НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

«На правах рукопису»
УДК 003.26+004.75

«До захисту допущено»
Завідувач кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2025 р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-науковою програмою
«Математичні методи криптографічного захисту інформації»

зі спеціальності: 113 Прикладна математика
на тему: **«Розробка та аналіз методів проведення тендерних закупівель з використанням блокчейн технологій»**

Виконав:
студент II курсу, групи ФІ-32мн
Баєвський Костянтин Олександрович _____

Керівник:
д.т.н., проф. каф. ММЗІ
Ковальчук Людмила Василівна _____

Рецензент:
д.ф., ст. викл. каф. ММАД
Яйлимова Ганна Олексіївна _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2025

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти — другий (магістерський)
Спеціальність — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2025 р.

ЗАВДАННЯ
на магістерську дисертацію

Студент: Баєвський Костянтин Олександрович

1. Тема роботи: «*Розробка та аналіз методів проведення тендерних закупівель з використанням блокчейн технологій*», науковий керівник дисертації: д.т.н., проф. каф. ММЗІ Ковальчук Людмила Василівна,

затверджені наказом по університету №__ від «__» _____ 2025 р.

2. Термін подання студентом роботи: «__» _____ 2025 р.

3. Об'єкт дослідження: *процес проведення тендерних закупівель.*

4. Предмет дослідження: *методи криптографічного захисту проведення тендерних закупівель.*

5. Перелік завдань:

– *Проведення загального огляду процедури тендерних закупівель, їхніх етапів та ключових принципів;*

– *Огляд сучасних методів проведення тендерів, включаючи електронні тендерні платформи та блокчейн–орієнтовані підходи;*

– *Аналіз їхніх переваг та недоліків, а також вразливих місць;*

– *Дослідження відомих атак на тендерні процедури, зокрема в електронних системах;*

– *Виявлення можливих нових загроз в разі перенесення тендерів у блокчейн без зміни підходів до їх організації;*

– *Розробка нових методів проведення тендерних закупівель з використанням сучасних криптографічних інструментів.*

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: *Презентація доповіді.*

7. Орієнтовний перелік публікацій: *Частина результатів даної роботи докладалась на XXIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (14-17 травня 2025 р., м. Київ, Україна).*

8. Дата видачі завдання: 10 вересня 2024 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2024 р.	Виконано
2	Огляд опублікованих джерел за тематикою тендерних закупівель та їхніх загроз	Вересень-жовтень 2024 р.	Виконано
3	Аналіз методів проведення тендерних закупівель	Листопад-грудень 2024 р.	Виконано
4	Дослідження загроз та шахрайських схем у тендерах	Січень-лютий 2025 р.	Виконано
5	Аналіз ризиків перенесення тендерних закупівель у блокчейн	Березень-квітень 2025 р.	Виконано
6	Розробка методів з використанням криптографічних інструментів	Квітень-травень 2025 р.	Виконано
7	Оформлення дипломної роботи	Травень 2025 р.	Виконано

Студент _____ Костянтин Баєвський

Керівник _____ Людмила Ковальчук

РЕФЕРАТ

Кваліфікаційна робота містить: 67 стор., 0 рисунків, 6 таблиць, 37 джерел.

Метою дослідження є розробка та аналіз методів проведення тендерних закупівель з використанням блокчейн технологій.

Об'єктом дослідження є процес проведення тендерних закупівель.

Предметом дослідження є методи криптографічного захисту проведення тендерних закупівель.

У результаті виконання роботи було досліджено сучасні підходи до організації тендерних закупівель та проаналізовано можливості інтеграції блокчейн технологій для підвищення прозорості, надійності та захищеності процесів. Розглянуто особливості застосування верифікованих випадкових функцій (VRF) і протоколів розподіленого генерування ключів (DKG) у контексті побудови безпечних і перевірюваних тендерних механізмів. Розроблено два нових методи проведення тендерів: один — з використанням VRF для забезпечення прозорого подання заявок, інший — із додатковим залученням DKG для збереження конфіденційності. Обидва підходи були проаналізовані з точки зору їхньої захищеності від атак, прозорості, перевірюваності та складності реалізації. Отримані результати підтверджують доцільність використання блокчейну в системах публічних закупівель і демонструють практичну цінність застосування криптографічних методів у цій сфері.

БЛОКЧЕЙН, ВЕРИФІКОВАНА ВИПАДКОВА ФУНКЦІЯ, ПРОТОКОЛИ РОЗПОДІЛЕНОГО ГЕНЕРУВАННЯ КЛЮЧІВ, ПЕРЕВІРЕНІ СХЕМИ ОБМІНУ СЕКРЕТОМ, ПУБЛІЧНІ ЗАКУПІВЛІ, ПРОЗОРІСТЬ, КОНФІДЕНЦІЙНІСТЬ

ABSTRACT

Qualification work contains: 67 pages, 0 figures, 6 tables, 37 sources.

The aim of the study is development and analysis of the methods for conducting tender procurement using blockchain technologies.

The object of research is the process of conducting tender procurement.

The subject of research is the methods of cryptographic protection of tender procurement.

As a result of this work, contemporary approaches to organizing tender procurement were examined, and the potential of blockchain technologies to improve the transparency, reliability, and security of such processes was analyzed. The study explored the application of Verifiable Random Functions (VRF) and Distributed Key Generation (DKG) protocols in building secure and auditable tender mechanisms. Two novel methods of conducting tenders were developed: one based on VRF to ensure transparent submission of bids, and another combining VRF with DKG to additionally preserve confidentiality. Both approaches were evaluated in terms of their security against attacks, transparency, verifiability, and implementation complexity. The results obtained confirm the feasibility of using blockchain in public procurement systems and demonstrate the practical value of cryptographic techniques in this domain.

BLOCKCHAIN, VERIFIABLE RANDOM FUNCTION, DISTRIBUTED KEY GENERATION, VERIFIABLE SECRET SHARING, PUBLIC PROCUREMENT, TRANSPARENCY, CONFIDENTIALITY

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ФТІ — Фізико-технічний інститут;

GPA (англ. Agreement on Government Procurement) — Угода про державні закупівлі;

СОТ (англ. World Trade Organization, WTO) — Світова організація торгівлі;

ЮНСІТРАЛ (англ. United Nations Commission on International Trade Law, UNCITRAL) — Комісія ООН з права міжнародної торгівлі;

ОЕСР (англ. Organisation for Economic Co-operation and Development, OECD) — Організація економічного співробітництва та розвитку;

НАБУ — Національне антикорупційне бюро України;

DDoS (англ. Distributed Denial of Service) — розподілена атака на відмову в обслуговуванні;

PoW — протокол консенсусу Proof-of-Work;

PoS — протокол консенсусу Proof-of-Stake.

ВСТУП

Актуальність дослідження. Тендерні закупівлі є важливою складовою економічної діяльності як у державному, так і в приватному секторі. Вони забезпечують прозорість, конкуренцію та ефективність розподілу ресурсів, однак водночас залишаються вразливими до різноманітних атак та шахрайських схем. Незважаючи на розвиток електронних систем проведення тендерів, існують численні ризики, пов'язані з маніпуляціями учасників, корупційними схемами, змовами та іншими загрозами. З появою блокчейн технологій виникла ідея впровадження децентралізованих тендерних систем, однак просте перенесення традиційних механізмів у блокчейн без зміни основних принципів їхньої роботи може не вирішити проблеми, а лише перенести їх у нове середовище. Тому детальний аналіз сучасних методів проведення тендерів, їхніх вразливостей, а також можливих атак у традиційних та блокчейн-системах є вкрай актуальним.

Метою дослідження є розробка та аналіз методів проведення тендерних закупівель з використанням блокчейн технологій.

Для досягнення мети необхідно виконати такі завдання:

1) Провести загальний огляд процедури тендерних закупівель, їхніх етапів та ключових принципів.

2) Розглянути сучасні методи проведення тендерів, включаючи електронні тендерні платформи та блокчейн–орієнтовані підходи.

3) Проаналізувати їхні переваги та недоліки, а також вразливі місця.

4) Дослідити відомі атаки на тендерні процедури, зокрема в електронних системах.

5) Виявити можливі нові загрози в разі перенесення тендерів у блокчейн без зміни підходів до їх організації.

6) Розробити нові методи проведення тендерних закупівель з використанням сучасних криптографічних інструментів.

Об'єктом дослідження є процес проведення тендерних закупівель.

Предметом дослідження є методи криптографічного захисту проведення тендерних закупівель.

Наукова новизна отриманих результатів полягає у розробці нових методів проведення тендерних закупівель з використанням блокчейн технологій, які суттєво підвищують рівень довіри, прозорості та безпеки процесу.

Практичне значення результатів полягає у можливості їх застосування для вдосконалення існуючих тендерних систем шляхом підвищення їх стійкості до зовнішніх атак та запобігання можливим шахрайським схемам. Отримані рекомендації й розроблені методи можуть бути впроваджені у процес розробки безпечних електронних платформ та блокчейн-базованих рішень для проведення тендерів, що сприятиме підвищенню прозорості та ефективності процесу закупівель.

Апробація результатів та публікації. Частина результатів даної роботи докладалась на XXIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (14-17 травня 2025 р., м. Київ, Україна).

1 ОГЛЯД ПРОЦЕДУРИ ТЕНДЕРНИХ ЗАКУПІВЕЛЬ ТА ЇХ МЕТОДИ ПРОВЕДЕННЯ

Сучасні тендерні закупівлі є важливим механізмом забезпечення прозорості та ефективності державних і приватних закупівель. Процес проведення тендеру передбачає участь різних зацікавлених сторін, дотримання чітких регламентів та використання спеціалізованих електронних платформ. Від правильного вибору моделі закупівлі залежить не лише економічна доцільність витрат, але й мінімізація корупційних ризиків та можливих шахрайських схем. У цьому розділі буде розглянуто основні принципи тендерної процедури, її ключові етапи, існуючі методи проведення закупівель, їхні особливості, переваги та недоліки. Це створить необхідну основу для подальшого аналізу вразливостей тендерних систем та потенційних атак на них у наступних розділах.

1.1 Основи тендерних закупівель

Щоб глибше зрозуміти суть тендерних процедур та особливості їхнього застосування, передусім слід окреслити ключові терміни, що лежать в основі системи публічних закупівель.

1.1.1 Визначення та поняття тендерних закупівель

Нижче наведено базові визначення, якими будемо послуговуватись упродовж подальшого аналізу структури, етапів та методів проведення тендерів.

Означення 1.1. Публічна закупівля [1] — це систематизований процес придбання товарів, робіт чи послуг замовниками (органами

державної влади, місцевого самоврядування чи іншими суб'єктами, що використовують бюджетні кошти), який здійснюється відповідно до встановлених законодавством процедур.

Метою публічних закупівель є забезпечення раціонального використання державних коштів, максимальна економія та досягнення високої якості результату за умов відкритості, прозорості та конкурентності.

Означення 1.2. Тендер (або процес закупівель, або торги) — це формалізована та структурована процедура, що здійснюється замовниками, зокрема державними або комунальними установами, з метою придбання товарів, послуг чи виконання робіт від зовнішніх постачальників або підрядників.

Цей процес регулюється законодавством і може проводитись як у письмовій, так і в електронній формі, при цьому тендерна документація містить детальний опис вимог до предмета закупівлі, умови виконання робіт чи постачання, визначену ціну та інші критерії відбору.

Основна мета тендеру полягає в забезпеченні проведення закупівель у прозорий, конкурентний і неупереджений спосіб, що сприяє досягненню оптимального співвідношення ціни та якості, раціональному використанню бюджетних коштів та зміцненню довіри громадськості до процесу розподілу державних ресурсів [2].

Означення 1.3. Замовник — це орган державної влади, орган місцевого самоврядування чи інша уповноважена юридична особа, яка здійснює публічні закупівлі з метою задоволення своїх потреб, використовуючи бюджетні кошти.

Означення 1.4. Предмет закупівлі — це конкретний об'єкт, що підлягає придбанню в рамках публічної закупівлі, який може бути представлений як товар, виконання певних робіт або надання послуг.

Він визначається технічними, якісними та кількісними характеристиками, викладеними у тендерній документації, що дозволяє

чітко окреслити вимоги замовника до очікуваного результату.

Означення 1.5. Тендерна документація — це комплекс документів, розроблений замовником для проведення процедури публічної закупівлі.

Вона містить детальний опис предмета закупівлі, вимоги до учасників, критерії оцінки тендерних пропозицій, а також зразок проекту договору, який буде укладено з переможцем. Документи забезпечують рівні умови участі для всіх потенційних учасників та сприяють прозорості та об'єктивності проведення закупівлі.

Означення 1.6. Тендерна пропозиція — це документ, який подається учасником (або потенційним постачальником) у відповідь на оголошення про публічну закупівлю.

Пропозиція містить конкретні умови, що відображають можливості учасника щодо постачання товарів, виконання робіт або надання послуг, а також зазначає ціну та інші параметри, які відповідають вимогам тендерної документації.

Означення 1.7. Тендерний комітет — це орган або група уповноважених осіб, які формуються замовником для організації, проведення та контролю процедури публічної закупівлі.

До його основних функцій належить підготовка тендерної документації, проведення оцінки отриманих тендерних пропозицій, визначення переможця закупівлі та забезпечення дотримання принципів конкурентності, об'єктивності та прозорості.

Означення 1.8. Учасник закупівлі — це фізична або юридична особа, яка бере участь у процедурі публічної закупівлі шляхом подання тендерної пропозиції та прагне укласти договір із замовником на поставку товарів, виконання робіт або надання послуг.

1.1.2 Принципи здійснення публічних закупівель

Незалежно від предмету закупівлі чи його очікуваної вартості замовник повинен дотримуватися наступних принципів здійснення публічних закупівель [3]:

1) *Добросовісна конкуренція.*

Принцип гарантує, що кожен потенційний учасник закупівлі матиме рівні можливості для участі, що виключає можливість виникнення штучних бар'єрів чи домовленостей, які могли б вплинути на чесність конкуренції. Такий підхід сприяє залученню найбільш кваліфікованих постачальників та забезпечує отримання найкращих пропозицій з точки зору ціни та якості.

2) *Максимальна економія, ефективність та пропорційність.*

Принцип орієнтується на раціональному використанні бюджетних коштів, коли закупівлі проводяться з метою досягнення найвигіднішого співвідношення вартості та якості. Він передбачає, що вимоги до постачальників повинні бути пропорційними обсягу та складності закупівлі, а критерії відбору – дозволяти визначити найекономічнішу та найефективнішу пропозицію.

3) *Відкритість та прозорість на всіх стадіях закупівель.*

Забезпечення відкритості означає, що інформація про кожен етап процедури закупівлі має бути доступною для зацікавлених сторін. Це стосується як публікації тендерної документації, так і оприлюднення результатів оцінки пропозицій, що сприяє підвищенню довіри до процесу та дозволяє контролюючим органам оперативно виявляти можливі порушення.

4) *Недискримінація учасників та рівне ставлення до них.*

Принцип передбачає, що умови участі у процедурі закупівлі мають бути однаковими для всіх учасників, без будь-якого упередженого ставлення чи дискримінації за будь-якими ознаками. Рівність можливостей дозволяє

кожному зацікавленому суб'єкту подати свою пропозицію, що сприяє формуванню справді конкурентного середовища.

5) *Об'єктивне та неупереджене визначення переможця процедури закупівлі/спрощеної закупівлі.*

Відбір переможця закупівлі базується на чітко визначених, прозоро задекларованих критеріях, які застосовуються до всіх учасників без виключень. Такий підхід дозволяє уникнути суб'єктивізму та забезпечує прийняття рішення, яке ґрунтується виключно на відповідності пропозицій встановленим вимогам та економічній доцільності.

6) *Запобігання корупційним діям і зловживанням.*

Основна мета цього принципу – мінімізувати можливості для незаконних дій та зловживань під час проведення закупівель. Впровадження електронних систем, чітка документальна процедура та контроль за дотриманням правил дозволяють створити систему, в якій прозорість і відповідальність стають головними механізмами запобігання корупції.

1.1.3 Основні види тендерів та їхні особливості

Існує декілька видів тендерів, кожен з яких має свої особливості, переваги та недоліки. Розглянемо основні з них:

1) **Відкриті тендери**

Відкриті тендери [4] є найбільш поширеною формою закупівель, що застосовуються державними установами. У цій процедурі участь можуть брати всі зацікавлені постачальники, які відповідають встановленим вимогам. Процес зазвичай включає публікацію оголошення про закупівлю, подання пропозицій учасниками, проведення аукціону (за наявності) та оцінку пропозицій для визначення переможця. Висока конкуренція сприяє отриманню оптимальних умов для замовника, а відкритість процедури знижує ризики шахрайства. Проте тривалість процесу та значні витрати на підготовку документації можуть бути його недоліками.

Переваги	**Недоліки**
Прозорість	Тривалість процесу
Конкурентність	Витрати на підготовку

Таблиця 1.1 – Переваги та недоліки відкритих тендерів

2) **Закриті тендери**

Закриті тендери передбачають обмежену участь постачальників, яких замовник запрошує безпосередньо. Ця процедура використовується, коли товари чи послуги можуть бути надані обмеженою кількістю постачальників або коли інформація про закупівлю є конфіденційною. Швидкість проведення може бути вищою за рахунок меншої кількості учасників, проте обмеження кола потенційних постачальників знижує рівень конкуренції, що може негативно позначитися на умовах закупівлі, а недостатня прозорість збільшує ризики корупційних дій.

Переваги	**Недоліки**
Швидкість проведення	Обмежена конкуренція
Конфіденційність	Ризики корупції

Таблиця 1.2 – Переваги та недоліки закритих тендерів

3) **Двоетапні тендери**

Двоетапні тендери [5] застосовуються у випадках, коли замовник не може чітко визначити технічні характеристики або інші аспекти закупівлі. Процедура складається з двох етапів: спочатку учасники подають попередні пропозиції без зазначення ціни, а потім – доопрацьовані

пропозиції з уточненими вимогами та визначенням вартості. Такий підхід дозволяє підвищити ефективність у складних закупівлях, де необхідна гнучкість, та зменшити ризики шахрайства, але водночас процедура є більш складною та тривалою.

Переваги	**Недоліки**
Гнучкість	Складність
Зменшення ризиків шахрайства	Тривалість

Таблиця 1.3 – Переваги та недоліки двоетапних тендерів

4) **Інші види тендерів**

- *Конкурентний діалог*

Застосовується для складних контрактів, коли замовник веде діалог з відібраними учасниками для визначення оптимальних рішень перед поданням остаточних пропозицій;

- *Торги з обмеженою участю*

Передбачає собою процедуру, в якій участь беруть лише ті постачальники, які пройшли попередню кваліфікацію.

Переваги	**Недоліки**
Ефективність	Обмежена конкуренція
Зменшення ризиків невиконання	Ризики корупції

Таблиця 1.4 – Переваги та недоліки інших видів тендерів

Ці види тендерів дозволяють замовнику більш точно визначити постачальника, що відповідає специфічним вимогам, підвищуючи

ефективність та знижуючи ризики невиконання контракту. Однак, обмеження конкуренції може призвести до менш вигідних умов та підвищити ризики.

1.2 Сучасні методи проведення тендерних закупівель

Сучасні тендерні закупівлі стрімко еволюціонують завдяки впровадженню цифрових технологій. Вони поділяються на два основні підходи: традиційний, що базується на паперових процедурах і ручному опрацюванні, та електронний, який використовує цифрові платформи, автоматизацію процесів і смарт-контракти. Кожен із них має свої особливості, переваги та недоліки [6].

1.2.1 Традиційні системи тендерів

Традиційні системи тендерних закупівель передбачають паперову форму проведення процедур. Учасники подають свої пропозиції у фізичному вигляді, а процес оцінки та вибору переможця здійснюється вручну. Цей метод є історично першим способом проведення тендерів і широко застосовувався до впровадження електронних систем. Незважаючи на те, що він дозволяє компаніям брати участь без необхідності використання цифрових технологій, процес залишається тривалим і менш прозорим.

Тривалість оцінки пропозицій та значні адміністративні витрати роблять традиційні тендери менш ефективними порівняно з сучасними цифровими альтернативами. Крім того, відсутність автоматизації ускладнює боротьбу з корупційними ризиками та людським фактором у процесі відбору переможця.

1.2.2 Електронні системи тендерів

Електронні системи закупівель передбачають використання цифрових платформ для проведення всіх етапів тендерного процесу — від оголошення закупівлі до укладення договору. Завдяки автоматизації та цифровізації ці системи значно підвищують ефективність закупівель, скорочують час обробки пропозицій і зменшують адміністративні витрати. Вони сприяють відкритості процесу, оскільки всі учасники мають рівний доступ до інформації та можуть відстежувати кожен етап закупівлі.

Електронні системи також дозволяють автоматично перевіряти відповідність пропозицій встановленим критеріям, що зменшує вплив людського фактору і ризик суб'єктивних рішень. Проте їх використання вимагає певного рівня цифрової грамотності від учасників, а також надійної кібербезпеки для захисту даних.

Приклади державних платформ:

• *Prozorro (Україна) [7]:* національна електронна система публічних закупівель, створена для забезпечення максимальної прозорості та ефективності державних закупівель. Система працює за принципом «всі бачать все», що дозволяє кожному зацікавленому спостерігати за всіма етапами тендерного процесу в режимі реального часу. Спільний проект українського уряду, бізнесу та громадянського суспільства, Prozorro сприяв значному зниженню корупційних ризиків та підвищенню конкуренції на ринку державних закупівель.

• *TED (Tenders Electronic Daily) (Європейський Союз) [8]:* офіційний онлайн-портал для публікації інформації про державні закупівлі в країнах-членах Європейського Союзу. Платформа забезпечує доступ до тендерів з усіх держав ЄС, сприяючи підвищенню прозорості та створенню умов для конкуренції на спільному ринку. TED дозволяє бізнесу з різних країн легко знаходити та брати участь у публічних закупівлях.

• *Government e Marketplace (GeM) (Індія) [9]:* інтегрована онлайн-платформа, розроблена для підвищення ефективності, прозорості та інклюзивності державних закупівель в Індії. Система централізує процес закупівель, забезпечуючи державні установи можливістю здійснювати покупки товарів та послуг через єдиний портал. Це дозволяє оптимізувати закупівельні процеси, сприяти залученню широкого кола постачальників та знижувати адміністративні витрати.

• *Gov.uk Contracts Finder (Велика Британія) [10]:* онлайн-платформа, на якій публікуються державні контракти, що перевищують певну вартість (зазвичай понад £10,000). Платформа забезпечує відкритий доступ до інформації про державні закупівлі, сприяючи прозорості процесу та надаючи бізнесу можливість оперативно знаходити та аналізувати тендерні пропозиції.

Перехід від традиційних до електронних систем тендерних закупівель є світовою тенденцією, спрямованою на підвищення ефективності, прозорості та зменшення корупційних ризиків у сфері державних закупівель.

Автоматизація процесів тендерних закупівель [11] полягає у використанні програмних засобів для виконання рутинних та повторюваних завдань, таких як:

• *автоматичне повідомлення про нові тендери:* учасники отримують сповіщення про нові можливості, що відповідають їхнім критеріям.

• *автоматизована оцінка пропозицій:* системи можуть автоматично оцінювати пропозиції на відповідність встановленим критеріям, що зменшує людський фактор та можливі помилки.

• *моніторинг та звітність:* системи автоматично генерують звіти та аналізують дані для виявлення можливих порушень або аномалій.

Використання таких підходів підвищує ефективність процесу закупівель, зменшує витрати часу та ресурсів, а також підвищує прозорість та підзвітність.

Використання смарт-контрактів у комерційних тендерах:

Означення 1.9. Смарт–контракти [12] — це самовиконувані контракти з умовами угоди, написаними в коді, які працюють на блокчейн-платформах.

У контексті комерційних тендерів смарт-контракти можуть забезпечити:

• *автоматизацію виконання умов контракту:* наприклад, автоматичне перерахування коштів постачальнику після підтвердження доставки товару або послуги.

• *зменшення потреби в посередниках:* смарт-контракти виконуються автоматично, що знижує потребу в третіх сторонах для забезпечення виконання умов угоди.

• *підвищення прозорості та довіри:* усі умови та транзакції в смарт-контрактах записуються в блокчейн, що забезпечує незмінність та доступність інформації для всіх учасників.

Впровадження смарт-контрактів у комерційні тендери може значно підвищити ефективність та безпеку процесів, зменшити ризики шахрайства та забезпечити автоматичне виконання умов угоди.

1.3 Процедура проведення тендеру

Ефективна процедура проведення тендеру є ключовою для забезпечення прозорості, чесної конкуренції та оптимального використання ресурсів. Вона регулюється відповідними стандартами та нормативними вимогами, а її успішність залежить від чітко визначених етапів та впливу різних факторів.

1.3.1 Основні етапи тендерного процесу

Процес проведення тендеру включає 6 основних етапів [13], які забезпечують послідовність, об'єктивність і результативність закупівель:

1) **Оголошення тендеру**

Замовник починає процес із публічного оголошення про проведення тендеру, де зазначає свої потреби, основні вимоги до товарів, послуг або робіт, а також терміни подання пропозицій і критерії їх оцінки.

Основною метою цього етапу є забезпечення відкритості та доступності інформації для всіх потенційних учасників, що дозволяє створити конкурентне середовище.

2) **Подача заявок**

Після оголошення тендеру зацікавлені постачальники готують і подають свої тендерні пропозиції. Ці заявки мають містити як технічну частину (опис товарів, робіт чи послуг), так і комерційну частину (розрахунок вартості, умови оплати, гарантії). Важливою вимогою є своєчасне та точне подання всіх необхідних документів згідно з тендерною документацією.

3) **Розгляд та оцінка пропозицій**

На цьому етапі тендерний комітет проводить детальний аналіз усіх отриманих пропозицій. Оцінка здійснюється за встановленими критеріями – відповідність технічним вимогам, конкурентність ціни, досвід та репутація постачальника, юридична чистота. За потреби можуть проводитися переговори для уточнення деталей або внесення коригувань до заявок. Ретельний аналіз дозволяє вибрати найбільш економічно та технічно вигідну пропозицію.

4) **Вибір переможця**

Після завершення оцінки тендерний комітет обирає переможця, який найкраще відповідає всім встановленим вимогам. Це рішення повинне бути прозорим, обґрунтованим і задокументованим, що гарантує чесність

і відкритість процедури.

5) **Підписання контракту**

На цьому етапі замовник та переможець тендеру формалізують свої домовленості шляхом укладання контракту. У документі чітко прописуються умови виконання, зокрема обсяг робіт, терміни, ціна, гарантії якості та санкції за невиконання. Підписання контракту стає юридичним зобов'язанням для обох сторін і є необхідним кроком для переходу до виконання закупівлі.

6) **Контроль виконання договору**

Після укладення контракту проводиться постійний моніторинг виконання зобов'язань. Це включає перевірку якості поставлених товарів або наданих послуг, проведення фінансових аудитів, аналіз відповідності виконання умов контракту і підготовку звітності. Систематичний контроль дозволяє своєчасно виявити і виправити можливі порушення, що сприяє успішній реалізації закупівлі.

Варто зазначити, що попри те, що базова структура тендерного процесу складається з 6 основних етапів, конкретна реалізація окремих кроків може варіюватися залежно від типу тендеру. Наприклад, у двоетапних тендерах окрім стандартних етапів проводиться додатковий попередній етап, на якому учасники подають попередні пропозиції без остаточного ціноутворення, а на другому етапі – доопрацьовані пропозиції з уточненими вимогами та вказаними цінами. Аналогічно, у процедурах конкурентного діалогу або переговорних тендерах можуть бути введені додаткові етапи для обговорення деталей і коригування пропозицій.

1.3.2 Регламенти та стандарти проведення тендерів

Публічні закупівлі регулюються широким спектром нормативних документів, що охоплюють нормативно-правові акти, стандарти провідних міжнародних організацій та внутрішні регламенти окремих установ [14]. Вони спрямовані на забезпечення прозорості, чесної

конкуренції, ефективного витрачання коштів та запобігання корупційним ризикам. Залежно від рівня застосування, регламенти умовно поділяються на:

1) **Нормативно-правові акти**

Національні нормативно-правові акти України:

• *Закон України «Про публічні закупівлі».* Цей закон є основним документом, що регулює сферу публічних закупівель в Україні. Він визначає загальні принципи та порядок проведення закупівель, права та обов'язки учасників, процедури оскарження та контролю.

• *Постанови Кабінету Міністрів України.* Такі постанови встановлюють особливості створення та діяльності централізованих закупівельних організацій, а також регламентують взаємодію між ними та замовниками. Наприклад, Постанова № 1178 від 12.10.2022 «Про затвердження особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України 'Про публічні закупівлі', на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування» [15].

• *Накази Міністерства економіки України.* Ці накази деталізують окремі аспекти проведення закупівель, такі як методики визначення очікуваної вартості, вимоги до тендерної документації та інші. Наприклад, Наказ № 40 від 08.06.2021 «Про затвердження Примірного положення про уповноважену особу» визначає вимоги до фахівців, відповідальних за проведення закупівель [16].

Міжнародні нормативно-правові акти:

• *Угода СОТ про державні закупівлі (GPA) [17].* Ця угода встановлює загальні принципи та процедури для державних закупівель серед країн-членів Світової організації торгівлі.

• *Директива 2014/24/ЄС Європейського Парламенту та Ради від 26 лютого 2014 року про державні закупівлі [18].* Ця директива встановлює правила для державних закупівель у країнах ЄС, спрямовані на забезпечення відкритості та конкуренції.

• *Директива 2014/25/ЄС Європейського Парламенту та Ради від 26 лютого 2014 року про закупівлі суб'єктами господарювання, що здійснюють діяльність у секторах водопостачання, енергетики, транспорту та поштових послуг [19].* Ця директива регулює специфічні аспекти закупівель у зазначених секторах.

2) **Міжнародні стандарти**

• *Типовий закон ЮНСІТРАЛ про публічні закупівлі.* Розроблений Комісією ООН з права міжнародної торгівлі, цей закон надає рекомендації щодо проведення публічних закупівель, які можуть бути адаптовані країнами для вдосконалення власних систем закупівель.

• *Керівні принципи ОЕСР щодо публічних закупівель.* Організація економічного співробітництва та розвитку розробила рекомендації для забезпечення цілісності, прозорості та ефективності публічних закупівель.

3) **Внутрішні регламенти**

• *Положення про тендерний комітет або уповноважену особу.* Ці документи визначають склад, повноваження та порядок роботи осіб або комітетів, відповідальних за організацію та проведення закупівель у конкретній установі.

• *Інструкції щодо підготовки та проведення закупівель.* Внутрішні документи організацій, які деталізують процедури планування, оголошення, оцінки та укладання договорів про закупівлю.

1.3.3 Фактори, що впливають на ефективність тендерних закупівель

Ефективність тендерних закупівель залежить від низки факторів, які впливають на прозорість, конкурентність та загальну результативність тендерних процедур. Нижче розглянемо ключові з них:

1) **Прозорість процесу**

Прозорість є фундаментальним принципом, який забезпечує довіру до

тендерних процедур. Відкритий доступ до інформації про всі етапи закупівлі дозволяє учасникам та громадськості контролювати процес, зменшуючи можливості для корупції та нечесної конкуренції. Системи електронних закупівель, такі як Prozorro, забезпечують публічний доступ до даних про тендери, що підвищує прозорість процесу [20].

2) **Конкурентність серед учасників**

Високий рівень конкуренції стимулює постачальників пропонувати кращі умови, що призводить до економії бюджетних коштів та підвищення якості товарів чи послуг. Публічне оголошення про тендери та відкритий доступ до участі сприяють залученню більшої кількості учасників, що підвищує конкурентність [21].

3) **Якість тендерної документації**

Чітко визначені вимоги та критерії оцінки у тендерній документації зменшують ризики непорозумінь та спорів. Деталізація технічних параметрів, кваліфікаційних критеріїв та умов договору забезпечує об'єктивність оцінки пропозицій та сприяє вибору найкращого постачальника.

4) **Професіоналізм та компетентність закупівельників**

Кваліфіковані фахівці, які володіють знаннями у сфері закупівель, здатні ефективно організувати та провести тендерні процедури, мінімізуючи ризики помилок та порушень. Постійне навчання та підвищення кваліфікації персоналу є важливим аспектом успішних закупівель.

5) **Використання сучасних технологій**

Інтеграція цифрових рішень, таких як електронні платформи та автоматизовані системи, спрощує процеси, зменшує людський фактор та підвищує ефективність закупівель. Наприклад, впровадження блокчейн технологій може забезпечити незмінність даних та підвищити довіру до системи.

6) **Нормативно-правове регулювання**

Чітке та зрозуміле законодавство у сфері публічних закупівель створює стабільне середовище для проведення тендерів. Дотримання міжнародних

стандартів та національних нормативно-правових актів забезпечує єдині правила гри для всіх учасників ринку.

7) **Планування та аналіз ринку**

Попереднє дослідження ринку, аналіз потенційних постачальників та цінових пропозицій дозволяють замовникам формувати реалістичні очікування та бюджети. Це сприяє отриманню конкурентоспроможних пропозицій та запобігає необґрунтованим витратам.

8) **Зворотний зв'язок та аналіз результатів**

Оцінка проведених тендерів, аналіз успішних та проблемних аспектів дозволяють вдосконалювати процеси та підвищувати ефективність майбутніх закупівель. Збір та врахування відгуків учасників сприяють покращенню процедур та підвищенню довіри до системи.

Врахування та оптимізація зазначених факторів сприяють раціональному використанню ресурсів та досягненню поставлених цілей.

1.4 Аналіз переваг та недоліків існуючих методів

Сучасні методи проведення тендерних закупівель можуть істотно відрізнятися за рівнем прозорості, швидкості та складності впровадження. Нижче наведено порівняльну таблицю, що допоможе оцінити переваги та недоліки основних підходів.

Особливість / Методи	**Традиційні**	**Електронні**
Прозорість	-	+
Швидкість	-	+
Управління даними	-	+
Ризики корупції	+	-
Тривалість процедур	+	-
Високі витрати	+	-
Оперативність змін	-	+
Потреба тех. забезпечення	-	+
Можливі технічні збої	-	+
Високі вимоги до безпеки	-	+
Потреба навчання персоналу	-	+

Таблиця 1.5 – Порівняння методів проведення тендерних закупівель

Детальний аналіз за таблицею:

1) **Прозорість**

У Традиційних процедурах прозорість обмежена паперовим документообігом, де складно забезпечити оперативний доступ до інформації. В свою чергу, електронні системи підвищують рівень прозорості, оскільки всі дані знаходяться у відкритому цифровому просторі.

2) **Швидкість**

Традиційні тендери повільні, адже передбачають багато ручних процедур.

У випадку електронних систем надається змога швидко обробляти заявки, скорочуючи часові витрати.

3) **Управління даними**

Традиційні методи мають складнощі з пошуком та аналізом даних у паперових архівах. В той час як електронні платформи надають зручний інструментарій для обробки й аналізу інформації.

4) **Ризики корупції**

Традиційні процедури схильні до зловживань через брак прозорості. У електронних систем навпаки істотно знижуються корупційні ризики, оскільки всі дії відбуваються у відкритому цифровому середовищі.

5) **Тривалість процедур**

Традиційні методи можуть затягуватися через ручне опрацювання документів і логістику. В той час як електронні системи значно прискорюють процеси, завдяки швидкому обміну інформацією.

6) **Високі витрати**

У Традиційних системах витрати високі через паперовий документообіг, логістику й архівування. В свою чергу, електронні системи здебільшого знижують витрати на адміністрування, проте вимагають оплату IT-сервісів.

7) **Оперативність змін**

Традиційні процедури потребують переоформлення документів та повторної відправки. Електронні системи навпаки дозволяють швидко коригувати дані, але все ще вимагають дотримання формальних правил.

8) **Потреба технічного забезпечення**

Традиційні методи мають мінімальні вимоги: папір, засоби друку, поштові або кур'єрські послуги. У випадку електронних платформ потребуються IT-інфраструктури, стабільний інтернет та обладнання.

9) **Можливі технічні збої**

Традиційні методи схильні до людських помилок, але не залежать від IT-інфраструктури. В той час як електронні системи іноді можуть потерпати від системних або мережевих збоїв, вірусних атак чи втрати даних, однак

більшість сучасних платформ мають резервні механізми відновлення.

10) **Високі вимоги до безпеки**

Традиційні процедури легко підробити (фальшиві печатки, підписи), але немає ризиків витоку даних через хакерські атаки. В свою чергу, електронні платформи вимагають потужних засобів кібербезпеки та захисту від несанкціонованого доступу.

11) **Потреба навчання персоналу**

Традиційні методи майже не потребують додаткового навчання, адже всі знайомі з паперовими процедурами. У випадку електронні системи вимагають вміння працювати з програмними інструментами, заповнювати форми онлайн тощо.

Таким чином, наведена порівняльна таблиця і подальший аналіз демонструють, що жоден із методів не є універсально ідеальним. Кожен підхід має унікальні переваги та недоліки, тому вибір оптимального підходу залежить від конкретних цілей, обставин, наявних ресурсів, вимог до швидкості, прозорості та безпеки процесу закупівель. Вдале поєднання або поступовий перехід між методами дає змогу досягти максимальної ефективності тендерних процедур.

Висновки до розділу 1

Тендерні закупівлі є ключовим механізмом ефективного розподілу ресурсів, що базується на принципах відкритості, чесної конкуренції та економічної доцільності.

Розгляд процедури тендерів дозволив виділити ключові етапи, серед яких формування документації, оцінка пропозицій та контроль виконання контрактів. Визначено, що ефективність закупівель значною мірою залежить від регламентів, механізмів моніторингу та автоматизації процесів.

Порівняльний аналіз існуючих методів продемонстрував переваги

електронних закупівель, проте їх впровадження вимагає посиленої кібербезпеки та вдосконалення нормативно-правової бази. Подальший розвиток тендерних систем має орієнтуватися на впровадження блокчейн технологій, алгоритмічного аналізу пропозицій та автоматизованих механізмів контролю для підвищення ефективності та захищеності процесів.

2 АТАКИ НА ТЕНДЕРНІ ЗАКУПІВЛІ ТА РИЗИКИ ЇХ ПЕРЕНЕСЕННЯ У БЛОКЧЕЙН

В цьому розділі будуть розглядатись відомі загрози та шахрайські схеми у тендерах, технічні недоліки електронних систем, завдяки яким можливі ті чи інші атаки, а також ризики перенесення тендерної процедури у блокчейн.

2.1 Відомі загрози та шахрайські схеми у тендерах

Процеси публічних закупівель нерідко стають об'єктом зловживань, пов'язаних як із людським фактором, так і з технічними вадами систем. З метою виявлення потенційних загроз для безпеки та доброчесності тендерних процедур розглянемо найпоширеніші ризики, що виникають на практиці.

2.1.1 Корупційні схеми та маніпуляції

У сфері тендерних закупівель існують різноманітні корупційні схеми та маніпуляції, які підривають прозорість і справедливість тендерних процедур. Розглянемо детальніше основні з них:

1) **Підтасовка результатів тендеру**

Схема передбачає навмисне викривлення оцінки пропозицій учасників з метою забезпечення перемоги заздалегідь обраного постачальника. Це може включати маніпуляції з оцінювальними балами, ігнорування недоліків обраного учасника або необґрунтоване відхилення пропозицій конкурентів. Такі дії призводять до неефективного використання бюджетних коштів та знижують довіру до системи публічних закупівель. У деяких розслідуваннях антикорупційних органів України було

встановлено випадки підтасовки результатів, що призводило до неефективного використання державних коштів та підривало довіру до системи закупівель [22].

2) **Змова учасників**

Змова учасників, або картельна змова, виникає, коли декілька компаній координують свої дії для маніпулювання результатами тендеру. Це може проявлятися у поданні фіктивних пропозицій, узгодженні цін або розподілі ринків. Ознаками змови можуть бути схожість документів, подання пропозицій з одного IP-адреси або використання однакових контактних даних. Такі дії порушують принципи добросовісної конкуренції та можуть призвести до завищення цін на товари чи послуги. Наприклад, у ряді європейських тендерних процедур було виявлено, що будівельні компанії узгоджували ставки для отримання державних контрактів, що негативно впливало на якість робіт та призводило до завищення вартості проектів [23].

3) **Підробка документів**

Даний тип шахрайства включає надання фальшивих документів, таких як сертифікати якості, ліцензії чи фінансові звіти для відповідності кваліфікаційним вимогам тендеру. Підроблені документи дозволяють учасникам, які фактично не відповідають вимогам, брати участь у тендері, що може призвести до неякісного виконання контрактів та фінансових втрат для замовника.

4) **Лобіювання**

Лобіювання в контексті тендерних закупівель передбачає використання неформальних засобів впливу на посадових осіб з метою прийняття рішень на користь певного учасника. Це може включати неформальні домовленості, надання подарунків, хабарів або інших вигод, що підривають принципи прозорості та об'єктивності, оскільки рішення приймаються не на основі якості пропозицій, а під впливом особистих інтересів.

Для мінімізації зазначених корупційних ризиків важливо

впроваджувати ефективні механізми контролю, забезпечувати прозорість процедур та підвищувати відповідальність посадових осіб за прийняті рішення.

2.1.2 Шахрайські дії з боку учасників та організаторів

У сфері тендерних закупівель існують різноманітні шахрайські схеми, які використовують як окремі учасники, так і організатори для отримання незаконних переваг. Серед них варто виділити наступні:

1) **Використання підставних компаній**

Цей вид шахрайства полягає у створенні або використанні фіктивних (shell) компаній для участі в тендерних процедурах. Підставні компанії часто реєструються з метою обходу кваліфікаційних вимог або для приховування справжньої ідентичності учасників тендеру. Таким чином, навіть коли здається, що в тендері бере участь багато незалежних компаній, реальна конкуренція відсутня, оскільки всі вони мають спільний контроль [24].

Наприклад, у розслідуваннях, проведених НАБУ, було встановлено випадки використання підставних компаній для маніпулювання результатами тендерів, що призводило до отримання контрактів заздалегідь обраним постачальникам.

2) **Заниження цін**

Поширена шахрайська схема, коли учасники тендеру подають пропозиції з надзвичайно низькою вартістю, що значно відрізняється від ринкових показників. Таке "заниження"може бути частиною змови між учасниками, які узгоджують свої ставки задля забезпечення перемоги певного суб'єкта, або використано як тактика для примусу до укладення контракту за неекономічно вигідними умовами. В результаті, після виграшу тендеру, постачальники часто не можуть забезпечити належну якість чи виконати контракт у встановлені терміни, що знижує ефективність закупівель і збільшує ризик порушення умов договору.

Подібні схеми описані як у міжнародних, так і в українських дослідженнях з публічних закупівель, зокрема в документах Світового банку та OECD Guidelines for Integrity in Public Procurement.

3) **Недобросовісне виконання контрактів**

Даний тип шахрайства характеризується тим, що після отримання контракту переможець тендеру навмисно порушує умови контракту або виконує їх на неналежному рівні. Це може проявлятися у вигляді постачання неякісних товарів або послуг, порушенні встановлених термінів, або невиконанні частин контракту, що призводить до значних фінансових втрат для замовника. Недобросовісне виконання часто є наслідком попередньої змови або недостатнього контролю з боку замовника, що в кінцевому результаті призводить до фінансових втрат і погіршення репутації системи публічних закупівель.

У розслідуваннях як Європейському Союзі, так і в Україні зафіксовано випадки, коли недобросовісне виконання контрактів стало результатом узгоджених дій між учасниками та/або організаторами тендерів.

Таким чином, зазначені шахрайські дії мають серйозний вплив на ефективність тендерних закупівель, підривають конкуренцію та довіру до системи, і можуть призвести до значних фінансових втрат. Боротися з такими схемами можна за допомогою підвищення прозорості, автоматизації процесів, впровадження електронних систем та суворого контролю з боку антикорупційних органів.

2.1.3 Технічні вразливості електронних тендерних систем

Електронні тендерні системи покликані забезпечувати прозорість та ефективність державних і приватних закупівель. Проте, як і будь-яка інформаційна система, вони можуть бути вразливими до кіберзагроз.

1) **Атаки на сервери тендерних платформ**

Даний вид атак спрямований на отримання несанкціонованого доступу до критичних даних або зміну інформації про учасників та їхні пропозиції.

Основні методи атак включають:

• *SQL-ін'єкції:* атака, що дозволяє зловмисникам маніпулювати базами даних шляхом введення шкідливого SQL-коду через веб-інтерфейси. Це може призвести до викрадення або зміни заявок, видалення важливих даних або отримання адміністративного доступу;

• *використання вразливостей у веб-додатках:* недоліки в коді тендерних платформ можуть дозволяти атаки типу XSS (Cross-Site Scripting) та CSRF (Cross-Site Request Forgery), які сприяють викраденню облікових даних користувачів або зміні інформації без їхнього відома;

• *атаки через бекдори (backdoors):* якщо зловмисники отримують доступ до серверів через вразливості операційної системи або встановлюють шкідливе програмне забезпечення, вони можуть контролювати роботу тендерної системи, змінювати умови закупівель або маніпулювати процесом визначення переможців.

2) **DDoS-атаки**

Один із найпоширеніших методів атак на електронні тендерні платформи. Їхня мета — перевантажити сервери великою кількістю запитів, що робить систему недоступною для користувачів. Наслідки таких атак включають:

• *зрив тендерних процедур:* якщо система не працює у критичний момент (наприклад, під час подання заявок або вибору переможця), це може призвести до скасування тендеру або його перенесення;

• *створення умов для маніпуляцій:* DDoS-атака може бути інструментом змови, коли недобросовісний учасник атакує платформу, щоб перешкодити конкурентам вчасно подати документи;

• *фінансові збитки:* організаторам доводиться витрачати ресурси на відновлення роботи системи, а учасники можуть зазнавати втрат через неможливість брати участь у торгах.

3) **Підробка цифрових підписів**

Електронні тендерні системи широко використовують цифрові підписи для підтвердження автентичності документів та учасників. Проте, якщо система має слабкі алгоритми захисту або зловмисники отримують

доступ до особистих ключів, можливі такі загрози:

• *підміна документів:* хакери можуть змінити подані заявки, підробити документи або підписати від імені іншої компанії;

• *перехоплення та крадіжка ключів:* якщо система зберігання приватних ключів ненадійна, вони можуть бути викрадені та використані для фальсифікації підписів;

• *атаки на криптографічні алгоритми:* використання застарілих або ненадійних алгоритмів підпису може дозволити злому підпису за допомогою квантових або обчислювально-інтенсивних атак.

Ці загрози свідчать про необхідність постійного вдосконалення механізмів захисту електронних тендерних систем шляхом використання сучасних методів шифрування та захисту даних, регулярного аудиту безпеки систем, впровадження механізмів моніторингу та раннього виявлення аномалій, а також використання стійких алгоритмів цифрового підпису та апаратних ключів для підписування документів.

2.2 Ризики перенесення тендерних закупівель у блокчейн

Перенесення тендерних закупівель у блокчейн може значно підвищити прозорість та усунути корупційні ризики. Проте й тут існують вразливості та недоліки, якими можуть скористатися зловмисники.

2.2.1 Безпека смарт-контрактів та можливі атаки

Зокрема, смарт-контракти, які автоматизують тендерний процес, мають певні вразливості. Розглянемо детальніше основні з них:

1) **Атака повторного входу (Reentrancy attack)**

Даний вид атаки виникає, коли смарт-контракт викликає зовнішній контракт перед оновленням свого стану. Якщо зовнішній контракт містить шкідливий код, він може повторно викликати оригінальний

контракт і отримати доступ до ресурсів (наприклад, ETH)), перш ніж завершиться початковий виклик.

У випадку тендерних закупівель: якщо учасник, що програв тендер, може отримати повернення застави, він може використати атаку повторного входу, щоб отримати кошти кілька разів.

Одним із найвідоміших прикладів reentrancy-атаки є взлом The DAO (2016) [25]. Через цю вразливість хакери вивели 3,6 млн ETH, що еквівалентно близько 6,8 млрд доларів станом на 2023 рік. Це призвело до розколу мережі Ethereum та створення Ethereum Classic.

2) **Атака маніпуляцією часу (Time Manipulation attack)**

Смарт-контракти можуть покладатися на `block.timestamp`, який майнери можуть змінювати в межах дозволеного діапазону (до 15 секунд). Це дозволяє маніпулювати часом, що може бути використано для шахрайства в лотереях, ставках або фармінгу токенів.

Наприклад, якщо контракт визначає переможця за `block.timestamp`, майнер може змінити час, щоб маніпулювати результатом на користь певного учасника.

3) **Атака на випередження (Front-Running attack)**

Дана атака відбувається, коли зловмисник спостерігає транзакцію після того, як користувач її надіслав, і вона очікує в пулі пам'яті (особливість блокчейну, що транзакції у мемпулі видно до їх виконання). Таким чином, зловмисник може відправити свою транзакцію з вищою комісією та випередити жертву.

Наприклад, учасник тендеру може перехопити пропозицію іншого учасника, якщо транзакції відправляються у відкритий мемпул. Таким чином, змінивши свою ставку, щоб виграти тендер несправедливо.

4) **Переповнення чисел (Integer Overflow/Underflow)**

Ці атаки виникають, коли змінна виходить за межі дозволеного діапазону. Наприклад, якщо змінна uint8 (ціле число від 0 до 255) зменшиться на 1, вона стане 255, що може призвести до критичних помилок у контракті.

У випадку тендерних закупівель: якщо тендерний смарт-контракт працює

з числовими значеннями (наприклад, ставки у тендері), то некоректне обчислення може призвести до переповнення (overflow), що може дати змогу зловмиснику зробити ставку безкоштовно.

У 2018 році проект BeautyChain (BEC) зазнав атаки integer overflow, внаслідок якої хакери змогли створити величезну кількість токенів і обвалити їхню вартість [26].

5) **Змова між учасниками (Collusion attack)**

Дана атака передбачає, що учасники можуть домовитися та змінити свої ставки, до того ж ще й в останній момент, оскільки всі дані на блокчейні публічні.

Наприклад, група підрядників може синхронізувати ставки в останній момент, щоб створити видимість конкурентного тендеру, але уникнути справжньої конкуренції.

6) **Флеш-кредити (Flash Loan attack)**

Flash Loans дозволяють брати величезні кредити без застави, якщо вони повертаються у межах одного блоку. Це може використовуватись для маніпуляцій цінами, ліквідацій позик, крадіжки коштів із DeFi-протоколів.

Наприклад, якщо тендер передбачає фінансові зобов'язання або механізм авансів/депозитів, атаки через флеш-кредити можуть використовуватися для маніпуляцій (штучного підвищення ставок і т.п.).

7) **Маніпуляція оракулами (Oracle Manipulation attack)**

Смарт-контракти часто використовують oracles для отримання зовнішніх даних (наприклад, курс валют або ціни активів). Якщо зловмисник отримає контроль над oracle або подасть йому фальшиві дані, він може маніпулювати умовами тендера.

У 2020 році хакери атакували проект bZx через oracle-маніпуляцію, використовуючи флеш-кредити (flash loans). Вони тимчасово змінили курс активів та отримали прибуток у розмірі 370 000 доларів [27].

8) **Прихована цензура (Soft Censorship)**

У блокчейн-системах цензура можлива, коли вузли мережі (майнери або

валідатори) навмисно відхиляють певні транзакції або блоки. Це може бути використано для впливу на тендерний процес.

У мережі Ethereum soft censorship стала проблемою у 2022 році після запровадження санкцій OFAC. Деякі валідатори почали відхиляти певні транзакції, що викликало дебати про децентралізацію [28].

9) **Зависання контракту (Contract Freezing)**

Зависання контракту відбувається, коли функціонал контракту блокується через критичну помилку або несправну логіку, що робить контракт нефункціональним.

У випадку тендерних закупівель: якщо контракт має критичні функції (наприклад, повернення депозитів), його зависання може призвести до фінансових втрат

Один із найгучніших випадків – Parity Wallet Hack (2017), де помилка в коді призвела до замороження 513 774 ETH (280 млн доларів) [29].

2.2.2 Атаки на блокчейн-мережі

Окрім смарт-контрактів, самі блокчейн-мережі вразливі до певних атак, які можуть поставити під загрозу надійність та цілісність системи.

1) **Атака** 51%

Атака 51% виникає в блокчейн-мережах, що використовують PoW або PoS, коли одна група майнерів або валідаторів отримує контроль над більш ніж 50% обчислювальної потужності (у випадку PoW) або частки стейкінгу (у випадку PoS). Завдяки цьому зловмисник може маніпулювати процесом валідації блоків: він може переписувати історію транзакцій, здійснювати подвійні витрати (double spending) та тимчасово блокувати підтвердження нових транзакцій. Хоча у великих мережах, таких як Bitcoin, здійснення такої атаки є вкрай складним через величезну сумарну потужність мережі, менш популярні або нові проекти можуть стати об'єктом таких атак.

У випадку тендерних закупівель: якщо тендерний контракт працює на маленькому блокчейні, атака 51% може відкотити блок, в якому вигідна

ставка була подана чесно з метою перемоги іншого учасника.

Наприклад, у 2020 році була здійснена атака на Ethereum Classic (ETC) завдяки якій зловмисники отримали контроль над мережею та здійснили подвійне витрачання на суму понад 5 мільйонів доларів. Також, трохи раніше — у 2018 році відбулась атака на Bitcoin Gold (BTG), у результаті якої біржі втратили близько 18 мільйонів доларів через атаку 51% [30].

2) **Сибіл-атака (Sybil Attack)**

Сибіл-атака полягає у створенні великої кількості фальшивих ідентичностей (ноди, акаунти), які діють узгоджено для впливу на мережу. Зловмисник, створивши численні псевдоніми, може маніпулювати голосуваннями, змінювати розподіл ролей у мережі або спотворювати результати процесів, які залежать від розподіленої участі. Ця атака є особливо небезпечною для систем, де контроль за ідентичністю вузлів не забезпечено достатніми механізмами верифікації, що може знизити рівень децентралізації та безпеки мережі.

У випадку тендерних закупівель: якщо в тендері немає жорсткої перевірки учасників, зловмисники можуть створити видимість конкуренції, шляхом створення фальшивих облікових записів з метою маніпуляції тендером.

Наприклад, у 2014 році була відбулась сибіл-атака (Tor Network Attack) з метою перехоплення анонімного трафіку. А через рік — у 2015 дослідники виявили у Bitcoin P2P Network, що через сибіл-атаку можна здійснювати deanonymization-атаки [31].

3) **Атаки на рівні мережевої інфраструктури**

Атаки, що спрямовані на мережеву інфраструктуру, включають кілька напрямків:

- *DDoS-атаки*;
- *Атаки типу Eclipse (екліптичні атаки)*, при якій зловмисник ізолює окремий вузол або групу вузлів, змушуючи їх взаємодіяти лише з атакуючою стороною. Це може призвести до маніпуляції інформацією, яка надходить до ізольованих вузлів, і порушення цілісності процесу валідації транзакцій.

• *Маршрутизаційні атаки (наприклад, через BGP)*, в яких зловмисники можуть маніпулювати маршрутами передачі даних між вузлами, що може спричинити затримки або втрату важливої інформації в мережі. Цей тип атаки є серйозною загрозою для розподілених систем, оскільки може порушити нормальну роботу всієї мережі.

У випадку тендерних закупівель: якщо учасники тендеру залежать від мережевого з'єднання, BGP-атака може відключити певний регіон, і частина учасників не зможе подати заявки.

Наприклад, у 2015 році дослідники виявили Bitcoin Eclipse Attack [32], при якій можлива ізоляція Bitcoin-нод. А вже у 2020 році була здійснена атака на Ethereum Classic, яка включала BGP Hijacking, що спричинило втрату зв'язку між нодами [32].

Висновки до розділу 2

Аналіз загроз та шахрайських схем у тендерних закупівлях показав, що як традиційні, так і електронні системи залишаються вразливими до атак і маніпуляцій. Корупційні схеми, підробка документів, змови учасників та використання фіктивних компаній є поширеними проблемами. Електронні тендерні платформи підвищують прозорість, проте залишаються вразливими до DDoS-атак, зламу серверів, компрометації цифрових підписів та маніпуляцій із даними.

Перенесення тендерних закупівель у блокчейн потенційно може усунути низку загроз завдяки децентралізації, незмінності даних та автоматизації через смарт-контракти. Однак блокчейн-системи також мають свої ризики: атаки на смарт-контракти (reentrancy, маніпуляції з Oracle), атаки 51%, цензура транзакцій та вразливості на рівні мережевої інфраструктури.

Для безпечного впровадження блокчейну необхідний комплексний підхід: вдосконалення безпеки смарт-контрактів, аудит коду, використання децентралізованих Oracle, механізми захисту від сибіл-атак та надійні криптографічні технології.

3 РОЗРОБКА МЕТОДІВ З ВИКОРИСТАННЯМ VRF ТА DKG

У цьому розділі розглядаються основи технології блокчейн та її властивості, зокрема її визначення та основні властивості, а також спроби впровадження блокчейну в публічні закупівлі. Окрема увага приділяється криптографічним інструментам VRF та DKG, які можуть бути використані для вирішення існуючих проблем. Також в розділі описано і проаналізовано нові методи проведення тендерних закупівель із застосуванням зазначених технологій.

3.1 Поняття технології блокчейн

Блокчейн є фундаментальною технологією, що лежить в основі сучасних розподілених систем та застосовується у багатьох сферах, де важлива надійність і прозорість зберігання даних. Нижче наведено базове визначення та ключові особливості цієї технології.

Означення 3.1. Блокчейн (англ. Blockchain) [33] — це децентралізована база даних або реєстр, в якій інформація зберігається у вигляді ланцюга блоків, кожен з яких містить геш попереднього блоку, часову мітку та дані транзакцій. Особливістю є незмінність даних за рахунок лінійного порядку зв'язних блоків і розподіленого зберігання.

Взагалі, термін «блокчейн» уперше здобув широке застосування завдяки криптовалюті Bitcoin, однак надалі ця технологія була адаптована для десятків галузей — фінансів, охорони здоров'я, ідентифікації, логістики, та, зокрема, державного управління і публічних закупівель.

Основні властивості блокчейну:

• Децентралізація (англ. decentralization): інформація не зберігається на одному сервері — кожен учасник мережі володіє копією

реєстру. У публічних тендерах це дозволяє зменшити ризики корупції та втручання адміністратора.

• Незмінність (англ. immutability): дані, які одного разу були записані в блокчейн, не можуть бути змінені чи видалені без погодження більшості учасників мережі. Це гарантує цілісність записів запобігає запобігає ретроспективному редагуванню інформації, наприклад, щодо результатів тендеру.

• Консенсус (англ. consensus): усі зміни в системі відбуваються лише після досягнення згоди між вузлами мережі згідно з вибраним консенсусним алгоритмом (наприклад, Proof of Work, Proof of Stake або Practical Byzantine Fault Tolerance).

• Прозорість та верифікованість: більшість блокчейн-систем є відкритими для перегляду, що дозволяє будь-якому учаснику перевірити справжність транзакцій, простежити ланцюг операцій та здійснити аудит. При цьому зберігається псевдонімність — користувачі ідентифікуються за криптографічними адресами, що зберігає конфіденційність.

• Безпека: блокчейн базується на криптографічних принципах, зокрема використанні відкритих і закритих ключів, гешування, цифрових підписів. Завдяки цьому забезпечується захист даних від несанкціонованого доступу, а також автентичність і цілісність інформації.

Ці властивості створюють середовище, де довіра до платформи базується не на авторитеті якогось певного органа, а на математично формалізованих гарантіях.

3.2 Спроби впровадження блокчейну в публічні закупівлі

У випадку держзакупівель ключова ціль технології — підвищення прозорості та підзвітності. Вже існують окремі пілотні проєкти: наприклад, у 2017 році Баскський уряд (Іспанія) оголосив тендер (EJIE-133-2017) на впровадження блокчейну в реєстрі підрядників [34]. Схожі ініціативи стартували у Чилі та Перу, де державні платформи

держзакупівель запустили пілотні проєкти з використанням блокчейну для реєстрації тендерів і контрактів. Такі практики мають на меті забезпечити незмінність записів, відстеження змін у контрактах і запобігання «забутим» поправкам до тендерних умов.

Блокчейн створює відкритий реєстр усіх транзакцій та змін у документах, що ускладнює фальсифікацію даних. Завдяки цьому суттєво зростає контроль над процесом: для будь-якої дії залишається цифровий слід. Автоматизація через смарт-контракти скорочує бюрократію і підвищує оперативність.

Проте, сам по собі блокчейн не вирішує всіх викликів: хоча дані й незмінні, публічність реєстру створює ризики для конфіденційності, а смарт-контракти не мають вбудованих механізмів перевірки правильності прихованих дій. Для усунення цих недоліків у блокчейн-моделях закупівель дедалі частіше розглядають використання додаткових криптографічних інструментів.

3.3 Криптографічні інструменти для вирішення проблем у блокчейні

Вирішити згадані вище проблеми в контексті тендерних закупівель можуть сучасні криптографічні інструменти, а саме: верифіковані випадкові функції (VRF) та протоколи розподіленого генерування ключів (DKG).

3.3.1 Verifiable Random Function

Означення 3.2. Верифікована випадкова функція (англ. Verifiable Random Function, VRF) [35] — це криптографічна функція з відкритим ключем, яка генерує псевдовипадкові значення і забезпечує можливість їх верифікації.

Зокрема, вона може бути розглянута як розширена версія криптографічного гешу з відкритим ключем. Лише власник закритого ключа може обчислити геш, але кожен, хто має відкритий ключ, може перевірити правильність гешу. VRF корисні для запобігання перерахуванню структур даних на основі гешу.

Як випливає з назви, будь-яка випадкова функція з верифікацією визначається її основними характеристиками:

• Перевіряється (англ. verifiable) — будь-хто може перевірити, що випадкове число, згенероване VRF, є дійсним. Все, що їм потрібно зробити, це перевірити доказ і перевірити правильність виведення гешу. Хоча лише власник секретного ключа VRF може обчислити геш, будь-хто, хто має відкритий ключ, може перевірити правильність гешу.

• Випадковий (англ. random) — результат VRF абсолютно непередбачуваний (рівномірно розподілений) для будь-кого, хто не знає початкового чи закритого ключа та не слідує шаблону. У VRF кожен можливий результат є однаково ймовірним. Випадковість генерується унікальним поєднанням початкового та закритого ключів.

• Функція (англ. function) — VRF покладаються на математичний алгоритм для створення як випадкового числа, так і доказу, який підтверджує його автентичність. Для того, щоб функція вважалася VRF, RNG має тримати початкове число прихованим (неявним), щоб зберегти його непередбачуваність, тоді як доказ має бути явним і обчислюваним усіма (явним), щоб забезпечити його перевіреність.

Власник приватного ключа може згенерувати випадкове значення та відповідний доказ, який будь-хто з публічним ключем може перевірити. Ця властивість VRF забезпечує прозорість і захист від підробок.

Розрізняють кілька конструкцій VRF, які є безпечними в криптографічній моделі випадкового оракула. Одна з них базується на RSA, а інша — на еліптичних кривих (EC) [35].

Варто зазначити, що VRF на основі RSA, хоч і простіший в реалізації, проте не забезпечує достатньої ефективності для сучасних

блокчейн-систем. Крім цього, він поступається у швидкості та гнучкості VRF, які ґрунтуються на криптографії еліптичних кривих, зокрема на схемах спарювання (pairings). Очевидно, що доцільніше розглядати далі саме VRF на основі EC-Pairings.

Спочатку введемо деякі позначення:

- sk — приватний ключ учасника, $sk \in \mathbb{Z}_q$;
- pk — публічний ключ учасника, $pk \in \mathbb{G}_2$;
- α — точка на кривій, $\alpha \in \mathbb{G}_1$;
- H — деяка геш-функція, $H : \mathbb{G}_1 \to \mathbb{Z}_q$;
- e — pairing-функція, $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$;
- π — доведення того, що саме власник sk обчислив VRF;
- β — результат обчислення VRF.

Тоді згідно з [35]:

Алгоритм 3.1. Обчислення VRF на основі EC-Pairing.

Вхід: α.

Вихід: π, β.

1) Нехай $\mathbb{G}_1, \mathbb{G}_2$ — підгрупи еліптичної кривої E порядку q з базовими точками $P_1 \in \mathbb{G}_1, P_2 \in \mathbb{G}_2$, та pairing-функцією e.

2) Обираємо секретний ключ $sk = x \in \mathbb{Z}_q$ та обчислюємо публічний ключ:

$$pk = Q = x \cdot P_2;$$

3) Обчислюємо доведення:

$$\pi = x \cdot \alpha;$$

4) Обчислюємо результат VRF:

$$\beta = H(\pi).$$

Алгоритм 3.2. Верифікація VRF на основі EC-Pairing.

Вхід: α, Q, π, P_2, β.

Вихід: `true` або `false`.

1) Перевіряємо коректність доведення:

$$e(\alpha, Q) \stackrel{?}{=} e(\pi, P_2).$$

2) Перевіряємо коректність обчислення VRF:

$$\beta \stackrel{?}{=} H(\pi).$$

3) Якщо обидві умови істинні, повернути `true`; інакше — `false`.

У контексті тендерних закупівель VRF дозволить справедливо й прозоро обирати переможців на певних етапах процедури, при цьому зберігаючи довіру з боку учасників.

3.3.2 Distributed Key Generation

Означення 3.3. Розподілене генерування ключів (англ. Distributed Key Generation, DKG) [36] — це криптографічний протокол, який дозволяє групі з n учасників спільно створити пару відкритого та приватного ключів без залучення довіреної третьої сторони. У цьому процесі приватний ключ ніколи не формується повністю або централізовано; натомість кожен учасник отримує свою частку секрету, що забезпечує високий рівень безпеки та стійкість до компрометації окремих учасників.

Основні властивості DKG включають:

• *Децентралізація:* відсутність єдиного центру, що зменшує ризик компрометації системи;

• *Секретність:* жоден учасник не має повного доступу до приватного ключа, що унеможливлює його самостійне використання;

• *Стійкість до атак:* система здатна витримати компрометацію до

t учасників ($t < \frac{n}{2}$), зберігаючи безпеку;

• *Верифікованість:* використання схем верифікованого розподілу секрету (VSS) дозволяє перевіряти коректність часток.

У типовій схемі DKG можна виділити наступні етапи:

1) *Ініціалізація:* кожен учасник створює власну частку секрету;

2) *Розповсюдження:* всі частки передаються іншим учасникам разом із криптографічними доказами коректності;

3) *Агрегація часток:* на основі зібраних часток формується єдиний спільний публічний ключ, а кожен учасник зберігає свою приватну частку.

У 2006 році Rosario Gennaro та інші у своїй статті [36] показали, що перший протокол DKG (JF-DKG), який запропонував Pedersen у 1991 році, має обмеження у масштабованості та безпеці. Водночас, вони запропонували новий покращений протокол New-DKG, який покриває вищезазначені обмеження, покращує стійкість до атак та зменшує ризики розкриття секретів. Тому далі розглянемо схему удосконаленого протоколу New-DKG.

Нехай:

• n — кількість учасників;

• t — поріг (де $0 < t < n$);

• p, q — великі прості числа, де $q \mid p - 1$;

• $g, h \in \mathbb{G}_q \subset \mathbb{Z}_p^*$ — незалежні генератори підгрупи порядку q;

• y — спільний публічний ключ;

• x_j — приватна частка і-того учасника;

• x'_j — додаткова частка і-того учасника;

• x — спільне секретне значення.

Тоді:

Алгоритм 3.3. Протокол New-DKG.

Вхід: n, t, p, q, g, h.

Вихід: y, x_j, x'_j.

1) Генерація секрету z_i за допомогою протоколу Pedersen-VSS:

• Кожен учасник P_i в ролі дилера спочатку обирає два поліноми

ступеня t над $\mathbb{Z}_q$:

$$f_i(z) = a_{i0} + a_{i1}z + ... + a_{it}z^t,$$

$$f'_i(z) = b_{i0} + b_{i1}z + ... + b_{it}z^t.$$

Нехай секрет: $z_i = f_i(0)$. P_i обчислює значення C_{ik} (де $k = 0,...,t$) та значення частки s_{ij} і s'_{ij} (де $j = 1,...,n.$):

$$C_{ik} = g^{a_{ik}} h^{b_{ik}} \bmod p,$$

$$s_{ij} = f_i(j) \bmod q, s'_{ij} = f'_i(j) \bmod q.$$

Після чого надсилає (s_{ij}, s'_{ij}) до P_j.

• Кожен учасник P_j перевіряє для $i = 1,...,n$, що:

$$g^{s_{ij}} h^{s'_{ij}} = \prod_{k=0}^{t} C_{ik}^{j^k} \bmod p. \tag{3.1}$$

Якщо перевірка не проходить — учасник P_j відправляє скаргу на учасника P_i.

• Кожен дилер P_i відповідає на отриману скаргу, розкриваючи (s_{ij}, s'_{ij}) публічно, при чому частки задовільняють (3.1).

• Дискваліфікація: будь-хто з учасників може позначити будь-кого дискваліфікованим, якщо було отримано більше, ніж t скарг або відповіли хоча б на одну скаргу з фальсифікованими даними (3.1).

2) Формування QUAL: кожен учасник створює QUAL (Qualified set) — список недискваліфікованих учасників.

3) Спільне секретне значення дорівнює:

$$x = \sum_{i \in QUAL} z_i \bmod q.$$

Проте жодна сторона явно його не обраховує. Також кожен P_i обчислює

свою частку секрету:

$$x_i = \sum_{j \in QUAL} s_{ji} \bmod q, x'_i = \sum_{j \in QUAL} s'_{ji} \bmod q.$$

4) Витяг публічного ключа: кожен $i \in$ QUAL надає $y_i = g^{z_i} \bmod p$ через протокол Feldman-VSS:

• Кожен учасник P_i, де $i \in QUAL$, публікує для $k =$ 0,...,t:

$$A_{ik} = g^{a_{ik}} \bmod p.$$

• Кожен учасник P_j для кожного $i \in$ QUAL, що передані іншими, перевіряє:

$$g^{s_{ij}} = \prod_{k=0}^{t} A_{ik}^{j^k} \bmod p. \tag{3.2}$$

Якщо не виконується — учасник P_j відправляє скаргу на учасника P_i, а також публікує значення (s_{ij}, s'_{ij}), які задовільняють (3.1), але не задовільняють (3.2).

• Для всіх P_i, що отримали хоч одну таку дійсну скаргу, інші сторони запускають фазу реконструкції Pedersen-VSS для публічного обчислення z_i, $f_i(z)$, A_{ik}, де $k =$ 0,...,t. Для всіх $i \in QUAL$ фіксується $y_i = A_{i0} = g^{z_i} \bmod p$. Публічний ключ отримується наступним чином:

$$y = \prod_{i \in QUAL} y_i \bmod p.$$

У подальшому під DKG розуміється удосконалений протокол New-DKG, якщо не зазначено інше.

У контексті тендерів використання DKG може забезпечити спільне управління ключами, що підвищує довіру до процесу та зменшує ризик змови.

3.4 Запропоновані методи проведення тендерних закупівель на блокчейні

Розглянемо два нових методи проведення публічних закупівель на блокчейні: спрощений — з використанням VRF, та ускладнений — із використанням VRF та DKG. В обох методах фігуруватимуть наступні ролі: *замовник, тендерний комітет, учасники.*

3.4.1 Метод з використанням VRF

Особливістю цього методу є використання VRF для обчислення геш-значення заявки, що одночасно підтверджує, що пропозицію було подано до дедлайну, та незмінність вмісту після дедлайну. Завдяки цьому гарантується прозорість процедури (відсутність сторонніх втручань і маніпуляцій, таких як корупція) та цілісність поданих даних (учасники не можуть змінити свої заявки після дедлайну або отримати доступ до чужих пропозицій). Цей метод рекомендований для публічних закупівель, де важлива відкритість, незмінність і дозволена публічність змісту заявок.

Спрощена процедура проведення тендеру:

1) *Оголошення тендеру:* замовник публікує умови закупівлі у блокчейні, включаючи дедлайни та критерії оцінки.

2) *Створення заявки:* учасники формують заявки відповідно до вимог.

3) *Обчислення гешу заявки за допомогою алгоритму обчислення VRF:* кожен учасник використовує свій приватний ключ для обчислення значення VRF від заявки. Це гарантує автентичність заявки та її незмінність без можливості маніпуляцій.

4) *Публікація гешу заявки у блокчейні:* учасники записують у

блокчейн геш-значення своїх заявок разом із доказом коректності обчислення VRF.

5) *Подача заявки:* після дедлайну кожен учасник розкриває зміст заявки, додаючи її до блокчейну або передаючи її згідно з механізмом подання.

6) *Верифікація заявки:* використовуючи VRF-доказ, тендерний комітет або смарт-контракт перевіряє, що заявка відповідає раніше опублікованому гешу.

7) *Розгляд та оцінка заявок:* всі перевірені заявки аналізуються згідно з критеріями тендеру.

8) *Вибір переможця:* визначається найкраща пропозиція відповідно до встановлених правил тендера.

9) *Підписання контракту:* укладається договір між переможцем та замовником у блокчейні.

10) *Контроль виконання договору:* прогрес виконання контракту відстежується через блокчейн або сторонні джерела.

3.4.2 Метод з використанням VRF та DKG

Метод базується на тому, що заявка учасника шифрується за допомогою публічного ключа, який сформований спільно учасниками тендерного комітету з використанням протоколу DKG. Це гарантує конфіденційність — навіть замовник не має доступу до змісту заявки до завершення етапу подання заявок. Як і в попередньому методі, в даному підході використовується VRF для обчислення геш-значення, що підтверджує своєчасність та незмінність заявки. Завдяки цьому забезпечується прозорість і довіра до тендерної процедури. Метод доцільно використовувати для закритих закупівель, зокрема у військовій або урядовій сферах, де критично важлива конфіденційність змісту заявки.

Ускладнена процедура проведення тендеру:

1) *Оголошення тендеру:* замовник публікує умови тендеру, а тендерний комітет ініціює процедуру генерації розподіленого ключа за допомогою протоколу DKG.

2) *Генерація публічного ключа (DKG):* учасники тендерного комітету спільно генерують публічний ключ для шифрування заявок. Приватний ключ розподілений між членами комітету.

3) *Створення заявки:* кожен учасник формує свою заявку відповідно до вимог.

4) *Обчислення гешу заявки за допомогою алгоритму обчислення VRF:* кожен учасник обчислює значення VRF від своєї заявки за допомогою приватного ключа для підтвердження чесності та незмінності.

5) *Шифрування заявки:* зміст заявки шифрується на спільному публічному ключі, створеному через протокол DKG, що забезпечує конфіденційність до моменту розшифрування.

6) *Публікація гешу заявки у блокчейні:* учасники записують у блокчейн геш-значення заявки та доказ коректності обчислення VRF.

7) *Подача зашифрованої заявки:* кожен учасник додає свою зашифровану заявку до блокчейну або передає її згідно з механізмом подання.

8) *Розшифрування заявок:* після завершення прийому заявок тендерний комітет спільно розшифровує заявки, використовуючи свої частини ключа з DKG.

9) *Верифікація заявки:* використовуючи VRF-доказ, тендерний комітет або смарт-контракт перевіряє, що розшифрована заявка відповідає раніше опублікованому гешу.

10) *Розгляд та оцінка заявок:* всі розшифровані та перевірені заявки аналізуються згідно з критеріями тендеру.

11) *Вибір переможця:* визначається найкраща пропозиція відповідно до встановлених правил тендера.

12) *Підписання контракту:* укладається договір між переможцем та

замовником у блокчейні.

13) *Контроль виконання договору:* прогрес виконання контракту відстежується через блокчейн або сторонні джерела.

Запропоновані методи поєднують переваги блокчейн технологій із сучасними криптографічними механізмами, вирішуючи ключові проблеми прозорості, конфіденційності та довіри у публічних закупівлях. Метод з VRF забезпечує відкриту та чесну процедуру відбору, тоді як варіант з DKG гарантує захист від публічного доступу до змісту заявок.

Наведені методи також було опубліковано автором у [37].

3.5 Формалізація моделі та криптографічні гарантії методів

У розроблених методах розглядається модель відкритого блокчейну, де всі транзакції є публічними, незмінними та доступними для перевірки будь-яким учасником. Передбачається наявність n учасників, серед яких щонайбільше $t < \frac{n}{2}$ можуть бути зловмисними. Вважається, що мережа функціонує коректно, а механізми консенсусу забезпечують цілісність блокчейну.

3.5.1 Припущення моделі

У моделі передбачається виконання таких криптографічних та системних припущень:

- VRF (Verifiable Random Function) забезпечує:

  – *псевдовипадковість:* результат неможливо передбачити без знання секретного ключа;

  – *неспотворюваність:* неможливо створити інший коректний результат чи підробити доведення;

  – *відкриту верифікацію:* будь-хто з публічним ключем може перевірити коректність результату.

- DKG (Distributed Key Generation) гарантує:
  - спільну генерацію відкритого ключа без довіреної сторони;
  - стійкість до саботажу через перевірку часткових ключів;
  - можливість порогового розшифрування лише за умови наявності $t + 1$ чесних учасників.
- Криптографічна стійкість усіх застосованих примітивів:
  - складність задачі дискретного логарифмування;
  - неможливість підробки доведення у VRF;
  - стійкість застосованої схеми шифрування.
- Системні припущення:
  - більшість учасників (щонайменше $\frac{n}{2} + 1$) є чесними;
  - блокчейн є стійким до атак подвійної витрати (double-spending) та атак розгалуження (forking).

3.5.2 Очікувані властивості запропонованих методів

Зазначимо властивості, які є бажаними для запропонованих методів, та пояснимо якими механізмами та за яких припущень вони гарантуються:

- *незмінність та достовірність заявки*: забезпечується гешуванням заявки за допомогою VRF та її закріпленням у блокчейні;
- *конфіденційність заявки до моменту розкриття*: забезпечується у другому методі шляхом використання шифрування з пороговим розшифруванням на основі DKG;
- *стійкість до маніпуляцій при розшифруванні*: досягається перевіркою коректності часткових розшифрувань у пороговому протоколі;
- *публічна верифікація етапів*: як VRF, так і DKG передбачають відкриту перевірку коректності результатів;
- *прозорість процесу*: всі дії зберігаються у блокчейні, і можуть бути перевірені будь-якою третьою стороною.

3.5.3 Обґрунтування виконання властивостей при виконанні припущень

Виконання вищезазначених властивостей забезпечується за таких умов:

- *Незмінність та достовірність заявки* гарантується завдяки:
  - псевдовипадковості та неспотворюваності VRF;
  - незмінності записів у блокчейні;
  - неможливості створення альтернативної довшої гілки (fork), яка б містила підроблену заявку.
- *Конфіденційність заявки до моменту розкриття* досягається завдяки:
  - використанню схеми шифрування, стійкої до розкриття без відповідного ключа;
  - пороговості DKG (без $t + 1$ учасників розшифрування неможливе);
  - децентралізованому управлінню ключами, що унеможливлює зловживання одним учасником.
- *Стійкість до маніпуляцій при розшифруванні* досягається:
  - можливістю виявлення некоректних часткових розшифрувань (завдяки властивостям DKG);
  - вимогою наявності більшості чесних учасників.
- *Публічна верифікація* гарантується через:
  - можливість незалежної перевірки доведень VRF;
  - відкриту валідацію часткових результатів у DKG, зокрема при генерації ключів та розшифруванні;
  - збереження усіх ключових даних і доведень у блокчейні.
- *Прозорість процесу* забезпечується:
  - децентралізованою природою блокчейну;
  - доступністю всіх необхідних даних для незалежного аудиту;

– незмінністю записів, що унеможливлює фальсифікацію історії.

Таким чином, запропоновані методи базуються на формально доведених властивостях криптографічних примітивів та припущеннях щодо моделі учасників і мережі, що дає змогу досягти високого рівня прозорості, довіри та захищеності процесу тендерних закупівель.

3.6 Аналіз запропонованих методів

Критерій	**Метод з VRF**	**Метод з VRF та DKG**
Прозорість	Висока	Висока
Конфіденційність	Низька	Висока
Перевірюваність критеріїв	Публічна, криптографічна	Після розшифрування
Маніпуляції даними	Виключені після подачі	Унеможливлені
Гарантія незмінності даних	Після публікації геш-значення	Забезпечена
Витрати ресурсів	Низькі	Помірні
Складність реалізації	Низька	Висока
Атаки на оцінювання	Існує ризик упередженості	Мінімізовані
Атаки з боку організатора	Можливі до подачі	Блокуються
Рекомендації застосування	Відкриті тендери	Закриті тендери

Таблиця 3.1 – Порівняння запропонованих методів

Детальний аналіз критеріїв:

1) *Прозорість:* обидва методи забезпечують високий рівень прозорості. У методі з VRF всі події фіксуються у блокчейні, а коректність геш-значень підтверджується доведеннями. У методі з DKG прозорість додатково посилена спільною генерацією ключів без єдиного

центру.

2) *Конфіденційність:* метод з VRF не передбачає конфіденційності без додаткових засобів шифрування — вся інформація публічна. Натомість метод з DKG використовує порогове шифрування, що дозволяє зберігати таємницю до моменту розкриття.

3) *Перевірюваність критеріїв:* у спрощеному методі перевірка можлива безпосередньо після подачі заявки. У випадку з DKG — лише після розшифрування, що гарантує чесність та захист від підробок.

4) *Маніпуляції даними:* у методі з VRF є теоретична можливість змін до моменту подачі, після чого дані стають незмінними. У випадку ускладненого методу — інформація одразу зашифрована, що виключає несанкціоновані втручання.

5) *Гарантія незмінності даних:* у спрощеному методі дані залишаються незмінними після моменту публікації геш-значення заявки, однак до цього можливі маніпуляції на стороні учасника або організатора. У методі з DKG дані одразу фіксуються у зашифрованому вигляді, а доступ до розшифрування контролюється спільно всіма учасниками, що гарантує незмінність протягом усього процесу.

6) *Витрати ресурсів:* метод з VRF вимагає мінімальних ресурсів і простий у реалізації. В свою чергу, метод з DKG потребує більше обчислень та координації учасників, однак залишається практичним для реалізації.

7) *Складність реалізації:* реалізація VRF може бути інтегрована у смарт-контракт з мінімальними зусиллями. Натомість метод з DKG потребує розробки протоколів VSS, обміну частками та верифікації комітментів.

8) *Атаки на оцінювання:* відкритість критеріїв у методі з VRF може викликати упередженість. Метод з DKG, завдяки шифруванню, приховує дані до завершення тендера, мінімізуючи таким чином ризики.

9) *Атаки з боку організатора:* у методі з VRF організатор може впливати на дані до подачі. DKG унеможливлює це завдяки розподіленому управлінню ключами, що таким чином блокуючи

централізоване втручання.

10) *Рекомендації застосування:* метод з VRF доцільно використовувати у відкритих процедурах, де важлива відкритість і дозволена публічність. Метод з DKG більше підходить для конфіденційних закупівель, де критично важлива приватність і стійкість до атак.

Висновки до розділу 3

У цьому розділі було запропоновано два методи проведення тендерних закупівель з використанням блокчейн технологій, кожен з яких орієнтований на підвищення довіри, безпеки та стійкості до маніпуляцій у процесі закупівель. Перший метод, заснований на використанні верифікованих випадкових функцій (VRF), забезпечує прозорість та незмінність процесу подачі заявок, дозволяючи всім учасникам перевірити коректність виконання протоколу. Другий метод поєднує VRF з розподіленою генерацією ключів (DKG), що дозволяє зберігати конфіденційність вмісту заявок — критично важливий аспект для закритих тендерів.

Також у межах дослідження було описано формальну модель, яка передбачається у розроблених методах, та проведено детальний аналіз обох підходів з технічної та процедурної точок зору, включаючи оцінку їхньої стійкості до атак, конфіденційності та складності реалізації.

Результати дослідження демонструють перспективність використання блокчейн технологій у поєднанні з сучасними криптографічними механізмами для підвищення прозорості, безпеки та довіри до систем публічних закупівель.

ВИСНОВКИ

У результаті виконання дипломної роботи було розглянуто теоретичні основи та ключові особливості проведення тендерних закупівель, зокрема в контексті відкритості, чесної конкуренції та ефективного використання ресурсів. Проаналізовано сучасні підходи до організації тендерних процедур, а також виявлено їхні основні переваги й недоліки. Порівняння паперових і електронних систем дозволило зробити висновок про доцільність подальшого розвитку саме електронних платформ із підвищеним рівнем автоматизації та безпеки.

На основі аналізу типових загроз та шахрайських схем, пов'язаних із тендерами, було встановлено, що навіть сучасні електронні системи залишаються вразливими до атак і маніпуляцій. У цьому контексті було обґрунтовано доцільність використання блокчейн технологій, які завдяки децентралізації, незмінності даних і автоматизованим механізмам можуть суттєво знизити рівень ризиків. Водночас визначено потенційні загрози, властиві самим блокчейн-системам, та запропоновано підходи до їх нейтралізації.

У рамках дослідження було розроблено два методи проведення тендерних закупівель із використанням блокчейну. Перший метод ґрунтується на використанні верифікованих випадкових функцій (VRF) і забезпечує прозору та незмінну фіксацію подачі заявок. Другий метод доповнює перший протоколом розподіленої генерації ключів (DKG), що дозволяє приховати вміст заявок до моменту їх розкриття, зберігаючи тим самим конфіденційність. Обидва підходи були детально проаналізовані за критеріями прозорості, стійкості до атак і складності реалізації, що дало змогу оцінити їхню придатність для використання в реальних умовах.

Запропоновані рішення демонструють перспективність інтеграції блокчейну та криптографічних протоколів у сферу публічних закупівель.

Вони можуть суттєво підвищити довіру до процесу, знизити ризики маніпуляцій та покращити захист даних. У подальшій роботі варто зосередитися на практичній реалізації та тестуванні запропонованих методів, а також на розробці інтерфейсів і компонентів, що забезпечуватимуть зручну інтеграцію з існуючими тендерними платформами.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Верховна Рада України. *Закон України "Про публічні закупівлі"*. Офіційний сайт Верховної Ради України, останнє оновлення: [15-03-2025]. URL: https://zakon.rada.gov.ua/laws/show/922-19#Text.

[2] *Державний тендер — це що таке, визначення, суть, принцип роботи*. URL: https://termin.in.ua/derzhavnyy-tender/.

[3] *Принципи здійснення публічних закупівель*. URL: https://tndr.com.ua/article/princzipi-zdijsnennya-publichnih-zakupivel/.

[4] Marijn Overvest. *Open and Closed Tendering — Explanation*. URL: https://procurementtactics.com/open-and-closed-tendering/.

[5] Adam Hoyle. *6 Types of Tender Used in Public Procurement*. URL: https://tendereyessoftware.com/blog/6-types-of-tender-used-in-public-procurement/.

[6] Neha Motaiah. *E-Tendering vs. Traditional Tendering: A Comparative Analysis for Construction Firms*. URL: https://proqsmart.com/blog/e-tendering-vs-traditional-tendering-a-comparative-analysis-for-construction-firms/.

[7] *Головна | Prozorro*. URL: https://prozorro.gov.ua/uk.

[8] *TED —- EU Tenders, the Supplement to the Official Journal*. URL: https://ted.europa.eu/en/.

[9] *Government e Marketplace (GeM) | National Public Procurement Portal, Government of India*. URL: https://gem.gov.in/.

[10] *Contracts Finder*. URL: https://www.gov.uk/contracts-finder.

[11] Product Evangelist Paul Stone. *Automation in Procurement: Top Processes You Can Automate in 2025*. URL: https://www.flowforma.com/blog/procurement-automation.

[12] *Blockchain and Smart Contracts in Procurement: A Strategic Guide.* URL: https://tokenminds.co/blog/blockchain-projects/blockchain-in-procurement.

[13] *A Complete Guide to the Public Procurement Tender Process.* URL: https://tendium.ai/en/learn/guide-to-the-public-procurement-tender-process/.

[14] *Нормативно-правові акти у сфері публічних закупівель.* URL: https://www.treasury.gov.ua/diyalnist/publichni-zakupivli/normativno-pravovi-akti-u-sferi-derzhavnih-zakupivel.

[15] Кабінет Міністрів України. *Постанова "Про затвердження особливостей здійснення публічних закупівель .."* URL: https://zakon.rada.gov.ua/laws/show/1178-2022-%D0%BF#Text.

[16] Міністерство економіки України. *Наказ Мінекономіки "Про затвердження примірного положення про уповноважену особу".* URL: https://me.gov.ua/view/ddf62e32-7955-43d4-aea5-691db8817f64.

[17] *WTO/Government procurement-The plurilateral Agreement on Government Procurement (GPA).* URL: https://www.wto.org/english/tratop_e/gproc_e/gp_gpa_e.htm.

[18] *Директива 2014/24/ЄС про публічні закупівлі.* URL: https://zakon.rada.gov.ua/laws/show/984_052-14\#Text.

[19] *Директива 2014/25/ЄС про про здійснення суб'єктами закупівель у водній, енергетичній ..* URL: https://zakon.rada.gov.ua/laws/show/984_053-14\#Text.

[20] *Як Тендерні Процедури Сприяють Ефективнішим Закупівлям?* URL: https://vynnyky-visnyk.com.ua/2024/06/07/iak-tenderni-protsedury-spryiaiut-efektyvnishym-zakupivliam.

[21] *Підвищення ефективності закупівель - Держзовнішінформ ДП.* URL: https://dzi.gov.ua/services/pidvyshhennya-efektyvnosti-zakupivel.

[22] *Викрито масштабну схему підтасовки медичних тендерів – ГПУ.* 2019. URL: https://www.pravda.com.ua/news/2019/02/21/7207301/.

[23] The Guide. *Case Examples of Collusive Bidding by Contractors | Guide to Combating Corruption.* URL: https://guide.iacrc.org/proof/case-examples/case-example-of-collusive-bidding-by-contractors/.

[24] Sirko V.S. «Corruption risks in public procurement: Analysis of corruption risks and methods of their minimization, including legislative and organizational measures». В: *Juridical scientific and electronic journal* 9 (2024), с. 260—262.

[25] Dominik Muhs. *Reentrancy - Smart Contract Security Field Guide.* URL: https://scsfg.io/hackers/reentrancy/.

[26] *Integer Overflow | Conflux Documentation.* URL: https://doc.confluxnetwork.org/es/docs/general/build/smart-contracts/contract-security/overflow.

[27] *Flash Loan Attacks: A Case Study.* URL: https://www.aon.com/en/insights/cyber-labs/flash-loan-attacks-a-case-study.

[28] Daniejjimenez. *Ethereum Censorship and SafeStake: MEV, OFAC and Flashbots (Part I).* URL: https://medium.com/ethereum-on-steroids/ethereum-censorship-and-safestake-mev-ofac-and-flashbots-part-i-2efba4b3d3c.

[29] *PARITY Wallet Hack Demystified: All You Need to Know!* URL: https://medium.com/@web3author/parity-wallet-hack-demystified-all-you-need-to-know-91b8dcb5b81.

[30] *51% Attack: The Concept, Risks & Prevention.* URL: https://hacken.io/discover/51-percent-attack/.

[31] *Sybil Attack in Blockchain: Examples & Prevention.* URL: https://hacken.io/insights/sybil-attacks/.

[32] Ethan Heilman та ін. *Eclipse Attacks on Bitcoin's Peer-to-Peer Network*. 2015. URL: https://eprint.iacr.org/2015/263.pdf.

[33] Adam Hayes. *Blockchain Facts: What Is It, How It Works, and How It Can Be Used*. Англ. 24 бер. 2025. URL: https://www.investopedia.com/terms/b/blockchain.asp.

[34] Alfredo Collosa. *Blockchain en el sector público*. Ісп. 23 груд. 2021. URL: https://www.ciat.org/ciatblog-blockchain-en-el-sector-publico/.

[35] S Goldberg та ін. *RFC 9381: Verifiable Random Functions (VRFs)*. Англ. Серп. 2023. URL: https://datatracker.ietf.org/doc/html/rfc9381.

[36] Rosario Gennaro та ін. «Secure Distributed Key Generation for Discrete-Log Based Cryptosystems». В: *J. Cryptology* 20 (2007), с. 51—83. DOI: 10.1007/s00145-006-0347-3.

[37] Баєвський К. О. та Ковальчук Л. В. *Розробка методів проведення тендерних закупівель з використанням блокчейн технологій.* Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XXIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (14 – 17 травня 2025 р., м. Київ, Україна). Київ : КПІ ім. Ігоря Сікорського: Видавництво «Політехніка», 2025. URL: https://drive.google.com/file/d/1iT4SajI_-KPcoVur55G3TIlGFROWAnyz/view.