КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.875
УДК 004.056

Балацька Валерія Сергіївна
старший викладач кафедри управління інформаційною безпекою,
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID ID: 0000-0002-6262-6792
v.balatska@ldubgd.edu.ua

Дмитрів Назарій Степанович
аспірант
Приватний вищий навчальний заклад «Європейський університет», Київ, Україна
ORCID ID: 0009-0007-0326-3622
nazarii.dmytriv@gmail.com

МІЖОРГАНІЗАЦІЙНИЙ ОБМІН КОНФІДЕНЦІЙНИМИ ПЕРСОНАЛЬНИМИ ДАНИМИ НА ОСНОВІ ДОЗВІЛЬНОГО БЛОКЧЕЙН

Анотація. У статті досліджено проблему забезпечення конфіденційного обміну персональними даними в міжорганізаційних інформаційних системах в умовах зростаючої цифрової взаємодії суб'єктів публічного та приватного секторів. Констатовано, що централізовані моделі обробки та обміну персональними даними не забезпечують належного рівня захисту інформації від несанкціонованого доступу, підробки транзакцій, а також не гарантують необхідного рівня прозорості щодо операцій над даними. Ці обмеження унеможливлюють повноцінне дотримання регуляторних вимог, зокрема положень Загального регламенту про захист даних (GDPR), стандартів ISO/IEC 27001 та 27701, а також положень національного законодавства у сфері захисту інформації. У межах дослідження обґрунтовано доцільність застосування дозвільного блокчейн як архітектурної основи для реалізації захищеного, децентралізованого обміну персональними даними з гарантованим контролем доступу, аудиту транзакцій і незмінності записів. Запропоновано концептуальну модель інформаційної системи, що передбачає використання смарт-контрактів для управління згодою суб'єктів даних, розмежування прав доступу, а також інтеграцію децентралізованої файлової системи IPFS для забезпечення стійкого зберігання даних. Додатково у моделі передбачено застосування криптографічних механізмів з нульовим розголошенням (Zero Knowledge Proof) та поведінкових критеріїв верифікації транзакцій. Окрему увагу приділено аналізу ризиків, пов'язаних з обробкою персональних даних у міжорганізаційному середовищі, а також використанню допоміжних засобів захисту — маскування, псевдонімізації, пертурбації — для зниження потенційних втрат у разі витоку інформації. Визначено перелік технічних та організаційних критеріїв відповідності системи вимогам міжнародних і національних стандартів у сфері інформаційної безпеки. Метою дослідження є проєктування архітектурної моделі міжорганізаційного обміну персональними даними на основі дозвільного блокчейн, що забезпечує конфіденційність, цілісність, контрольований доступ і відповідність нормативно-правовим вимогам у сфері захисту інформації.

Ключові слова: персональні дані; міжорганізаційний обмін; дозвільний блокчейн; смарт-контракти; IPFS; конфіденційність; Zero Knowledge Proof; криптографічний захист; управління згодою; нормативно-правові вимоги; GDPR.

ВСТУП

Упродовж останнього десятиліття світова тенденція до цифрової трансформації державного управління, охорони здоров'я, освіти, фінансового та банківського секторів зумовила інтенсивне зростання обсягів персональних даних, які обробляються та передаються між організаціями. Україна, слідуючи європейським інтеграційним курсом, активізувала впровадження електронних державних сервісів — зокрема, екосистеми

«Дія» [1], платформи електронного здоров'я (eHealth), державного земельного кадастру, автоматизованих податкових і соціальних реєстрів. Функціонування таких систем передбачає регулярний міжорганізаційний обмін конфіденційними персональними даними громадян, що потребує гарантованої безпеки, прозорості, підзвітності та відповідності міжнародним стандартам.

Разом із тим, переважна більшість інформаційних систем, які оперують персональними даними, ґрунтуються на централізованих архітектурах. Це породжує низку критичних проблем: зосередження даних у єдиній точці контролю призводить до високих ризиків витоку інформації, порушення конфіденційності, несанкціонованого доступу та цілеспрямованих атак. Крім того, централізовані моделі ускладнюють реалізацію принципів прозорості та відслідковуваності, визначених Загальним регламентом про захист даних (GDPR), таких як право на доступ до інформації, право на обмеження обробки, право на видалення (право на забуття), а також обов'язок реєстрації транзакцій доступу [2].

Іншою суттєвою проблемою є відсутність єдиного механізму довіри між суб'єктами обміну, що ускладнює розмежування прав доступу, управління згодами на обробку даних та фіксацію взаємодії в правовому полі. В існуючих моделях контроль часто зосереджено на адміністраторах баз даних або власниках платформи, що відкриває широкі можливості для зловживань, несанкціонованої модифікації записів або відсутності належного аудиту.

У відповідь на ці виклики зростає інтерес до застосування децентралізованих технологій, зокрема дозвільного блокчейн, як інструменту побудови довірених, верифікованих середовищ обміну інформацією. На відміну від публічних блокчейн-мереж, дозвільний (permissioned) блокчейн функціонує у межах визначеного кола учасників, які автентифіковані та мають рольову модель доступу. Це дозволяє не лише зберігати дані в незмінному вигляді, а й забезпечити механізм фіксації транзакцій, контроль доступу на основі смарт-контрактів, управління згодою користувача, а також розмежування прав доступу за контекстними або поведінковими ознаками [3].

До архітектурних переваг такого підходу можна віднести можливість інтеграції децентралізованих систем зберігання даних (зокрема IPFS), застосування доказів з нульовим розголошенням (Zero Knowledge Proof) для верифікації без розкриття змісту даних, а також вбудовані криптографічні механізми для шифрування, псевдонімізації, маскування або пертурбації персональних записів.

Особливої уваги набуває і нормативний контекст. В Україні з 2025 року набрав чинності Закон №4336-IX, який регламентує обов'язкове впровадження комплексної системи захисту інформації (КСЗІ) класу АС-1 для інформаційних ресурсів, що обробляють персональні дані у державному секторі. Це означає, що всі організації, залучені до міжреєстрового або міжвідомчого обміну, повинні не лише впровадити технічні засоби захисту, а й обґрунтувати архітектурну модель, яка виключає ризики компрометації даних.

У цьому контексті постає необхідність науково обґрунтованої моделі міжорганізаційного обміну персональними даними, що поєднує вимоги конфіденційності, криптографічного захисту, контрольованого доступу та відповідності законодавству.

Метою дослідження є проєктування архітектурної моделі міжорганізаційного обміну персональними даними на основі дозвільного блокчейн, що забезпечує конфіденційність, цілісність, аудит доступу та відповідність нормативно-правовим вимогам у сфері захисту інформації.

Постановка проблеми. У цифровому середовищі міжорганізаційний обмін персональними даними є критично важливим компонентом функціонування державних

сервісів, зокрема електронного врядування, систем охорони здоров'я, соціального захисту, освіти та фінансів. Цей обмін дедалі частіше здійснюється через інтегровані інформаційні системи, які, втім, здебільшого побудовані за централізованою архітектурою. Така модель зосереджує обробку та зберігання даних у межах окремих платформ або реєстрів, що формує технічну та організаційну залежність від окремих адміністраторів систем.

Централізація породжує низку системних обмежень у контексті забезпечення конфіденційності, прозорості й довіри до механізмів обробки інформації. Зокрема, в таких моделях ускладнюється реалізація аудиту доступу до персональних даних, відсутній механізм технічно гарантованого управління згодою користувача, а самі транзакції над даними залишаються непрозорими для зацікавлених сторін. Усе це суперечить основним принципам сучасного регулювання обігу персональних даних, зокрема вимогам Загального регламенту про захист даних (GDPR) щодо інформування, обмеження, відкликання згоди та права на забуття.

Крім того, централізовані системи є вразливими з точки зору інформаційної безпеки, адже наявність єдиного центру зберігання й обробки даних створює потенційну точку компрометації, яка може бути використана як зовнішніми зловмисниками, так і внутрішніми суб'єктами з розширеними правами доступу. В умовах активного міжвідомчого обміну такими даними відсутність механізму взаємного підтвердження достовірності, а також недостатня сумісність систем доступу, лише поглиблюють проблему.

На цьому тлі особливої актуальності набуває необхідність у розробці таких архітектурних рішень, які здатні забезпечити не лише технічний захист інформації, але й юридично значущий механізм підтвердження кожної операції, контроль за доступом і управління згідно з волею суб'єкта даних. Це вимагає переходу до моделей, що вбудовують довіру в саму структуру системи, зокрема через децентралізацію, криптографічний захист, автоматизовані механізми контролю та фіксації транзакцій.

Таким чином, постає проблема проєктування міжорганізаційної системи обміну персональними даними, яка відповідала б вимогам сучасного правового поля, забезпечувала захист інформації від компрометації, реалізовувала принципи прозорості та підзвітності, а також дозволяла гнучке й контрольоване управління доступом. Одним з перспективних напрямів розв'язання цієї проблеми є впровадження дозвільного блокчейн як базової архітектурної основи, що поєднує децентралізовану логіку обміну з криптографічним контролем, вбудованим аудитом та можливістю масштабованого впровадження у державні інформаційні платформи.

Аналіз останніх досліджень і публікацій. Проблематика захисту персональних даних у цифровому середовищі в умовах зростання міжорганізаційного інформаційного обміну активно досліджується у світовій та вітчизняній науковій спільноті. Сучасні публікації свідчать про зростаючий інтерес до застосування децентралізованих технологій, зокрема блокчейн, для гарантування конфіденційності, цілісності та підзвітності під час обробки персональної інформації. Блокчейн розглядається як технологія, здатна забезпечити незмінність транзакцій і прозорість взаємодії між учасниками без залучення центрального посередника.

Окрему увагу приділено моделі дозвільного блокчейн, яка передбачає участь лише верифікованих користувачів та забезпечує контроль доступу, аудит транзакцій, ідентифікацію операцій над даними. Такі моделі поступово знаходять застосування в публічному адмініструванні, охороні здоров'я, системах цифрової ідентифікації, управлінні земельними, фінансовими та соціальними реєстрами. Їх перевагою є можливість побудови довіреної інфраструктури для обміну даними, де кожна дія фіксується та верифікується без можливості ретроспективної модифікації [4].

Суттєвий внесок у дослідження захисту персональних даних на основі блокчейн-технологій зроблено в напрямі застосування смарт-контрактів. Вони розглядаються як механізми автоматизації управління згодою користувачів на обробку даних, реалізації політик доступу, а також забезпечення дотримання регламентованих процедур відповідно до чинного законодавства [5]. Смарт-контракти дозволяють мінімізувати вплив людського чинника, виключити суб'єктивне втручання та забезпечити юридично значущу фіксацію дій над інформацією.

Ще одним напрямом, що активно розробляється, є впровадження децентралізованих систем зберігання даних. Зокрема, технологія IPFS (InterPlanetary File System) дозволяє організувати стійке, розподілене та масштабоване збереження інформації, яке не залежить від окремих серверів [6]. Це забезпечує цілісність і доступність даних навіть у випадку пошкодження окремих вузлів, а також створює умови для реалізації принципів прозорості, сумісності та відстежуваності, закріплених у сучасному регуляторному полі.

У сфері забезпечення конфіденційності дослідники зосереджуються на застосуванні криптографічних механізмів, зокрема доказів з нульовим розголошенням (Zero Knowledge Proof). Такі механізми дозволяють підтверджувати достовірність фактів або операцій без необхідності розкриття самих даних, що є особливо важливим в умовах обмеженої довіри між суб'єктами обміну [7]. Також розглядаються засоби маскування, псевдонімізації та пертурбації, які забезпечують додатковий рівень приватності при обробці персональної інформації [8].

З нормативної точки зору, визначальними документами залишаються Загальний регламент про захист даних (GDPR), міжнародні стандарти ISO/IEC 27001 і ISO/IEC 27701, а також національне законодавство, зокрема Закон України № 4336-IX, який визначає обов'язковість впровадження КСЗІ у державних інформаційних системах.

У сучасних дослідженнях підкреслюється, що дотримання цих норм вимагає інтеграції технологічних, організаційних та процедурних складових безпеки на всіх рівнях обробки даних. Водночас у проаналізованих джерелах спостерігається фрагментарність підходів — більшість публікацій зосереджена лише на окремих аспектах захисту, таких як зберігання або ідентифікація, без урахування повного циклу обміну та без побудови інтегрованої архітектури міжорганізаційної взаємодії. Це актуалізує необхідність комплексного підходу, який поєднує технології блокчейн, засоби децентралізованого зберігання, смарт-контракти та криптографічні протоколи в межах єдиної моделі з відповідністю чинним регуляторним вимогам.

Мета статті. Метою статті є розроблення моделі міжорганізаційного обміну конфіденційними персональними даними на основі дозвільного блокчейн з урахуванням вимог безпеки, прозорості та нормативно-правового регулювання.

Основними завданнями статті виступають:

1. Аналіз сучасних проблем захисту персональних даних в умовах міжорганізаційного інформаційного обміну в цифровому середовищі.
2. Дослідження потенціалу дозвільного блокчейн як інструменту забезпечення прозорості, цілісності та контрольованого доступу до персональних даних.
3. Обґрунтування доцільності застосування смарт-контрактів для управління згодами, перевірки прав доступу та автоматизованої фіксації транзакцій.
4. Оцінка ролі децентралізованих систем зберігання, зокрема IPFS, у побудові надійної інфраструктури для обміну чутливою інформацією між організаціями.
5. Формулювання моделі безпечного міжорганізаційного обміну конфіденційними персональними даними з урахуванням вимог GDPR, ISO/IEC 27701 та українського законодавства.

Реалізація запропонованого підходу дозволяє сформувати цифрове середовище, в якому кожна транзакція є заздалегідь регламентованою, верифікованою та підзвітною, що забезпечує високий рівень довіри між організаціями, мінімізує ризики витоку даних і сприяє дотриманню міжнародних стандартів захисту інформації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Аналіз сучасних проблем захисту персональних даних в умовах міжорганізаційного інформаційного обміну в цифровому середовищі

Сучасна цифровізація публічного сектору зумовлює необхідність швидкого, ефективного та безпечного обміну персональними даними між державними установами, комерційними організаціями, органами місцевого самоврядування та іншими уповноваженими суб'єктами. Водночас із розширенням електронних сервісів (зокрема, таких як «Дія», eHealth, реєстрові сервіси Міністерства юстиції України) загострюється проблема гарантування захисту персональної інформації в умовах зростаючої міжорганізаційної взаємодії [9].

Одним із ключових викликів є забезпечення достовірності, цілісності та конфіденційності персональних даних при їх передачі між окремими суб'єктами, що функціонують у різних нормативно-правових, технологічних та організаційних середовищах. У багатьох випадках передачі даних відбуваються через централізовані шлюзи або API без повної перевірки автентичності джерела або правомірності запиту. Такий підхід створює потенційні вектори атак, пов'язані з несанкціонованим доступом, підробкою транзакцій, перехопленням даних або зловживанням службовими повноваженнями.

Крім технічних ризиків, виявляються й організаційні слабкості, серед яких:

- відсутність єдиних політик управління згодою користувачів;
- слабка регламентація міжвідомчого доступу до даних;
- обмежені можливості аудитування дій операторів у реальному часі.

У контексті міжнародного досвіду, значною проблемою залишається невідповідність національних практик вимогам Регламенту (ЄС) 2016/679 (GDPR), що визначає принципи законності, прозорості, обмеженості мети, мінімізації даних і забезпечення прав суб'єкта. Брак механізмів незалежного контролю, журналювання доступу й ефективного відкликання згоди ускладнює дотримання цих принципів [10].

Зі зростанням масштабів цифрового урядування та популярністю платформ, які об'єднують кілька функцій (ідентифікація, реєстрація, надання послуг), виникає небезпека накопичення надмірної кількості даних у точках концентрації, що суперечить принципам «data minimization» і «purpose limitation». У разі компрометації такого вузла наслідки можуть мати катастрофічний характер.

Особливо вразливими залишаються процеси делегування прав доступу третім сторонам, коли між організаціями відсутній сталий механізм верифікації транзакції — чи мав той чи інший суб'єкт право на виконання конкретної дії з даними в конкретний час. Це створює «сліпі зони довіри», які не завжди можна виявити класичними засобами контролю доступу (RBAC, ABAC).

Окремим вектором ризику виступає відсутність механізмів фіксації транзакцій доступу до персональних даних у незмінному вигляді. У разі суперечок або розслідувань, організації часто не можуть надати незалежний доказ факту доступу чи обробки. Саме в цьому контексті актуальності набувають дозвільні блокчейн-рішення, здатні забезпечити як криптографічне підтвердження транзакції, так і автоматизоване управління правами доступу з використанням смарт-контрактів.

Таким чином, існує системна проблема відсутності інтегрованої, прозорої та захищеної моделі обміну персональними даними між організаціями. Вона поєднує нормативні, технічні та архітектурні аспекти й вимагає перегляду підходів до організації цифрових міжорганізаційних платформ з урахуванням принципів захисту даних на етапі проєктування (Privacy by Design) [11].

Дослідження потенціалу дозвільного блокчейн як інструменту забезпечення прозорості, цілісності та контрольованого доступу до персональних даних

У контексті цифрової трансформації державного управління зростає потреба у створенні архітектур, що дозволяють гарантувати прозорість і довіру при обміні чутливою інформацією між організаціями. Одним із найперспективніших технологічних підходів у цьому напрямі визнано дозвільний блокчейн (permissioned blockchain), який на відміну від публічних мереж забезпечує обмежене коло учасників, контроль доступу, а також вищий рівень відповідності нормативно-правовим вимогам [12].

Основними перевагами дозвільного блокчейн як інструменту захисту персональних даних є:

- Контрольована участь: доступ до мережі мають лише авторизовані суб'єкти (державні установи, реєстратори, надавачі послуг), що дозволяє централізовано регламентувати правила доступу, не втрачаючи децентралізованих властивостей;
- Прозорість транзакцій: всі транзакції записуються у розподілений журнал і можуть бути верифіковані іншими вузлами, що виключає можливість несанкціонованих змін;
- Незмінність даних: завдяки механізмам консенсусу (наприклад, Raft, PBFT) дані стають криптографічно зафіксованими та неможливими до модифікації без згоди мережі;
- Аудит та підзвітність: кожна дія (внесення, зчитування, запит доступу) фіксується з цифровим слідом, що дозволяє будувати прозорі механізми аудиту.

Серед наявних рішень найбільше поширення для реалізації дозвільного блокчейн в державному секторі здобула платформа Hyperledger Fabric, що підтримує:

- модульну архітектуру;
- конфігуровані канали доступу до даних;
- інтеграцію зі смарт-контрактами (chaincode), написаними мовами Go або JavaScript;
- можливість створення окремих політик конфіденційності для груп учасників (Private Data Collections).

На рис. 1 представлено архітектуру міжорганізаційного обміну персональними даними, реалізовану за допомогою дозвільного блокчейн Hyperledger Fabric із використанням peer-вузлів, смарт-контрактів, реєстру транзакцій, IPFS-сховища та модулів перевірки та згоди користувача.

Користувач формує запит, який надходить до Установи А. Там він обробляється смарт-контрактом, який перевіряє наявність згоди користувача через відповідний модуль. У разі успішної верифікації транзакція фіксується у централізованому реєстрі транзакцій, копія якого розподіляється серед peer-вузлів мережі через механізм синхронізації стану. Дані, що мають великий обсяг або не підлягають зберіганню у Ledger, розміщуються в IPFS з посиланням у блокчейн. Установа В, яка отримує доступ до запису, перевіряє транзакцію за допомогою власного смарт-контракту та модуля перевірки.

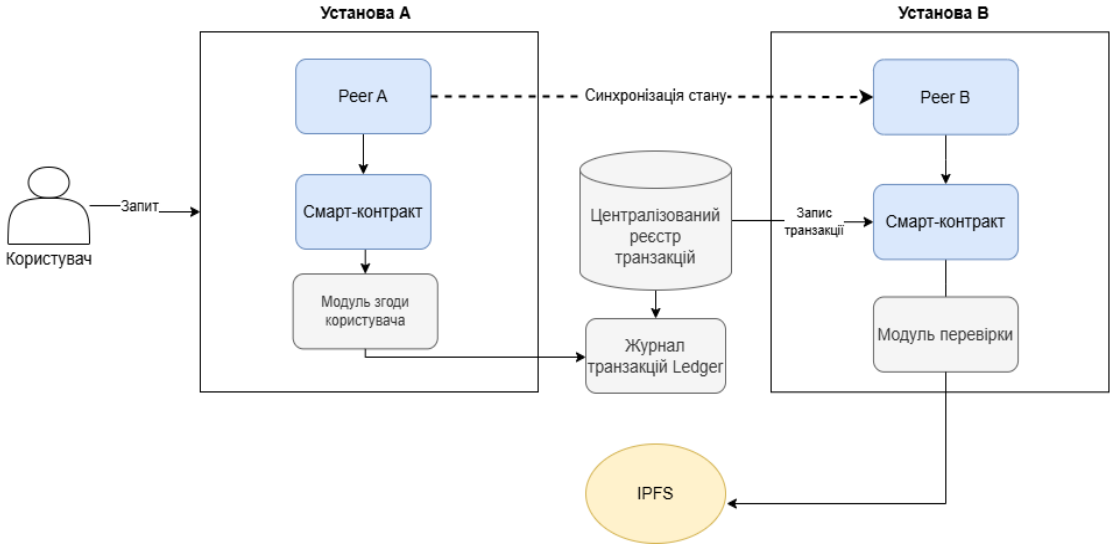

Рис. 1. Архітектура міжорганізаційного обміну персональними даними з використанням дозвільного блокчейн, смарт-контрактів, IPFS і модулів згоди/перевірки

Управління доступом до персональних даних у дозвільному блокчейн реалізується на основі чітко визначених ролей користувачів, що відповідають політикам доступу, заздалегідь узгодженим між учасниками цифрової платформи. Це дозволяє мінімізувати ризики несанкціонованого доступу, автоматизувати процеси перевірки прав користувачів та забезпечити прозорість в обробці даних.

Залежно від функціональної ролі, учасники мають доступ лише до тих дій, які передбачені їхньою компетенцією: наприклад, реєстратор може створювати та підписувати записи, тоді як перевіряючий — лише читати і підтверджувати інформацію. Громадянин має доступ до власних даних і можливість надавати або відкликати згоду. У свою чергу, аудитор може аналізувати повну історію змін у реєстрі в межах верифікаційних процедур. Деталізовану структуру доступу наведено в табл. 1.

Таблиця 1

Ролі користувачів у системі дозвільного блокчейн-доступу до персональних даних

Роль користувача	Дії з даними	Приклад застосування
Реєстратор	Запис, підпис	Внесення нової інформації у реєстр
Перевіряючий	Зчитування, підпис	Перевірка достовірності при запиті
Громадянин	Обмежене зчитування, надання згод	Перегляд власних даних, керування згодами
Аудитор	Повний доступ до журналів транзакцій	Проведення контролю та верифікації

Ця модель дозволяє інтегрувати механізм управління згодою, що забезпечує правомірність обробки персональних даних відповідно до вимог GDPR та Закону України № 2297-VI «Про захист персональних даних». Кожна транзакція допускається лише після перевірки згоди користувача, що реалізується на рівні смарт-контрактів та забезпечує гнучкість у керуванні правами доступу в реальному часі.

Механізми забезпечення цілісності та довіри в міжорганізаційному обміні даними

Цілісність та довіра є фундаментальними вимогами до систем, які забезпечують обмін персональними даними між різними організаціями в межах публічних та адміністративних сервісів [13]. Технологія дозвільного блокчейн, у поєднанні з

криптографічними алгоритмами, механізмами цифрової ідентифікації та розподіленим зберіганням, дозволяє реалізувати надійну інфраструктуру обміну, що виключає втручання зловмисників, втрату даних або несанкціонований доступ.

Одним із ключових елементів забезпечення цілісності транзакцій є використання механізму консенсусу [14], який забезпечує однозначність результатів верифікації транзакцій усіма вузлами мережі. У дозвільних мережах, таких як Hyperledger Fabric, можуть застосовуватись механізми Raft або PBFT (Practical Byzantine Fault Tolerance), які гарантують:

- неможливість внесення змін до транзакцій після досягнення консенсусу;
- захист від атак із боку компрометованих вузлів;
- збереження синхронності журналів транзакцій у всіх установах-учасниках.

Кожна транзакція супроводжується криптографічним підписом ініціатора, що дозволяє не лише підтвердити її походження, а й запобігти підробці вмісту. Для цього використовуються асиметричні алгоритми (наприклад, ECDSA) [15], а відкриті ключі сертифікуються відповідними органами у межах системи ідентифікації.

Додатково, для забезпечення достовірності інформації, яка передається між установами, впроваджено механізм перевірки цілісності на основі геш-функцій. Усі об’єкти, що зберігаються у IPFS або записуються у блокчейн, супроводжуються контрольними хешами (SHA-256), які дозволяють:

- переконатися у відсутності змін у даних;
- перевірити цілісність навіть при частковій передачі файлів;
- здійснити автентифікацію результатів перевірки в інституціях, що не є ініціаторами транзакції.

Окрему роль у формуванні довіри відіграє модуль згоди користувача, який забезпечує автоматичну перевірку того, чи надала особа дозвіл на обробку її персональних даних для конкретної установи та цілі. Смарт-контракти в обох установах перевіряють цей дозвіл до початку обробки або передачі, що:

- гарантує дотримання принципу privacy by design;
- дозволяє автоматизувати перевірку прав доступу;
- мінімізує ризик порушення GDPR або українського законодавства про захист персональних даних.

Загалом, сукупність вищенаведених механізмів створює середовище обміну з високим рівнем довіри, у якому кожен учасник має підтверджену ідентичність, а всі транзакції — фіксовану, перевірену та незмінну історію [16].

Роль децентралізованих систем зберігання (IPFS) у побудові надійної інфраструктури для обміну чутливою інформацією між організаціями

Ефективний міжорганізаційний обмін чутливою інформацією вимагає інфраструктури, здатної одночасно забезпечувати конфіденційність, цілісність, контроль доступу та масштабованість. У межах блокчейн-орієнтованих рішень одним з критичних викликів є обмежена пропускна здатність ланцюгів блоків щодо обробки великих обсягів даних. Саме тому децентралізовані системи зберігання, зокрема InterPlanetary File System (IPFS), відіграють ключову роль у побудові надійної гібридної інфраструктури [17].

Блокчейн добре підходить для зберігання незмінної, критичної метаінформації про транзакції (ідентифікатор, підписи, часові мітки, згода користувача). Однак він не оптимізований для зберігання файлів великого розміру, таких як: медичні зображення, цифрові копії ідентифікаційних документів, договори, що підлягають правовій експертизі, сертифікати, довідки тощо.

Розміщення таких даних у блокчейн призвело б до надмірного навантаження на мережу, уповільнення консенсусу та ризику масштабування. Замість цього пропонується гібридний підхід: блокчейн плюс IPFS, де IPFS виступає розподіленим сховищем, а блокчейн — реєстром і контролером доступу [18].

Ключова функція IPFS — адресація за хешем вмісту, а не за місцем розташування. Це означає, що кожен файл отримує унікальний ідентифікатор (CID) [19], який можна зберігати в транзакції блокчейн без самого контенту. Наприклад, файл з медичним висновком після завантаження в IPFS створює CID, який зберігається у смарт-контракті разом з інформацією про згоду пацієнта. Таким чином:

- Установа А (відправник) зберігає документ у IPFS.
- Блокчейн фіксує CID і перевіряє згоду через смарт-контракт.
- Установа В (отримувач) звертається до IPFS, отримує контент лише за умови наявності дозволу.

Цей механізм дозволяє обмежити доступ не лише на рівні файлової системи, а й на рівні транзакції — що критично важливо для персональних даних [20].

Щоб обґрунтувати доцільність використання IPFS у розподіленій інфраструктурі обміну персональними даними, доцільно порівняти його з типовими централізованими рішеннями (табл. 2).

Таблиця 2

Порівняння IPFS та централізованого сховища у контексті обміну чутливою інформацією

Критерій	Централізоване сховище (FTP, S3, сервер установи)	IPFS
Адресація	За місцем (URL, IP, каталог)	За вмістом (CID — Content Identifier)
Захист від підміни	Низький: можлива модифікація файлу без зміни URL	Високий: зміна вмісту змінює CID
Доступність при відмові вузла	Обмежена	Висока: децентралізоване зберігання
Можливість перевірки цілісності	Через контрольні суми, вручну	Автоматична, вбудована в CID
Придатність до блокчейн-інтеграції	Часткова, через API	Пряма (CID записується у смарт-контракт)
Контроль прав доступу	Через ACL, слабо масштабовані	Через політики на рівні смарт-контрактів

Ця таблиця демонструє, що IPFS, у комбінації з блокчейн, забезпечує не лише більшу стійкість до атак, а й інтегровану перевірку достовірності та вбудований контроль над доступом.

Типові сценарії застосування IPFS у дозвільному блокчейн:

1. Обмін цифровими документами між державними установами. Наприклад, під час обміну довідками про стан здоров’я, правовими документами, сертифікатами вакцинації тощо — дані зберігаються в IPFS, а у блокчейн зберігається лише хеш та підтвердження згоди користувача на доступ.
2. Зберігання доказової інформації у судових і реєстраційних процедурах. Акти, документи, скани зберігаються в IPFS з фіксацією метаданих у ланцюгу блоків, що дозволяє верифікувати їх цілісність у будь-який момент.

3. Довготривале зберігання та архівація без втрати контрольованості. IPFS дозволяє уникнути зносу інфраструктури централізованих сховищ, водночас підтримуючи контрольований, підтверджений доступ через смарт-контракти.

Модель безпечного міжорганізаційного обміну конфіденційними персональними даними

Формування надійної моделі обміну конфіденційною інформацією між організаціями потребує одночасного дотримання технічних, процедурних та нормативних вимог [21]. У цифровому середовищі, де великі обсяги персональних даних передаються між різними суб'єктами, особливу роль відіграють механізми, що забезпечують правомірність, прозорість і захист даних на кожному етапі життєвого циклу.

Розроблена модель ґрунтується на поєднанні таких компонентів:

- Дозвільний блокчейн (на базі Hyperledger Fabric) — як основа мережі довіри з контрольованим доступом;
- Смарт-контракти — як інструмент для автоматизації перевірки згоди, прав доступу та реєстрації транзакцій;
- IPFS (InterPlanetary File System) — для зберігання об'ємних даних поза блокчейном з криптографічною прив'язкою до реєстру;
- Модуль оцінки згоди — як частина цифрового механізму відповідності принципу lawful basis згідно з GDPR;
- Модуль аудиту та логування — з окремим доступом для зовнішніх або внутрішніх ревізорів.

Архітектура реалізує принципи мінімізації даних, захисту за замовчуванням та за дизайном, а також права суб'єкта на відкликання згоди, доступ до історії обробки, верифікацію джерела запиту. Схема такої моделі наведена на рис. 2.

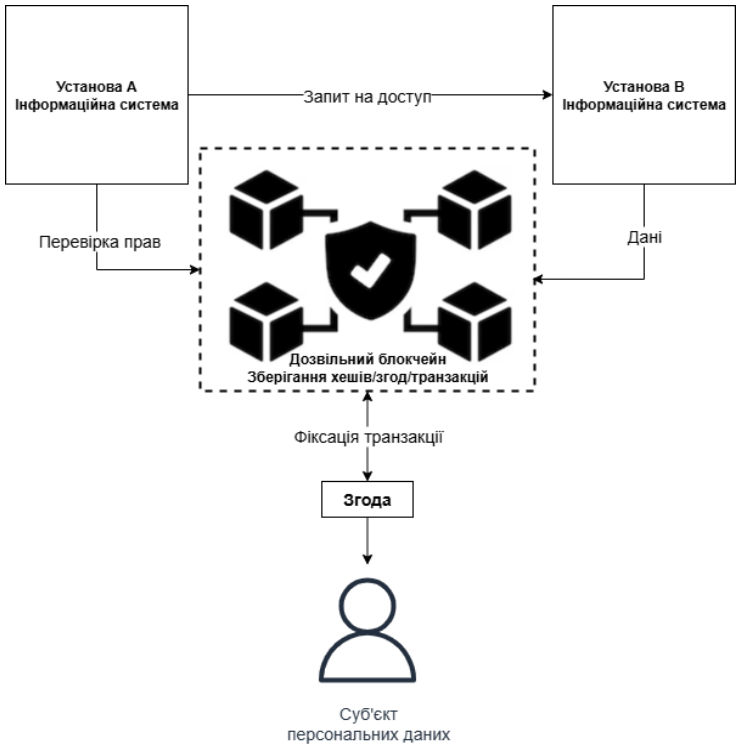

Рис. 2. Уніфікована модель безпечного міжорганізаційного обміну персональними даними на базі дозвільного блокчейн

Ключові принципи, на яких базується ця модель, відповідають статтям 5–9 Регламенту (ЄС) 2016/679 (GDPR), зокрема:

1. Законність і справедливість обробки (Lawfulness, Fairness);
2. Прозорість транзакцій (Transparency);
3. Мінімізація обсягу та строку зберігання (Data minimization);
4. Точність і незмінність (Accuracy, Integrity);
5. Підзвітність контролера (Accountability).

Також враховано вимоги ISO/IEC 27701:2019 щодо розмежування ролей PII Controller/Processor, управління ризиками доступу, зберігання журналів доступу, використання криптографічних механізмів і моніторингу відповідності [22].

В українському правовому полі модель відповідає принципам Закону України «Про захист персональних даних» № 2297-VI та рішенню Уповноваженого щодо транскордонної передачі. Зокрема, реалізовано такі аспекти:

- Вимога щодо ведення згод у доступній формі, яку можна відкликати;
- Фіксація кожного запиту/відповіді у блокчейн із зазначенням мети обробки;
- Використання українських КЕП при підписанні транзакцій.

Для глибшого розуміння розподілу функцій у межах міжорганізаційного обміну персональними даними доцільно розглянути ролі та відповідальність суб'єктів процесу у розрізі основних компонентів моделі [23]. Взаємодія між сторонами — установами, що ініціюють і приймають запити, блокчейн-реєстром, IPFS та суб'єктом персональних даних — має бути чітко визначеною як у технічному, так і в правовому вимірі.

У табл. 3 представлено узагальнення функцій кожного з ключових учасників моделі, з урахуванням контролю за згодами, фіксацією транзакцій, зберіганням даних та перевіркою доступу.

Таблиця 3

Розподіл функцій і відповідальності між учасниками моделі обміну персональними даними

Компонент моделі	Основні функції	Відповідальний суб'єкт	Контроль/верифікація
Дозвільний блокчейн	Фіксація хешів транзакцій, журнал доступу	Адміністратори мережі (спільно)	Криптографічна перевірка
Смарт-контракт	Автоматична перевірка згоди, реєстрація доступу	Розробники/власники правил	Аудит логіки та коду
IPFS	Децентралізоване зберігання зашифрованих даних	Власник інформації / обидві сторони	Посилання в блокчейн, хеш-функції
Модуль оцінки згоди	Перевірка наявності і валідності згоди користувача	Організація-контролер	Звірка з блокчейном
Суб'єкт персональних даних	Надання/відкликання згоди, перегляд журналу	Фізична особа	Право на доступ, згідно з GDPR
Установа ініціатор запиту	Формування запиту, зазначення мети обробки	Організація-ініціатор	Зобов'язання щодо обґрунтування
Установа — власник даних	Перевірка прав доступу, надання даних	Організація-власник	Верифікація через смарт-контракт

Запропонована модель забезпечує баланс між гнучкістю цифрових процесів та вимогами правового регулювання. Центральну роль відіграє дозвільний блокчейн, у якому хешуються всі транзакції, що дозволяє уникнути реплікації персональних даних у

ланцюжку блоків і зменшити ризик витоку. Фактичне зберігання інформації здійснюється в IPFS — з прив'язкою лише хешу до блокчейн, що унеможливлює ідентифікацію без криптографічного ключа.

Згода суб'єкта персональних даних не лише фіксується, але й перевіряється смарт-контрактом перед кожним доступом до даних. Це дозволяє автоматизувати правову відповідність (наприклад, ст. 6 GDPR — Lawfulness of processing), зменшити ризик людської помилки та підвищити довіру до транзакцій. Кожна з установ має власну зону відповідальності — ініціатор вказує мету, власник перевіряє права, а аудит ведеться у незмінному реєстрі, відкритому для моніторингу.

Таким чином, модель демонструє, як можна досягнути прозорого, контрольованого, зворотно перевірюваного обміну персональними даними між установами, дотримуючись водночас технічної ефективності та правових норм.

У практиці міжорганізаційної взаємодії зазвичай використовуються централізовані або гібридні підходи до обміну персональними даними [24]. Більшість таких систем базується на ручному погодженні, відправці запитів електронною поштою, синхронізації через VPN або окремі реєстрові API. Вони часто не забезпечують належного рівня прозорості, обліку згод чи стійкості до модифікації записів.

Для порівняння ефективності уніфікованої моделі, наведеної вище, проведено зіставлення ключових характеристик трьох підходів — класичного (централізованого), гібридного (з елементами автоматизації) та запропонованого (блокчейн з IPFS, смарт-контрактами і модулями згоди).

Таблиця 4

Порівняння підходів до обміну конфіденційними персональними даними

Критерій	Централізований підхід	Гібридний підхід	Запропонована модель (PB+IPFS+SC)
Контроль доступу	Адміністратор вручну	Локальні ACL / токени доступу	Смарт-контракт на основі згод
Прозорість транзакцій	Відсутня	Частково (в логах)	Повна фіксація в блокчейні
Сховище даних	Централізований сервер	Локальні сервери / хмара	IPFS + шифрування + хеш у блокчейні
Верифікація згоди	Паперова / PDF	Цифрова, не завжди прив'язана	Автоматична перевірка перед доступом
Незмінність записів	Вразлива до змін	Частково захищена	Гарантована властивістю блокчейну
Можливість аудиту	Потребує ручної перевірки	Частковий аудит логів	Повний аудит транзакцій і журналу доступу
Захист від внутрішніх атак	Мінімальний	Обмежений правами доступу	Розмежовані ролі + шифрування
Відповідність GDPR та ISO/IEC 27701	Часткова	Часткова	Повна відповідність ключовим вимогам

Як показано у таблиці, запропонована модель демонструє переваги у всіх ключових аспектах безпечного обміну персональними даними. Зокрема, завдяки використанню дозвільного блокчейн, смарт-контрактів і децентралізованого зберігання, досягається автоматизована правомірність доступу, фіксація кожної транзакції, а також відповідність міжнародним і національним вимогам захисту персональних даних.

Особливістю цього підходу є поєднання юридичних вимог (згода, мета обробки) з технічними інструментами, які не просто зберігають інформацію, а забезпечують її контрольований доступ, верифікацію і довіру між установами.

ВИСНОВКИ

У результаті проведеного дослідження сформовано модель безпечного міжорганізаційного обміну конфіденційними персональними даними, яка забезпечує комплексне дотримання принципів законності, прозорості, контрольованості доступу та цілісності інформації. В основі цієї моделі лежить дозвільний блокчейн Hyperledger Fabric, який забезпечує контроль за ідентифікованими учасниками мережі, а також інтеграція IPFS для зберігання великих масивів даних поза реєстром із криптографічною прив'язкою.

Запропоноване рішення дозволяє уникнути типових ризиків централізованих систем, зокрема несанкціонованого доступу, втрати достовірності даних або ускладнень у встановленні джерела витоку. Смарт-контракти відіграють ключову роль у моделі — вони забезпечують автоматичну перевірку умов доступу, згоди суб'єкта та відповідності транзакції встановленим політикам конфіденційності. Таким чином, юридично-значущі дії — наприклад, реєстрація запиту, згода на обробку або відкликання дозволу — фіксуються в блокчейн-мережі як незмінні цифрові події.

Модель підтримує гнучке керування життєвим циклом згоди відповідно до вимог GDPR (статті 5–9), реалізуючи принципи захисту за замовчуванням (privacy by default), мінімізації даних, права на забуття та аудит. Крім того, використання ролей PII Controller / Processor відповідно до ISO/IEC 27701:2019, журналів доступу, криптографічного підпису та валідації транзакцій забезпечує вищий рівень відповідності сучасним вимогам інформаційної безпеки.

Побудована архітектура пройшла концептуальне опрацювання на рівні узагальненої системи та сценаріїв її застосування в державному, освітньому та медичному секторах. Усі компоненти моделі мають чітку функціональну взаємодію: від peer-вузлів до систем логування та зовнішнього аудиту. Представлені графічні матеріали (рисунки та схеми) і таблиці відображають як логіку взаємодії елементів, так і відповідність положенням міжнародного та національного законодавства.

Отже, розроблена модель не лише концептуально відповідає вимогам цифрової трансформації державного управління та захисту персональних даних, а й має потенціал до практичного впровадження у міжвідомчих інформаційних системах. Її застосування сприятиме зростанню довіри між учасниками, зменшенню ризиків витоку чи спотворення даних, а також формуванню сталої цифрової інфраструктури для безпечного обміну чутливою інформацією між організаціями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Balatska, V. S., & Opirskyy, I. R. (2023). Ensuring personal data confidentiality and cybersecurity through blockchain. *Cybersecurity: Education, Science, Technology*, (4)20, 6–19. https://doi.org/10.28925/2663-4023.2023.20.619
2. Balatska, V., & Opirskyy, I. (2024). Blockchain as a tool for transparency and protection of government registries. *Ukrainian Scientific Journal of Information Security*, *30*(2), 221–230. https://doi.org/10.18372/2225-5036.30.19211
3. Balatska, V., & Poberezhnyk, V. (2024). Concept of applying blockchain technologies to enhance personal data protection in the Diia platform. *Cybersecurity: Education, Science, Technology*, (2)26, 268–290. https://doi.org/10.28925/2663-4023.2024.26.681
4. Balatska, V., Opirskyy, I., & Slobodian, N. (2024). Blockchain for enhancing transparency and trust in government registries. In *CEUR Workshop Proceedings* (Vol. 3826, pp. 50–59). https://ceur-ws.org/Vol-3826/

5. Balatska, V., Poberezhnyk, V., & Opirskyy, I. (2024). Use of non-fungible tokens and blockchain for access control to state registries. *Cybersecurity: Education, Science, Technology*, (4)24, 99–114. https://doi.org/10.28925/2663-4023.2024.24.99114
6. Balatska, V., Poberezhnyk, V., & Opirskyy, I. (2024). Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR. In *CEUR Workshop Proceedings* (Vol. 3800, pp. 70–80). http://ceur-ws.org/Vol-3800/
7. Balatska, V., Poberezhnyk, V., Petriv, P., & Opirskyy, I. (2024). Blockchain application concept in SSO technology context. In *CEUR Workshop Proceedings* (Vol. 3654, pp. 38–49). https://ceur-ws.org/Vol-3654/
8. Balatska, V. S., Poberezhnyk, V. O., Stefankiv, A. V., & Shevchuk, Y. A. (2025). Method for ensuring authenticity and security of personal data in state registry blockchain systems. *Computer Systems and Networks*, *7*(1), 1–16. https://doi.org/10.23939/csn2025.01.001
9. Balatska, V. S., & Opirskyy, I. R. (2025). Decentralized digital identity and consent management using blockchain: Integration with national registries. In *CEUR Workshop Proceedings* (Vol. 3900, pp. 102–112). https://ceur-ws.org/Vol-3900/
10. Benet, J. (2014). *IPFS – Content addressed, versioned, P2P file system* (arXiv:1407.3561). arXiv. https://arxiv.org/pdf/1407.3561.pdf
11. Cabinet of Ministers of Ukraine. (n.d.). *Digital transformation of Ukraine: National program "Diia"*. https://diia.gov.ua/en
12. Cachin, C. (2016). Architecture of the Hyperledger blockchain fabric. In *Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16)* (pp. 1–4). Chicago, USA.
13. 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
14. Deloitte. (2021). *Blockchain for government: Real-world applications and challenges*. https://www2.deloitte.com/insights
15. Elbahrawy, A., Alessandretti, L., Kandler, C., & Baronchelli, A. (2017). Evolutionary dynamics of the cryptocurrency market. *Royal Society Open Science*, *4*(11), 170623. https://doi.org/10.1098/rsos.170623
16. European Union Agency for Cybersecurity. (2020). *Data protection engineering – From theory to practice*. https://www.enisa.europa.eu/publications/data-protection-engineering
17. European Union Agency for Cybersecurity. (2023). *Blockchain security: A critical analysis of emerging threats*. https://www.enisa.europa.eu
18. International Organization for Standardization. (2019). *ISO/IEC 27701:2019. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*. Geneva, Switzerland: ISO.
19. Li, W., Sforzin, A., Fedorov, S., & Karame, G. H. (2018). Towards scalable and private industrial blockchains. *Future Generation Computer Systems*, *93*, 644–656. https://doi.org/10.1016/j.future.2018.01.061
20. Opirskyy, I., Balatska, V., & Poberezhnyk, V. (2023). Modern possibilities of use blockchain technology in the education system. *Ukrainian Scientific Journal of Information Security*, *29*(3), 138–146. https://doi.org/10.18372/2225-5036.29.18073
21. Poberezhnyk, V., Balatska, V., & Opirskyy, I. (2023). Development of the learning management system concept based on blockchain technology. In *CEUR Workshop Proceedings* (Vol. 3550, pp. 114–124). https://ceur-ws.org/Vol-3550/
22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union*, *L119*, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
23. Wang, W., Hoang, D. T., Xiong, Z., et al. (2020). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Systems Journal*, *15*(1), 57–75. https://doi.org/10.1109/JSYST.2020.2961798
24. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019). Smart contract-based access control for the Internet of Things. *ACM Computing Surveys*, *52*(3), 1–29. https://doi.org/10.1145/3316481

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Valeriia Balatska
Senior Lecturer at the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID: 0000-0002-6262-6792
v.balatska@ldubgd.edu.ua

Nazarii Dmytriv
Postgraduate Student
Private Higher Educational Institution "European University", Kyiv, Ukraine
ORCID ID: 0009-0007-0326-3622
nazarii.dmytriv@gmail.com

INTER-ORGANIZATIONAL EXCHANGE OF CONFIDENTIAL PERSONAL DATA BASED ON PERMISSIONED BLOCKCHAIN

Abstract. The article addresses the issue of ensuring confidential exchange of personal data in inter-organizational information systems under conditions of increasing digital interaction between public and private sector entities. It is noted that centralized models for processing and exchanging personal data fail to provide an adequate level of protection against unauthorized access, transaction tampering, and do not ensure sufficient transparency of data operations. These limitations hinder full compliance with regulatory requirements, particularly the provisions of the General Data Protection Regulation (GDPR), ISO/IEC 27001 and 27701 standards, as well as national legislation on information protection. The study substantiates the feasibility of using a permissioned blockchain as the architectural basis for implementing a secure, decentralized exchange of personal data with guaranteed access control, transaction audit, and data immutability. A conceptual model of the information system is proposed, involving smart contracts for managing data subject consent, access control, and the integration of the InterPlanetary File System (IPFS) for robust off-chain data storage. The model also includes the use of Zero-Knowledge Proof (ZKP) cryptographic mechanisms and behavioral verification criteria for transactions. Particular attention is given to risk analysis associated with personal data processing in inter-organizational environments, and to the application of supplementary protection tools—such as masking, pseudonymization, and data perturbation—to mitigate potential losses in the event of data leakage. A set of technical and organizational compliance criteria with international and national information security standards is outlined. The aim of this research is to design an architectural model for inter-organizational personal data exchange based on permissioned blockchain that ensures confidentiality, integrity, controlled access, and regulatory compliance in the field of information protection.

Keywords: personal data; inter-organizational exchange; permissioned blockchain; smart contracts; IPFS; confidentiality; Zero-Knowledge Proof; cryptographic protection; consent management; regulatory compliance; GDPR.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Balatska, V. S., & Opirskyy, I. R. (2023). Ensuring personal data confidentiality and cybersecurity through blockchain. *Cybersecurity: Education, Science, Technology*, (4)20, 6–19. https://doi.org/10.28925/2663-4023.2023.20.619
2. Balatska, V., & Opirskyy, I. (2024). Blockchain as a tool for transparency and protection of government registries. *Ukrainian Scientific Journal of Information Security*, *30*(2), 221–230. https://doi.org/10.18372/2225-5036.30.19211
3. Balatska, V., & Poberezhnyk, V. (2024). Concept of applying blockchain technologies to enhance personal data protection in the Diia platform. *Cybersecurity: Education, Science, Technology*, (2)26, 268–290. https://doi.org/10.28925/2663-4023.2024.26.681
4. Balatska, V., Opirskyy, I., & Slobodian, N. (2024). Blockchain for enhancing transparency and trust in government registries. In *CEUR Workshop Proceedings* (Vol. 3826, pp. 50–59). https://ceur-ws.org/Vol-3826/

5. Balatska, V., Poberezhnyk, V., & Opirskyy, I. (2024). Use of non-fungible tokens and blockchain for access control to state registries. *Cybersecurity: Education, Science, Technology*, (4)24, 99–114. https://doi.org/10.28925/2663-4023.2024.24.99114
6. Balatska, V., Poberezhnyk, V., & Opirskyy, I. (2024). Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR. In *CEUR Workshop Proceedings* (Vol. 3800, pp. 70–80). http://ceur-ws.org/Vol-3800/
7. Balatska, V., Poberezhnyk, V., Petriv, P., & Opirskyy, I. (2024). Blockchain application concept in SSO technology context. In *CEUR Workshop Proceedings* (Vol. 3654, pp. 38–49). https://ceur-ws.org/Vol-3654/
8. Balatska, V. S., Poberezhnyk, V. O., Stefankiv, A. V., & Shevchuk, Y. A. (2025). Method for ensuring authenticity and security of personal data in state registry blockchain systems. *Computer Systems and Networks*, *7*(1), 1–16. https://doi.org/10.23939/csn2025.01.001
9. Balatska, V. S., & Opirskyy, I. R. (2025). Decentralized digital identity and consent management using blockchain: Integration with national registries. In *CEUR Workshop Proceedings* (Vol. 3900, pp. 102–112). https://ceur-ws.org/Vol-3900/
10. Benet, J. (2014). *IPFS – Content addressed, versioned, P2P file system* (arXiv:1407.3561). arXiv. https://arxiv.org/pdf/1407.3561.pdf
11. Cabinet of Ministers of Ukraine. (n.d.). *Digital transformation of Ukraine: National program "Diia"*. https://diia.gov.ua/en
12. Cachin, C. (2016). Architecture of the Hyperledger blockchain fabric. In *Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16)* (pp. 1–4). Chicago, USA.
13. 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
14. Deloitte. (2021). *Blockchain for government: Real-world applications and challenges*. https://www2.deloitte.com/insights
15. Elbahrawy, A., Alessandretti, L., Kandler, C., & Baronchelli, A. (2017). Evolutionary dynamics of the cryptocurrency market. *Royal Society Open Science*, *4*(11), 170623. https://doi.org/10.1098/rsos.170623
16. European Union Agency for Cybersecurity. (2020). *Data protection engineering – From theory to practice*. https://www.enisa.europa.eu/publications/data-protection-engineering
17. European Union Agency for Cybersecurity. (2023). *Blockchain security: A critical analysis of emerging threats*. https://www.enisa.europa.eu
18. International Organization for Standardization. (2019). *ISO/IEC 27701:2019. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*. Geneva, Switzerland: ISO.
19. Li, W., Sforzin, A., Fedorov, S., & Karame, G. H. (2018). Towards scalable and private industrial blockchains. *Future Generation Computer Systems*, *93*, 644–656. https://doi.org/10.1016/j.future.2018.01.061
20. Opirskyy, I., Balatska, V., & Poberezhnyk, V. (2023). Modern possibilities of use blockchain technology in the education system. *Ukrainian Scientific Journal of Information Security*, *29*(3), 138–146. https://doi.org/10.18372/2225-5036.29.18073
21. Poberezhnyk, V., Balatska, V., & Opirskyy, I. (2023). Development of the learning management system concept based on blockchain technology. In *CEUR Workshop Proceedings* (Vol. 3550, pp. 114–124). https://ceur-ws.org/Vol-3550/
22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union*, *L119*, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
23. Wang, W., Hoang, D. T., Xiong, Z., et al. (2020). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Systems Journal*, *15*(1), 57–75. https://doi.org/10.1109/JSYST.2020.2961798
24. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019). Smart contract-based access control for the Internet of Things. *ACM Computing Surveys*, *52*(3), 1–29. https://doi.org/10.1145/3316481