів для підвищення довіри до системи

Основна наукова новизна полягає у використанні децентралізованих систем зберігання даних, таких як блокчейн, для забезпечення незмінності записів і прозорості обробки інформації. Це особливо актуально в умовах глобального зростання обсягу цифрових державних послуг, зокрема в Україні, де проєкт «Дія» став важливим елементом цифрової трансформації. Проблеми безпеки персональних даних в державних реєстрах зумовлюють необхідність впровадження інноваційних технологій для захисту інформації [13].

Унікальність блокчейн полягає у тому, що кожен запис або зміна в системі фіксуються і зберігаються в незмінній формі, що дозволяє відстежувати всі транзакції, пов’язані з персональними даними. Це забезпечує високий рівень безпеки та мінімізує можливість маніпуляцій або несанкціонованого доступу до даних.

Обґрунтування застосування блокчейн у державних реєстрах

Традиційні централізовані державні реєстри мають низку недоліків, серед яких:

1. Єдина точка відмови — центральні системи можуть стати мішенню для хакерських атак або технічних збоїв, що може призвести до масових втрат даних.
2. Недостатня прозорість — системи часто не дозволяють чітко відстежувати всі операції з даними, що створює труднощі для забезпечення дотримання прав користувачів відповідно до Загального регламенту про захист даних (GDPR).
3. Управління згодами — сучасні системи не завжди мають можливість автоматично відслідковувати і контролювати згоди на обробку персональних даних.

Блокчейн вирішує ці проблеми завдяки таким ключовим властивостям:

1. Децентралізація — дані зберігаються на кількох вузлах мережі, що унеможливлює централізовані атаки і забезпечує стійкість до збоїв.

2. Незмінність записів — після внесення даних до блокчейн вони стають незмінними. Будь-яка спроба змінити або видалити інформацію фіксується в системі, що забезпечує максимальну цілісність даних.
3. Прозорість — кожен запис у блокчейн доступний для перегляду всіх учасників системи, що забезпечує повну прозорість обробки персональних даних.

На рис. 1 представлено схематичну архітектуру державного реєстру на основі блокчейн-технологій, яка ілюструє основні елементи системи.

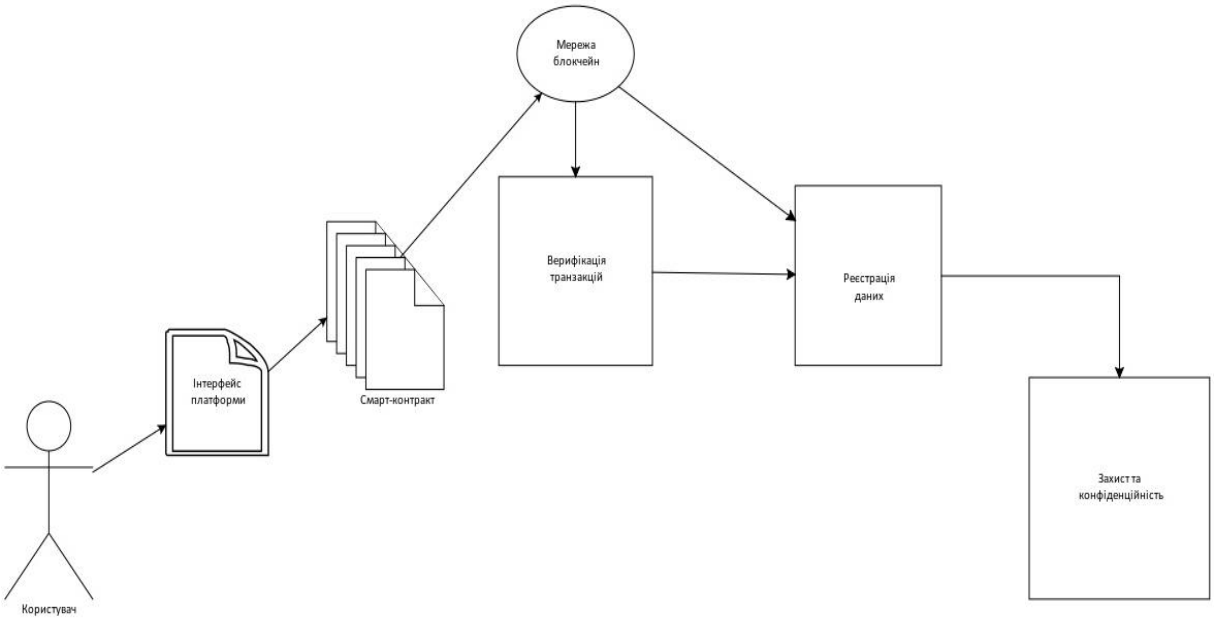

Рис. 1. Архітектура державного реєстру на основі блокчейн-технологій

Система включає децентралізовані вузли, де зберігаються дані, і смарт-контракти для автоматизації управління доступом. Кожна транзакція фіксується у блокчейн, а дані зберігаються в зашифрованому вигляді для додаткового захисту.

Використання смарт-контрактів для автоматизації управління доступом

Смарт-контракти є одним із ключових елементів блокчейн-технології, що дозволяє автоматизувати процеси обробки та управління доступом до персональних даних. Вони можуть бути використані для:

1. Автоматичного надання згоди на обробку даних або відкликання такої згоди.
2. Регулювання прав доступу до персональних даних відповідно до попередньо визначених умов.
3. Фіксації змін у даних та забезпечення їх прозорого відстеження.
4. Завдяки смарт-контрактам можна мінімізувати людські помилки і зловживання доступом до інформації, оскільки всі дії автоматично фіксуються в системі. Це забезпечує більшу надійність і підвищує відповідність вимогам GDPR.

У табл. 2 представлено порівняльний аналіз різних підходів до захисту персональних даних у державних реєстрах на основі блокчейн.

Таблиця 2

Порівняльний аналіз підходів до захисту даних у державних реєстрах на основі блокчейн

Підхід	Опис	Переваги	Недоліки
Децентралізоване зберігання	Дані розподіляються між вузлами мережі	Відсутність єдиної точки відмови, висока стійкість	Висока складність управління, витрати на підтримку
Смарт-контракти	Автоматизація управління згодами користувачів	Автоматизація, прозорість	Складність реалізації та впровадження
Псевдоанонімізація	Заміна реальних даних користувача на штучні ідентифікатори	Високий рівень конфіденційності	Можливість відновлення оригінальних даних

Аналіз показує, що децентралізоване зберігання забезпечує високу стійкість до атак і мінімізує ризики втрат даних через технічні збої. Смарт-контракти, у свою чергу, забезпечують прозорість і точність у процесах управління доступом і згодами користувачів, що дозволяє системі працювати відповідно до вимог GDPR [14].

Переваги застосування блокчейн у державних реєстрах є те, що кожна транзакція та дія з персональними даними фіксується і може бути відстежена, що дозволяє гарантувати, що всі операції відповідають законодавству. Також після внесення інформації до блокчейн будь-які спроби її зміни будуть видимі для всіх учасників, що забезпечує збереження оригінальних даних.

Смарт-контракти дозволяють автоматично регулювати згоди користувачів на обробку їхніх даних, що мінімізує ризики людських помилок, а децентралізоване зберігання даних знижує вразливість системи до атак, оскільки дані розподіляються між різними вузлами.

Проведене дослідження доводить, що блокчейн-технології можуть значно підвищити рівень безпеки та прозорості обробки персональних даних у державних реєстрах. Впровадження децентралізованих систем зберігання та смарт-контрактів дозволяє автоматизувати процеси управління згодами та доступом до даних, забезпечуючи відповідність вимогам GDPR. Прозорість і незмінність даних, забезпечені блокчейн, також підвищують рівень довіри до державних цифрових систем і мінімізують ризики втрат даних через зловживання або технічні збої.

Інтеграції смарт-контрактів для автоматизації процесів управління доступом до даних і згод користувачів у державних реєстрах

Інтеграція смарт-контрактів у платформу «Дія» відкриває нові можливості для управління персональними даними громадян. Смарт-контракти автоматизують процеси, пов’язані з наданням згоди на обробку даних, доступом до них та зберіганням інформації у державних реєстрах. Це дозволяє забезпечити не лише високий рівень безпеки, але й прозорість усіх операцій, що проводяться з даними [15].

Однією з ключових переваг смарт-контрактів є те, що вони можуть автоматично виконувати певні дії при наданні згоди користувачем. Наприклад, після підтвердження користувачем згоди на обробку його даних, смарт-контракт фіксує цей факт і надає доступ до даних тільки тим особам або системам, які мають відповідні права. У випадку,

коли користувач вирішує відкликати свою згоду, смарт-контракт автоматично обмежує доступ до цих даних, гарантуючи, що інформація більше не буде доступною для обробки. Такий підхід значно знижує ризики несанкціонованого доступу і людських помилок, що характерно для традиційних систем, де адміністратори можуть помилково надати або не відкликати доступ.

Крім того, інтеграція смарт-контрактів у «Дію» дозволяє підвищити швидкість обробки запитів на доступ до даних. У традиційних системах часто потрібно ручне втручання для надання або відміни доступу до інформації, що може призвести до затримок, особливо в умовах масштабного використання платформи. Смарт-контракти автоматизують ці процеси, що забезпечує миттєве виконання умов доступу. Це дозволяє значно прискорити роботу з даними, підвищити ефективність роботи платформи і забезпечити дотримання законодавчих норм щодо термінів обробки запитів [16].

Ще одним важливим аспектом використання смарт-контрактів є їх здатність фіксувати всі дії, що здійснюються з персональними даними, у блокчейн. Це означає, що будь-яка операція — надання доступу, відкликання згоди або редагування даних — залишається незмінною і прозорою для всіх сторін, які мають доступ до системи. Така прозорість дозволяє не лише спростити аудит, але й підвищити рівень довіри громадян до державних цифрових сервісів. Вони можуть бути впевненими, що їхні дані захищені, а всі дії з ними можна легко перевірити і відслідкувати.

Концепція полягає у впровадженні смарт-контрактів, які автоматично регулюють процеси збору, зберігання та управління доступом до персональних даних на платформі «Дія». Основна роль смарт-контрактів — це забезпечення точного виконання прав користувачів на обробку даних (згода, відкликання згоди), автоматизація цих процесів і прозоре фіксування всіх операцій у блокчейн.

На рис. 2 продемонстровано концепцію інтеграції смарт-контрактів у систему, починаючи від моменту подачі даних користувачем і до фіксації створення запису у блокчейн.

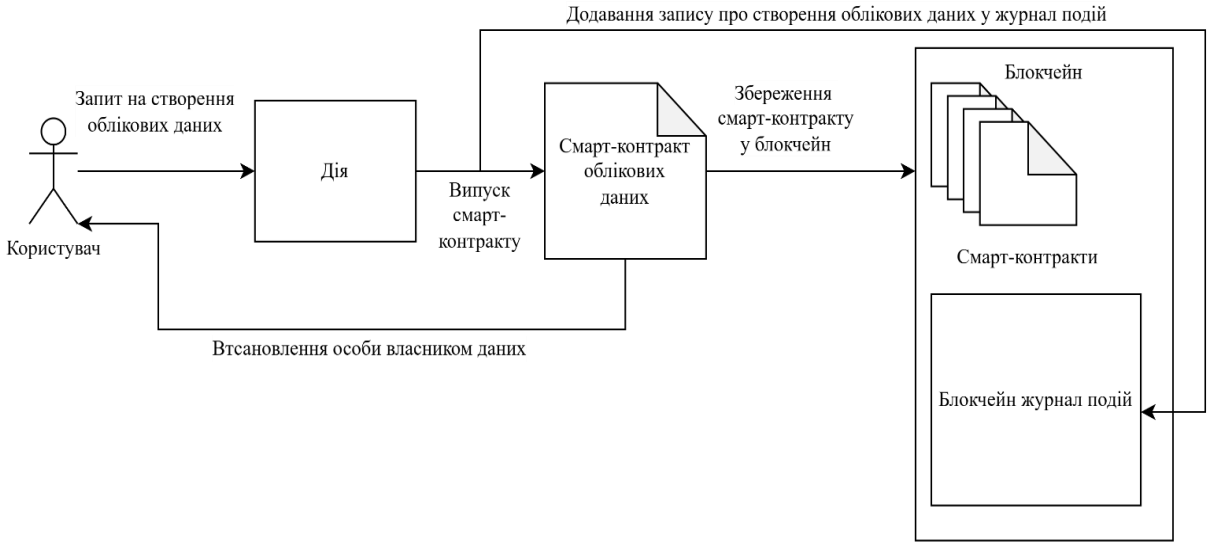

Рис. 2. Концепція інтеграції смарт-контрактів у платформу «Дія»

Алгоритм створення облікових даних користувача:

1. Користувач подає дані та запит на створення облікових даних у системі.
2. Портал «Дія» обробляє запит та випускає новий смарт-контракт і встановлює користувача власником даних.
3. Смарт-контракт зберігається в мережі блокчейн, а інформації про створення смарт-контракту зберігається у журналі подій.

Ця концепція показує чітку послідовність автоматизованих дій, яка мінімізує ризики помилок та підвищує ефективність процесів створення даних у систему.

Унікальність цієї концепції полягає в інтеграції смарт-контрактів у систему, що дозволить використовувати їх для автоматизації процесів управління доступом до персональних даних у державних реєстрах, зокрема на платформі «Дія». Концепція керування доступом буде розглянута у наступних розділах.

Важливим аспектом роботи такої системи є співставлення наявного запису в мережі і особи, тобто ідентифікація. Цю проблему можна вирішити використанням уже наявних інструментів та характеристик самої технології блокчейн: унікальність адрес у блокчейн та застосування цифрового підпису Дія [17].

Унікальність адреси у блокчейн забезпечується криптографією на еліптичних кривих, основним елементом якої є приватний ключ, доступ до має тільки його власник. Використання приватного ключа дає можливість згенерувати публічний ключ через застосування множення на еліптичних кривих, результатом якого є публічний ключ з якого формується адреса. Варто зазначити, що наявність публічного ключа у відкритому доступі не дає можливості виділити з нього приватний ключ, оскільки операції оберненої до множення на еліптичних кривих не існує, а розв’язок такої задачі перетворюється у проблему знаходження дискретного логарифму ІІ порядку, яка на цей момент є неможливою для розв’язання.

Також застосування цифрового підпису «Дії» дозволяє ідентифікувати власника, як легітимного, оскільки такий підпис дозволяє ідентифікувати особу, а його наявність може свідчити про те, що дані були створені конкретною особою.

Отже, поєднання цих двох аспектів через накладання цифрового підпису на смарт-контракт, який містить адресу користувача, як адресу власника даних, дозволяє забезпечити ідентифікацію користувача як легітимного.

Основний інноваційний аспект полягає в застосуванні децентралізованої технології блокчейн для автоматизації всіх дій, пов’язаних з обробкою згод користувачів та доступом до їхніх даних, що забезпечує прозорість, незмінність та безпеку записів.

Елементи

1. Автоматизація процесів згоди та доступу через смарт-контракти. Раніше в традиційних системах ці процеси залежали від людського втручання або складних адміністративних процедур. Інтеграція смарт-контрактів усуває необхідність ручного управління, автоматизуючи весь процес відповідно до заздалегідь встановлених умов. Це дозволяє системі функціонувати без участі адміністраторів, що підвищує швидкість і точність виконання запитів користувачів.
2. Незмінність і прозорість дій з персональними даними. Завдяки використанню блокчейн, всі дії з персональними даними фіксуються в незмінному реєстрі, що забезпечує повну прозорість операцій. Це рішення дозволяє автоматично контролювати, хто і коли мав доступ до даних, що є новим підходом для державних реєстрів і державних послуг на прикладі «Дії».

3. Підвищений рівень безпеки і конфіденційності. Традиційні централізовані системи зберігання даних схильні до ризиків, пов'язаних з людськими помилками, внутрішніми зловживаннями або кіберзагрозами. Використання смарт-контрактів у поєднанні з блокчейн дозволяє створити систему, де дані захищені на рівні програмного коду, що унеможливлює їх несанкціоновану модифікацію або доступ.
4. Відповідність вимогам GDPR. Система автоматично забезпечує виконання вимог Загального регламенту захисту даних (GDPR), зокрема прав користувачів на доступ, зміну та видалення своїх даних. Смарт-контракти забезпечують негайне реагування на будь-які зміни у згодах або доступі до даних, що гарантує відповідність міжнародним стандартам.

Традиційні системи доступу до даних залежать від людського втручання і адміністративного контролю, що робить їх вразливими до помилок і зловживань. У табл. 3 наведено порівняння традиційних систем і систем, що використовують смарт-контракти.

Таблиця 3

Порівняльний аналіз систем доступу у платформі «Дія»

Критерій	**Традиційна система доступу**	**Система на основі смарт-контрактів у «Дія»**
Прозорість	Часткова, важко відстежувати всі дії	Залежить від обраної моделі блокчейн (відкритий, приватний, гібрид)
Швидкість виконання	Залежить від людського втручання	Автоматичне виконання умов смарт-контрактів, зчитування — швидке, запис — залежить від об'єму даних
Безпека	Піддається ризикам людських помилок	Автоматичний контроль, мінімізація ризиків, відсутність центральної точки вразливості
Гнучкість управління	Потрібна постійна участь адміністратора	Смарт-контракти автоматично керують доступом

Як видно з табл. 3, смарт-контракти мають значні переваги у порівнянні з традиційними системами. Вони забезпечують повну прозорість і контроль за всіма діями з даними, автоматично виконуючи попередньо запрограмовані умови без необхідності втручання адміністратора. Крім того, система на основі смарт-контрактів є значно більш масштабованою та безпечною, що особливо важливо для платформи «Дія», яка обслуговує велику кількість користувачів та обробляє значний обсяг персональних даних.

Основні переваги системи на основі смарт-контрактів:

1. Кожна операція з даними фіксується в блокчейн, що забезпечує можливість проведення аудиту та відстеження всіх дій.
2. Смарт-контракти автоматично виконують операції, зменшуючи навантаження на адміністраторів та прискорюючи процеси доступу до даних.
3. Використання блокчейн для зберігання даних та управління доступом мінімізує ризики, пов'язані з людськими помилками та можливими зловживаннями.
4. Інтеграція смарт-контрактів дозволяє забезпечити відповідність вимогам GDPR, що є важливою умовою для захисту прав користувачів на доступ, зміну та видалення своїх даних.

Впровадження смарт-контрактів у державні реєстри, такі як платформа «Дія», може стати основою для майбутньої цифрової трансформації державних послуг. Використання децентралізованих технологій на основі блокчейн дозволяє забезпечити ефективне управління персональними даними, підвищити довіру громадян до цифрових сервісів та сприяти дотриманню міжнародних стандартів у сфері захисту даних.

Таким чином, запропонована концепція інтеграції смарт-контрактів на платформі «Дія» демонструє значний потенціал для покращення безпеки та ефективності обробки персональних даних у державних реєстрах, що є важливим кроком у розвитку сучасних інформаційних систем.

Концепція системи надання доступу

Зважаючи на те, що застосунок «Дія» має доступ до багатьох державних реєстрів, взаємодія із ними потребує чіткого розмежування доступу та логування усіх дій, які виконувалися із реєстрами. Також варто зважати на те, що портал «Дія» є централізованою системою, тому вона містить в собі загрози, які характерні для даного типу систем: наявність центральної точка вразливості, складність у відновленні втрачених даних, існування користувачів із привілеями тощо. Тому, навіть попри те, що сам застосунок «Дія» не зберігає дані про користувачів системи, а лише передає їх від реєстрів до застосунку, а далі — користувачу, існує потреба захисту даних від можливого несанкціонованого доступу чи модифікації, а також надійного збереження журналу подій системи, які можуть використовуватися одночасно для підвищення довіри користувачів до системи, дослідження історії подій в разі виявлення несанкціонованого доступу чи витоку, відлякування зловмисників від можливих зловмисних дій тощо. Це стає можливим завдяки природі технології блокчейн, зокрема таким властивостям як розподіленість та незмінність, що унеможливить видалення чи зміну записів у журналі доступу.

Також, слід зважати на те, що проєкт «Дія» працює з державними реєстрами, які не використовують технологію блокчейн, а також сам проєкт не базується на цій технології, тому застосування технології «Блокчейн» та смарт-контрактів не повинне впливати на працездатність самої системи та вміти працювати із класичними (централізованими) технологіями.

Забезпечити виконання цієї вимоги можна через застосування програмного шлюзу, який буде виконувати роль ланки, що пов’яже проєкт «Дія», державні реєстри та пропоновану систему забезпечення прозорості на основі технології «Блокчейн» та смарт-контрактів.

В цьому підході блокчейн відіграватиме ролі журналу подій та основою для системи управління даними користувача, а смарт-контракти відповідатимуть за приведення інформації, яка потраплятиме у блокчейн, до стану, в якому вони будуть відповідати необхідним критеріям.

На рис. 3 зображено модель системи.

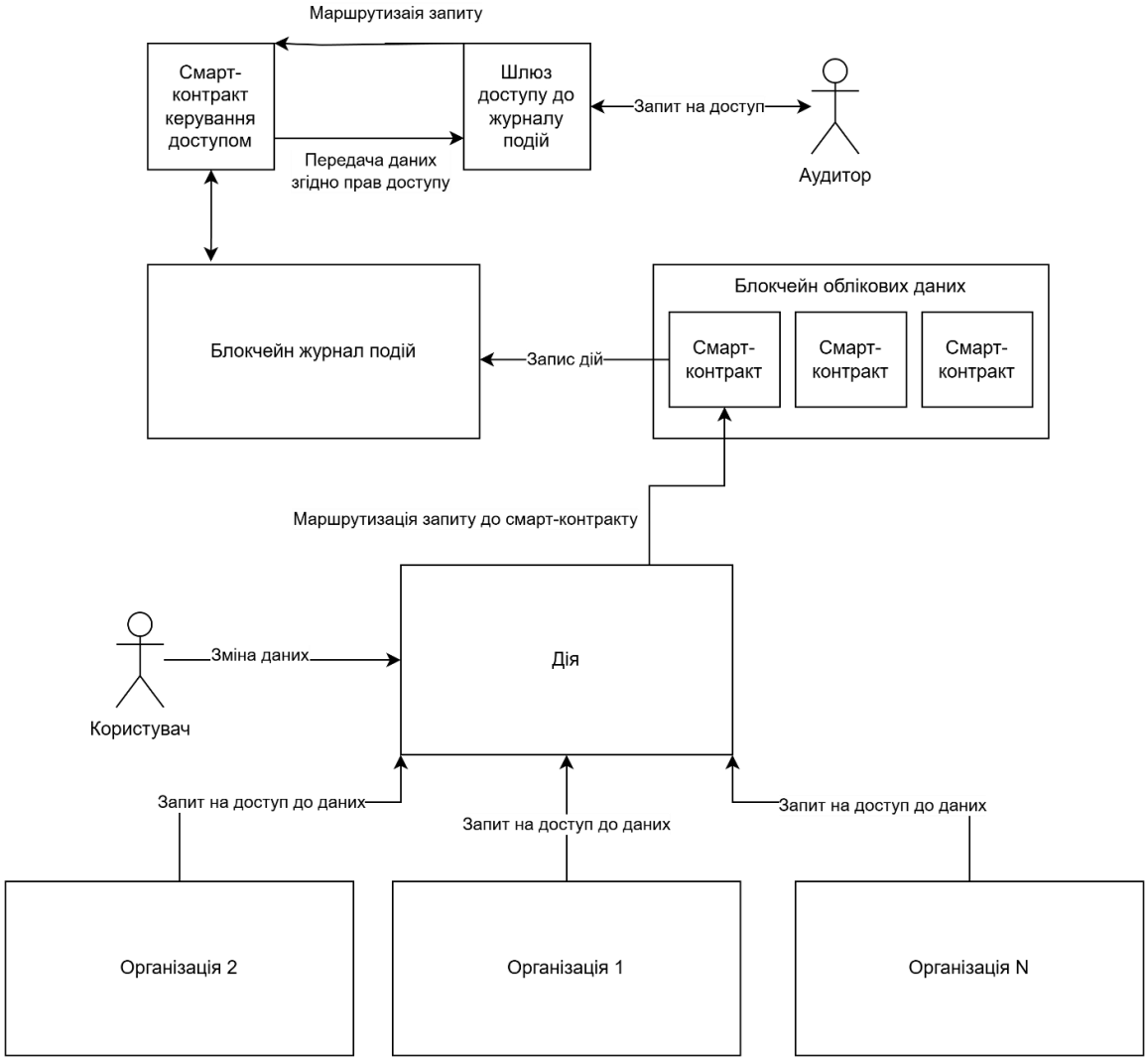

Рис. 3. Модель системи надання доступу

Основним компонентом системи, який відповідає за згаданий раніше функціонал є запис даних користувача в блокчейн. Основним методами збереження даних для завдань, які пов’язані є *on-chain* та *off-chain*. У табл. 4 наведено аналіз обох методів.

Таблиця 4

Аналіз методів збереження даних

Характеристика	On-chain	Off-chain
Місце зберегіння	Безпосередньо у блокчейн	Зберігається поза блокчей з посиланням на дані
Доступ	Безпосередньо через вузли мережі	Потребує зовнішній шлюз
Масштабування	Складне	Простіше
Цілісність даних	Висока	Залежить від обраної системи
Безпека	Висока	Залежить від обраної системи
Швидкість обробки	Нижча, оскільки запис в блокчейн об’ємних даних потребує більше часу	Вища

Прикладом збереження даних on-chain, будуть дані, які мають високу важливість наприклад: дані транзакцій, смарт-контракти, облікові записи тощо, а прикладом off-chain можуть бути NFT.

Зважаючи на дані наведені в таблиці, доцільним буде обрати варіант із on-chain збереженням, оскільки облікові дані користувачі та дозволи на роботу з ними є інформацією, яку можна розглядати як важливу. Тому для створення такого запису в мережі блокчейн доцільним є використання смарт-контракту, оскільки вони надають можливість відстежувати власника контракту та зберігати дані, які можуть змінюватися [18], на відміну від простого запису в мережі блокчейн, які є незмінними. На рис. 4 наведено концептуальну модель смарт-контракту, який є обліковим записом.

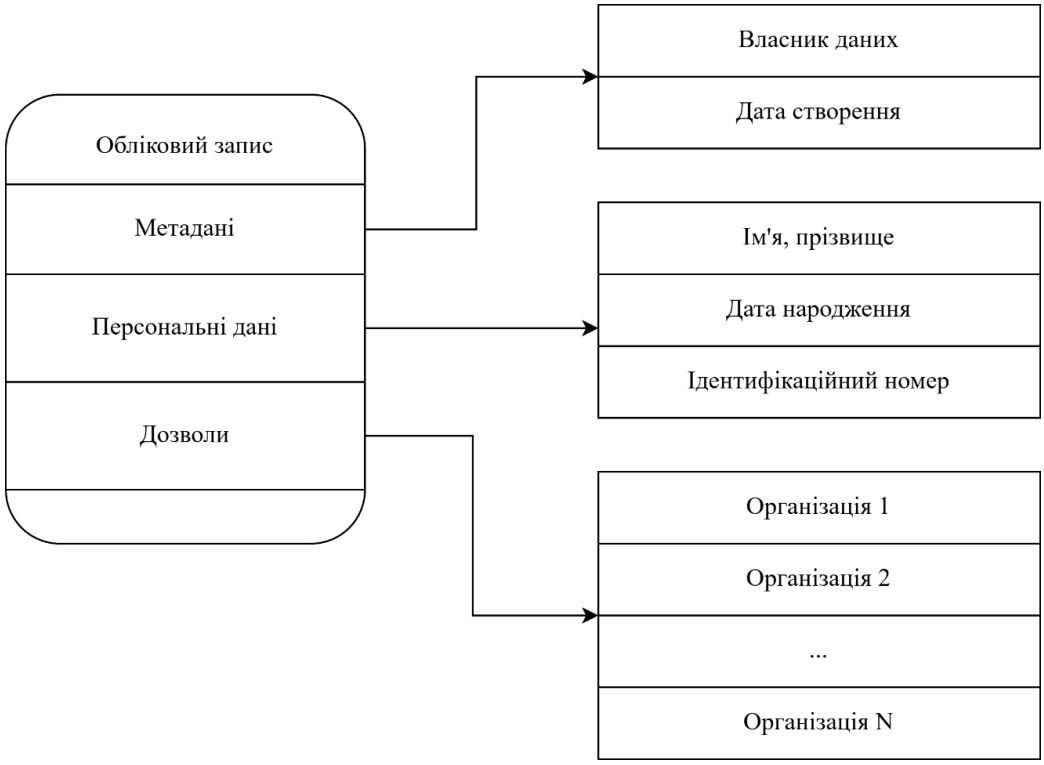

Рис. 4. Концепція смарт-контракту облікових даних

Такий підхід дозволить забезпечити існування смарт-контракту, який зможе мати змінний список із наявними дозволами для доступу до персональної інформації, наявність ідентифікатора організації в якому дозволить отримати цій організації збережену інформацію в мережі. Ба більше, факт того, що смарт-контракти є кодом, який виконується в мережі блокчейн, дозволяє розробляти їх відповідно до вимог системи, наприклад при намаганні доступу до даних створювати запис в журналі подій чи записувати в журнал подій дані про зміни тощо.

При створенні такої системи необхідно обрати тип блокчейн, який буде використовувати для побудови мережі. Для забезпечення максимальної прозорості найкращим вибором є блокчейн відкритого типу, який дає можливість будь-кому отримати доступ до даних збережених в блокчейн. Втім, робота із даними, які є персональною інформацією потребує захисту, що свідчить про необхідність використання блокчейн приватного типу. Однак вимоги, які ставляться до такої системи

спонукають до використання блокчейн гібридного типу, оскільки він дає можливість обрати які дані будуть у відкритому доступі, а які буду мати обмеження на доступ. Звісно, такий підхід може знижувати рівень децентралізації системи, але це є необхідним кроком для забезпечення можливості роботи системи у відповідності до вимог законодавства, що є необхідним для виконання.

В пропонованій концепції до відкритої частини можна віднести журнал подій, оскільки можливість вільного слідкування за запитами на доступ до інформації дозволить підвищити рівень довіри до системи, наприклад відсутність записів в журналі на інформацію від різних структур, які не потребують її для виконання своїх обов'язків може свідчити про те, що організація керується правилами, або наявність записів про блокування доступу до інформації, може свідчити про те, що система блокує спроби несанкціонованого доступу до інформації, що буде підвищувати рейтинг такої системи у користувачів. Також, такий смарт-контракт, не має записувати саму персональну інформацію у журнал подій, оскільки це не просто становитиме загрозу для користувачів системи, але й порушуватиме саме законодавство.

Алгоритм надання доступу до даних матиме такий вигляд:

1. Користувач створює обліковий запис та вносить акредитовані ідентифікатори організацій.
2. Організація намагається отримати доступ до інформації.
3. Смарт-контракт перевіряє наявність ідентифікатора організації у списку акредитованих організацій.
4. Якщо організація містить у списку акредитованих: надається доступ до інформації і створюється запис в журналі подій про успішний доступ.
5. Якщо організація відсутня в списку: доступ до інформації блокується, створюється запис в журналі про спробу несанкціонованого доступу.

Такий підхід гарантуватиме те, що будь-які дії будуть збережені в журналі подій. Також, будуть можливі для використання тільки ті можливості, які будуть запрограмовані наперед, а можливість прихованої зміни правил роботи мережі буде неможливою, оскільки такі зміни будуть відображатися у всій мережі, бо для застосування таких змін потрібно буде отримати згоду всієї мережі [19].

Алгоритм надання доступу для аудитора буде мати дещо інші кроки, оскільки він повинен працювати уже із збереженими даними, також варто зважати на те, що в якості аудитора може виступати не лише авторизований користувач з високим рівнем довіри, оскільки він буде мати доступ до більш детальних даних про транзакцію, але й будь-який користувач, який повинен отримати дані у такому вигляді, який не зможе скомпрометувати особу, яку стосуються дані в журналі подій.

Алгоритм надання доступу до журналу подій:

1. Аудитор надсилає запит на доступ до інформації журналу подій.
2. Смарт-контракт перевіряє рівень доступу аудитора та приймає рішення про доступну для аудитора інформацію
3. Інформація в обробленому вигляді надається аудитору
4. Відбувається запис у журнал подій інформація про отримання аудитором доступу.

У табл. 5 наведено приклад вибору доступної для аудитора інформації в залежності від рівня доступу. Для прикладу допускається існування користувачів 3 рівнів: I — не авторизований користувач, II — авторизований користувач, III — аудитор, обробка інформації — анонімізація.

Таблиця 5

Переваги та недоліки пропонованої системи

Рівень доступу	Анонімізована інформація	Деталізована для конкретного користувача	Детальна інформація
I	+	-	-
II	+	+	-
III	+	+	+

Такий підхід дозволить розмежувати доступ до інформації і, наприклад, будь-яка зацікавлена особа чи організація зможе отримати доступ до анонімізованої інформації, авторизований користувач зможе отримати детальний доступ до збережених записів, які стосуються його самого і доступ до решти записів у анонімізованому вигляді, а авторизований аудитор, при потребі, зможе отримати детальну інформацію із журналу подій.

Переваги та недоліки пропонованої системи наведено в табл. 6.

Таблиця 6

Переваги та недоліки пропонованої системи

Критерій	Переваги	Недоліки
Зберігання даних	Збереження даних за принципом on-chain, гарантує цілісність та незмінність	Складність у збереженні даних великого об'єму, оскільки це впливатиме на швидкодію мережі та вартість обслуговування
Доступ до даних	Можливість розмежовування прав на доступ	Зниження рівня децентралізації, оскільки існуватимуть користувачі із різними правами
Використання блокчейн гібридного типу	Можливість розмежовувати доступ до даних та мережі	Зниження рівня децентралізації
Застосування смарт-контрактів	Підвищення довіри до системи через автоматизацію процесів. Можливість редагування чи видалення даних з мережі, що дозволяє забезпечити виконання вимоги GDPR	Можлива складність в реалізації коду смарт-контрактів. Необхідність залучення фахівців високого рівня, оскільки помилки при проектуванні коду смарт-контракту можуть призвести до вразливостей та несанкціонованого доступу
Використання блокчейн журналу подій	Неможливість приховати чи видалити дані про дії у мережі. Високий рівень цілісності та достовірності інформації в журналі.	Із часом журнал подій збільшуватиметься у розмірі, що може призвести до зниження швидкодії. Неправильні налаштування логування можуть призвести до потрапляння у відкритий доступ персональних даних, які буде неможливо видалити із журналу. Неправильні налаштування логування можуть призвести до можливого приховування інформації зловмисником.

Зважаючи на переваги, які надає пропонована система, можна зробити висновок про перспективність даного підходу для побудови державних реєстрів, зокрема реєстрів із персональними даними громадян, новітнього зразка. Однак згадані недоліки потребують вирішення, оскільки вони можуть мати серйозний вплив на систему і можливість її застосування.

Одним із згаданих недоліків є складність у зберігання об'ємних даних за принципом on-chain, оскільки розмір таких даних впливає на швидкодію мережі, особливо під час збереження чи редагування даних, оскільки збільшення розміру збережених даних, відповідно й розміру самого блоку, негативно впливатиме на саму мережу. Шляхом вирішення даної проблеми може стати застосування IPFS технології, про яку згадувалося раніше. Цей принцип уже застосовується у різних платформах з продажу NFT. За аналогією, застосування IPFS дозволить винести зберігання об'ємних даних за межі блокчейн та застосувати підхід off-chain збереження даних. Таким чином розподіл даних на відносно малі, які можна зберегти у самому смарт-контракті, та відносно великі, які необхідно зберігати поза межами мережі блокчейн, дозволить знизити негативні наслідки даних відносно великого об'єму на швидкодію мережі. Однак, такий підхід може додати нових складнощі у побудові системи, оскільки такі дані необхідно не лише пов'язати із обліковими даними на основі смарт-контракту, але й забезпечити надійне збереження та транспортування даних. Саме доступність даних та безпеку транспортування технології IPFS підтримує за замовчуванням, втім вона потребує додаткових зусиль для забезпечення конфіденційності інформації [20].

Наступним недоліком системи є зниження децентралізації в системі, однак це той крок, без якого забезпечити існування такої системи в контексті відповідності GDPR та українського законодавства є неможливим. Ба більше, шлях інтеграції із Європейським Союзом спонукає до того, що вимоги GDPR повинні обов'язково виконуватися. Оскільки одними з вимог GDPR є наявність доступу лише до мінімально необхідної інформації, наявність доступу лише в осіб, які потребують такого доступу для виконання посадових обов'язків тощо не залишається іншого вибору, ніж застосувати блокчейн мережу того типу, яка дозволяє керувати доступом до мережі та даних, тобто застосуванням блокчейн мережі гібридного типу. Ще одним критерієм застосування такої мережі є те, що сарт-контракти облікових даних хоч і належать користувачам мережі, проте задля безпеки вони повинні випускатися акредитованою організацією, у цьому випадку порталом «Дія», а не самими користувачами чи будь-якою іншою не акредитованою організацією. Отже, недоліки зниження рівня децентралізації системи є такими, які необхідно прийняти, оскільки вони дозволяють забезпечувати виконання вимог законодавства.

Ще одним недоліком у запропонованій системі є висока складність у створенні смарт-контрактів високого рівня якості. Технології смарт-контрактів є відносно новою технологією, яка постійно розвивається, через що кількість фахівців високого рівня може бути обмеженою, на відміну від спеціалістів, які працюють із класичними технологіями. Окрім цього допущені помилки в алгоритмах самого смарт-контракту можуть призвести до наявності вразливостей, які можуть призвести до несанкціонованого доступу до інформації, розкриття конфіденційної інформації тощо. Шляхом вирішення цієї проблеми є пошук досвідчених розробників смарт-контрактів, детальний аналіз та розробка вимог та проектування самого смарт-контракту, а також застосування принців SSDLS [21], які включають в себе такі фази: рання ідентифікація загроз, моделювання загроз та захищений дизайн, але не обмежується ними. Ще одним можливим шляхом вирішення проблеми є збереження коду смарт-контракту у відкритому доступі (open

source) та залучення програм баг-хантингу, що дозволить залучити до перевірки коду смарт-контракту і його роботи не лише обмежений ресурс розробників, але й ширше коло ентузіастів, білих-хакерів тощо. Також додатковим ефектом такого кроку буде підвищення довіри до системи з боку користувачів, оскільки у такому випадку до тестування системи буде залучена третя сторона.

Також, одним із можливих суттєвих недоліків може стати розмір блокчейн журналу подій та можливі неправильні налаштування параметрів роботи журналу та смарт-контракту доступу до нього. Для вирішення проблеми розміру блокчейн можна скористатися різними способами, наприклад замінити збереження логів методом on-chain на метод off-chain. Також, можливим варіантом є використання «обнулення» блокчейн при досяганні повного розміру. В цьому випадку при досяганні певного розміру блокчейн тіло блоків необхідно видалити і зберегти лише дані необхідні для збереження ланцюжка блоків, тобі з нього потрібно видаляти дані транзакцій, але в мережу потрібно ввести архівні вузли, які будуть містити повну версію блокчейн, які можна вважати пасивними і які використовуються лише для збереження всієї історії й активні, які будуть працювати в мережі та продовжувати записувати дані транзакцій у нові блоки [22].

При виборі варіанту із збереженням даних методом off-chain потрібно буде вибрати технологію зберігання даних за межами блокчейн, наприклад раніше згадану технологію «IPFS», або якусь іншу технологію, яка буде забезпечувати надійне зберігання даних журналу.

Іншого недолік, себто погану чи неправильну конфігурацію роботи журналу чи прав доступу до інформації можна вирішити шляхом застосування раніше згаданих принципів SSDLC, пошуком кваліфікованих кадрів та розміщенням коду смарт-контракту у відкритий доступ.

Зважаючи на це, застосування технології блокчейн та смарт-контрактів у державних реєстрах може мати свої перспективи. Однак, обмеження, які викликані природою блокчейн технології спонукають до пошуку їх нівелювання і такі рішення часто призводять до того, що побудувати систему, яка буде використовувати лише можливості блокчейн та смарт-контрактів може виявитися складним завданням, а деякі аспекти, як вимоги законодавства, взагалі унеможливлюють застосування лише цих технологій та спонукають до пошуку компромісних рішень, як продемонстровано в можливих рішення недоліків. Наприклад, необхідність можливості для користувача видаляти дані із реєстру є непереборною перепоною для лише самого блокчейн, втім застосування технології смарт-контрактів дозволяють обійти це обмеження.

Також потрібно зважати на те, що на теперішньому етапі розвитку технології блокчейн системи можуть мати відносно обмежене застосування, втім набір їхніх характеристик та можливостей, можуть запропонувати нові підходи для збереження важливої чи критичної інформації забезпечуючи цілісність, доступність та конфіденційність інформації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Зі зростанням цифровізації суспільства та збільшенням обсягів обробки персональної інформації необхідність у безпечних і прозорих рішеннях стає критично важливою. Аналіз сучасних підходів до захисту даних показує, що централізовані системи зберігання мають низку вразливих місць, які можуть стати об’єктами

зловмисних дій, що підкреслює необхідність децентралізації та використання інноваційних технологій.

Дослідження продемонструвало, що блокчейн забезпечує високий рівень безпеки завдяки властивостям незмінності даних і прозорості транзакцій. Використання смарт-контрактів дозволяє автоматизувати управління згодами на обробку даних, тим самим підвищуючи ефективність контролю та відповідність вимогам Загального регламенту про захист даних (GDPR). Ця технологія знижує залежність від людського фактору, зменшує ймовірність помилок та унеможливлює маніпуляції даними, оскільки будь-які зміни фіксуються у блокчейн й доступні для перевірки.

Впровадження децентралізованих файлових систем, таких як IPFS, забезпечує додатковий рівень захисту та надійність зберігання даних, знижуючи ризики втрати інформації через централізовані атаки або технічні збої. Цей підхід підтримує основні принципи конфіденційності та доступності даних, що відповідає високим стандартам інформаційної безпеки.

Проведений аналіз також демонструє, що впровадження блокчейн-технологій у державних реєстрах може стати важливим кроком у посиленні довіри громадян до цифрових сервісів, адже прозорість обробки даних і чітке управління згодами сприяють підвищенню відповідальності та прозорості роботи державних структур. Запропонована концепція створює передумови для цифрової трансформації державного управління з акцентом на безпеку й ефективність.

Наукова новизна роботи полягає у комплексному підході до застосування блокчейн-технологій, включаючи інтеграцію смарт-контрактів та децентралізованих систем зберігання, що забезпечує відповідність як українському законодавству, так і вимогам GDPR. Такий підхід дозволяє не лише підвищити рівень захисту персональних даних, а й покращити загальну стійкість системи до кіберзагроз. Використання блокчейн та смарт-контрактів автоматизує процеси управління доступом, що позитивно впливає на швидкість і точність виконання запитів користувачів, а також сприяє зменшенню ризиків, пов’язаних з людським фактором.

У підсумку, впровадження блокчейн-технологій у цифрові державні платформи є стратегічно важливим кроком для забезпечення довгострокової стійкості інформаційних систем. Подальші дослідження можуть бути спрямовані на оптимізацію цих технологій та розробку нових методів захисту, що дозволять інтегрувати їх у більш широкий спектр державних сервісів. Це відкриває перспективи для розвитку державних реєстрів нового покоління, що забезпечать надійність, прозорість та захист персональних даних відповідно до найвищих стандартів сучасного цифрового суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Cabinet of Ministers of Ukraine. Digital Transformation of Ukraine: National Program “Diia”*. (б. д.). State services online | Diia. https://diia.gov.ua/en
2. *Forbes Ukraine. Investigation into a possible data leak in the “Diia” app.* (б. д.). https://forbes.ua/news/rosiyski-khakeri-zayavili-pro-zlam-kmda-motor-sichi-i-dii-24022023-12156
3. Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. *Springer International Publishing*. https://doi.org/10.1007/978-3-319-57959-7
4. Wright, A., & De Filippi, P. (2018). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Harvard Law Review, 18*, 593–625. https://doi.org/10.2139/ssrn.2580664
5. Custers, B., Ursic, H., & Schermer, B. (2019). EU Personal Data Protection in Policy and Practice. *European Law Journal, 25(3),* 341–360. https://doi.org/10.1111/eulj.12305

6. Kivimaa, T., & MacDonald, M. (2021). Blockchain's Role in Data Privacy Protection: A Comprehensive Overview. *Journal of Information Security, 10(4),* 289–306. https://doi.org/10.4236/jis.2021.104017
7. Benet, J. (2017). *IPFS - Content Addressed, Versioned, P2P File System*. arXiv preprint.
8. Goonasekera, J., Fernando, S., & Jayasuriya, S. (2020). Integration of Blockchain and IPFS for Secure and Transparent Data Management. *International Journal of Network Security, 22(2),* 239–250. https://doi.org/10.6633/IJNS.202003_22(2).09
9. Lundkvist, C., & Kravchenko, S. (2020). Securing Digital Identities: The Role of Blockchain in Data Integrity. *Digital Transformation Journal, 11(5),* 140–154. https://doi.org/10.18356/4024c4eb-en
10. Zhang, Y., & Lee, G. (2021). Privacy-Preserving Techniques for Data Security: Challenges and Solutions. *Cybersecurity Science Review, 7(2),* 45–62. https://doi.org/10.1109/CyberSecRev.2021.00007
11. Ghosh, A., & Dutta, S. (2021). Blockchain and GDPR: Synergies and Tensions. *Journal of European Law Studies, 9(3),* 125–141. https://doi.org/10.2139/ssrn.3348065
12. Poberezhnyk, V., Balatska, V., & Opirskyy, I. (2023). Development of the Learning Management System Concept based on Blockchain Technology. In: *Cybersecurity Providing in Information and Telecommunication Systems II, Vol. 3550,* 143–156.
13. Custers, B., Ursic, H., & Schermer, B. (2019). EU Personal Data Protection in Policy and Practice. *European Law Journal, 25(3),* 341–360. https://doi.org/10.1111/eulj.12305
14. Balatska, V., Poberezhnyk, V., Petriv, P., & Opirskyy, I. (2024). Blockchain Application Concept in SSO Technology Context. In: *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3654,* 38–49.
15. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36,* 55–81. https://doi.org/10.1016/j.tele.2018.11.006
16. Dinh, T. T. A., et al. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering, 30(7),* 1366–1385. https://doi.org/10.1109/TKDE.2017.2781227
17. *Frequently asked questions about Diia ID.* (б. д.). State services online | Diia. https://ca.diia.gov.ua/faq_diia_id
18. *Ethereum. Anatomy of a Smart Contract.* (б. д.). https://ethereum.org/en/developers/docs/smart-contracts/anatomy/
19. Hussein, Z., Salama, M. A. & El-Rahman, S. A. (2023). Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. *Cybersecurity 6, 30.* https://doi.org/10.1186/s42400-023-00163-y
20. *Privacy and encryption.* (б. д.). https://docs.ipfs.tech/concepts/privacy-and-encryption/#what-s-public-on-ipfs
21. *What is the SSDL (Secure Software Development Life Cycle)?* (б. д.). HackerOne. https://www.hackerone.com/knowledge-center/what-ssdlc-secure-software-development-life-cycle
22. Poberezhnyk, V., & Opirskyy, I. (2023). Developing of blockchain method in message interchange systems. In: *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3421,* 148–157.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Valeriia Balatska
Cybersecurity Department Postgraduate
Lviv Polytechnic National University, Lviv, Ukraine
Lecturer at the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID: 0000-0002-6262-6792
valeriia.s.balatska@lpnu.ua, lera31505@gmail.com

Vasyl Poberezhnyk
Cybersecurity Department Postgraduate
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-7523-2557
vasyl.poberezhnyk@gmail.com

THE CONCEPT OF APPLYING BLOCKCHAIN TECHNOLOGIES TO INCREASE THE SECURITY OF PERSONAL DATA OF THE "DIYA" PLATFORM: COMPLIANCE WITH THE REQUIREMENTS OF THE GDPR AND UKRAINIAN LEGISLATION

Abstract. With the development of digital government services and the "Diya" project in Ukraine, the issue of personal data protection is becoming one of the most important challenges, especially in the context of compliance with the requirements of the General Data Protection Regulation (GDPR) and national legislation. Modern digital solutions must ensure transparency, security and compliance with legal norms regarding the processing and storage of citizens' personal information. This study proposes the integration of blockchain technologies into the "Diya" project as an effective means of increasing the confidentiality and security of personal data. The use of blockchain ensures the immutability and transparency of data in state registers, allowing to track all operations with information and record each request for access. This is especially important for compliance with the principles of the GDPR, such as transparency of data processing, the right to information and the right to be forgotten. The proposed system includes key technological components, such as smart contracts to automate the management of consent to data processing and the delimitation of access to them. Smart contracts allow for automatic and secure execution of agreements between the user and the system, significantly reducing the risks of human error or abuse. In addition, the use of the decentralized IPFS file system guarantees reliable file storage, which eliminates the possibility of centralized attacks or information loss. Data protection methods such as masking, pseudo-anonymization and perturbation help reduce the risk of unauthorized disclosure of information even in the event of a data leak. This is especially relevant for state registers containing sensitive information about citizens, and provides a high level of protection in accordance with GDPR standards. The implementation of this concept within the framework of the "Diya" project will not only increase citizens' trust in state digital services, but also create conditions for Ukraine's integration into the European legal space in terms of personal data protection. The proposed solution can become the foundation for the further development of state registers and other digital services focused on data protection within the framework of the latest technologies. The purpose of the research is to analyze and develop an innovative system for protecting personal data in state registers of Ukraine based on blockchain technologies, which meets the requirements of GDPR and national legislation. This approach will ensure reliability, security and transparency of data processing, which will contribute to the digital transformation of public administration.

Keywords: personal data protection; blockchain; "Diya"; smart contracts; GDPR; Ukrainian legislation; IPFS; decentralized systems.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Cabinet of Ministers of Ukraine. Digital Transformation of Ukraine: National Program "Diia".* (n. d.). State services online | Diia. https://diia.gov.ua/en
2. *Forbes Ukraine. Investigation into a possible data leak in the "Diia" app.* (n. d.). https://forbes.ua/news/rosiyski-khakeri-zayavili-pro-zlam-kmda-motor-sichi-i-dii-24022023-12156
3. Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. *Springer International Publishing*. https://doi.org/10.1007/978-3-319-57959-7
4. Wright, A., & De Filippi, P. (2018). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Harvard Law Review, 18*, 593–625. https://doi.org/10.2139/ssrn.2580664
5. Custers, B., Ursic, H., & Schermer, B. (2019). EU Personal Data Protection in Policy and Practice. *European Law Journal, 25(3),* 341–360. https://doi.org/10.1111/eulj.12305
6. Kivimaa, T., & MacDonald, M. (2021). Blockchain's Role in Data Privacy Protection: A Comprehensive Overview. *Journal of Information Security, 10(4),* 289–306. https://doi.org/10.4236/jis.2021.104017
7. Benet, J. (2017). *IPFS - Content Addressed, Versioned, P2P File System*. arXiv preprint.
8. Goonasekera, J., Fernando, S., & Jayasuriya, S. (2020). Integration of Blockchain and IPFS for Secure and Transparent Data Management. *International Journal of Network Security, 22(2),* 239–250. https://doi.org/10.6633/IJNS.202003_22(2).09
9. Lundkvist, C., & Kravchenko, S. (2020). Securing Digital Identities: The Role of Blockchain in Data Integrity. *Digital Transformation Journal, 11(5),* 140–154. https://doi.org/10.18356/4024c4eb-en
10. Zhang, Y., & Lee, G. (2021). Privacy-Preserving Techniques for Data Security: Challenges and Solutions. *Cybersecurity Science Review, 7(2),* 45–62. https://doi.org/10.1109/CyberSecRev.2021.00007
11. Ghosh, A., & Dutta, S. (2021). Blockchain and GDPR: Synergies and Tensions. *Journal of European Law Studies, 9(3),* 125–141. https://doi.org/10.2139/ssrn.3348065
12. Poberezhnyk, V., Balatska, V., & Opirskyy, I. (2023). Development of the Learning Management System Concept based on Blockchain Technology. In: *Cybersecurity Providing in Information and Telecommunication Systems II, Vol. 3550*, 143–156.
13. Custers, B., Ursic, H., & Schermer, B. (2019). EU Personal Data Protection in Policy and Practice. *European Law Journal, 25(3),* 341–360. https://doi.org/10.1111/eulj.12305
14. Balatska, V., Poberezhnyk, V., Petriv, P., & Opirskyy, I. (2024). Blockchain Application Concept in SSO Technology Context. In: *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3654*, 38–49.
15. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36,* 55–81. https://doi.org/10.1016/j.tele.2018.11.006
16. Dinh, T. T. A., et al. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering, 30(7),* 1366–1385. https://doi.org/10.1109/TKDE.2017.2781227
17. *Frequently asked questions about Diia ID.* (n. d.). State services online | Diia. https://ca.diia.gov.ua/faq_diia_id
18. *Ethereum. Anatomy of a Smart Contract.* (n. d.). https://ethereum.org/en/developers/docs/smart-contracts/anatomy/
19. Hussein, Z., Salama, M. A. & El-Rahman, S. A. (2023). Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. *Cybersecurity 6, 30.* https://doi.org/10.1186/s42400-023-00163-y
20. *Privacy and encryption.* (n. d.). https://docs.ipfs.tech/concepts/privacy-and-encryption/#what-s-public-on-ipfs
21. *What is the SSDL (Secure Software Development Life Cycle)?* (n. d.). HackerOne. https://www.hackerone.com/knowledge-center/what-ssdlc-secure-software-development-life-cycle
22. Poberezhnyk, V., & Opirskyy, I. (2023). Developing of blockchain method in message interchange systems. In: *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3421,* 148–157.