МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ATICE'2025)

ОДЕСА, УКРАЇНА, 18 ЛИПНЯ 2025 Р.

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

ОДЕСА

2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

INTERNATIONAL HUMANITARIAN UNIVERSITY

INTERNATIONAL CONFERENCE

ADVANCED TECHNOLOGY IN INFORMATION AND COMMUNICATION ENGINEERING

(ATICE'2025)

ODESA, UKRAINE, JULY 18, 2025

CONFERENCE PROCEEDINGS

ODESA

2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

Одеса, Україна, 18 липня 2025 р.

Видавничий дім
«Гельветика»
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL HUMANITARIAN UNIVERSITY

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2025)

Odesa, Ukraine, July 18, 2025

Conference Proceedings

Видавничий дім
«Гельветика»
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025)

Одеса, Україна, 18 липня 2025 р.

Матеріали конференції

Видавничий дім
«Гельветика»
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings. Odesa : International humanitarian university, 2025, 123 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції. Міжнародний гуманітарний університет, 2025. – Одеса: Видавничий дім «Гельветика», 2025. – 123 с.

ISBN 978-617-554-582-9

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГЛОБА Л. С . – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

РУСУ О.П. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.

ЙОНА Л.Г. – к.т.н., доц., Міжнародний гуманітарний університет, Одеса, Україна.

МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.

ПЕДЯШ В.В. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КУЧАЙ О.В. - д.п.н., проф., Національний університет біоресурсів і природокористування України.

ЖИГУЛІН О.А. – д.е.н., проф., Міжнародний гуманітарний університет, Одеса, Україна

ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Ковальчук Д. А.
здобувач вищої освіти третього (освітньо-наукового рівня)
спеціальності 125 Кібербезпека
Науковий керівник: Йона Л. Г.
Міжнародний гуманітарний університет м. Одеса, Україна

БЛОКЧЕЙН-ТЕХНОЛОГІЇ ТА ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА НЕЗМІННОСТІ ДАНИХ

У сучасних умовах стрімкого розвитку цифрових технологій та зростання обсягів даних забезпечення їхньої цілісності та незмінності стає одним із ключових аспектів кібербезпеки. Традиційні централізовані моделі зберігання інформації дедалі частіше виявляються вразливими до несанкціонованих змін, втрат або підробок даних. Це особливо критично для сфер, де дані мають правову або фінансову значущість: державні реєстри, банківські транзакції, медичні записи, ланцюги постачання.

У цьому контексті блокчейн-технології привертають значну увагу як інноваційний інструмент, що дозволяє створювати розподілені, прозорі та стійкі до фальсифікації системи зберігання даних. Завдяки використанню криптографічних алгоритмів і механізмів консенсусу, блокчейн забезпечує незмінність даних та їх перевірюваність протягом усього життєвого циклу.

Разом із тим, попри високий потенціал, впровадження блокчейн-рішень супроводжується низкою технологічних, організаційних і нормативних викликів. Таким чином, аналіз блокчейн-технологій з позиції кібербезпеки та захисту інформації є важливим кроком для формування нових підходів до гарантування цілісності, автентичності та прозорості даних у цифрову епоху.

Мета дослідження

Метою даного дослідження є всебічний аналіз потенціалу використання блокчейн-технологій як інструменту підвищення рівня кібербезпеки шляхом забезпечення цілісності, незмінності та достовірності даних у різних сферах діяльності.

Дослідження передбачає:

- розкриття ключових механізмів, за допомогою яких блокчейн гарантує захист інформації від несанкціонованих змін;
- визначення практичних переваг і недоліків впровадження блокчейн-рішень у системи, що потребують високого рівня інформаційної безпеки;
- аналіз типових викликів і обмежень (масштабованість, конфіденційність, юридичні аспекти);
- окреслення перспектив розвитку блокчейн-технологій у контексті сучасних кіберзагроз.

Отримані результати мають сприяти пошуку ефективних підходів до інтеграції блокчейн-технологій у існуючі системи захисту інформації та формуванню рекомендацій для їх подальшого наукового та практичного використання.

Механізми забезпечення цілісності та незмінності даних

Ключовою особливістю блокчейн-технологій, що робить їх перспективними у сфері кібербезпеки, є принципова архітектура з використанням розподіленого реєстру та криптографічних механізмів. Ці механізми дозволяють гарантувати цілісність та незмінність інформації навіть у разі спроби несанкціонованого втручання.

Основні елементи забезпечення цілісності включають:

- **Розподілений реєстр (Distributed Ledger):** усі учасники мережі зберігають однакові копії реєстру, що унеможливлює централізовану модифікацію або підробку даних без згоди більшості.
- **Консенсус-алгоритми (Proof of Work, Proof of Stake тощо):** забезпечують погодження між усіма учасниками щодо легітимності записів у реєстрі. Відсутність єдиної точки відмови підвищує стійкість до атак.
- **Криптографічні хеш-функції:** кожен блок містить хеш попереднього, що забезпечує ланцюговий захист. Зміна навіть одного байта даних призведе до зміни всіх наступних хешів, що миттєво виявляється.
- **Цифрові підписи та шифрування:** автентифікація транзакцій і прав доступу здійснюється на основі криптографічних ключів, що мінімізує ризик підробки або підміни даних.
- **Smart Contracts:** забезпечують автоматизацію виконання умовних операцій і перевірок, що знижує людський фактор і ризик маніпуляцій.

Поєднання цих елементів дозволяє реалізувати концепцію «середовища недовіри» (trustless environment), де учасники можуть взаємодіяти без необхідності централізованого посередника, що особливо важливо для підвищення рівня захисту критично важливої інформації.

Приклади використання

Блокчейн-технології вже знаходять практичне застосування у різних галузях, де критично важливо гарантувати цілісність, незмінність та прозорість даних. Одним із ключових аспектів їхнього використання є мінімізація ризиків шахрайства та корупційних схем шляхом створення середовища, де кожен запис є публічним, перевірюваним і незмінним.

Серед найпоширеніших прикладів можна виділити:

- **Державні реєстри та електронне урядування:** блокчейн може забезпечити прозорість ведення земельних кадастрів, реєстрів власності чи реєстрації бізнесу. Незмінність записів унеможливлює несанкціоновані виправлення чи фальсифікацію документів, що є важливим для протидії корупції у державному секторі.
- **Електронне голосування:** використання блокчейну для фіксації голосів виборців гарантує їх достовірність, унеможливлює подвійне голосування та фальсифікацію результатів.
- **Ланцюги постачання (supply chain):** завдяки блокчейну можна відстежувати походження товарів на кожному етапі логістики. Це мінімізує ризики підміни товарів, контрабанди або шахрайських схем.

- **Медична сфера:** забезпечення цілісності медичних записів пацієнтів і контроль доступу до них сприяє захисту конфіденційних даних і запобігає їхньому несанкціонованому редагуванню.
- **Антикорупційні ініціативи:** децентралізоване зберігання контрактів, тендерних процедур чи бюджетних витрат дозволяє забезпечити громадський контроль і зменшує можливості для маніпуляцій.

Таким чином, блокчейн-технології розглядаються не лише як технічне рішення для захисту інформації, а й як важливий інструмент підвищення прозорості та довіри до даних у сферах, де проблема корупції є системною.

Сучасні виклики та обмеження

Незважаючи на високий потенціал блокчейн-технологій у підвищенні рівня кібербезпеки та протидії корупції, їхнє впровадження супроводжується низкою суттєвих викликів і обмежень.

По-перше, однією з ключових проблем залишається масштабованість і продуктивність. Поширені механізми консенсусу (зокрема Proof of Work) забезпечують високу стійкість до атак, але потребують значних обчислювальних ресурсів та енергії, що робить такі системи дорогими та малоефективними для великих обсягів транзакцій.

По-друге, блокчейн за своєю природою забезпечує прозорість і публічність записів, що створює конфлікт між незмінністю даних і конфіденційністю. Для сфери захисту інформації це виклик, адже необхідно балансувати між відкритістю транзакцій та дотриманням вимог законодавства щодо захисту персональних даних.

По-третє, впровадження блокчейн-рішень у реальні бізнес-процеси стикається з організаційними та нормативно-правовими бар'єрами. Багато країн досі не мають чіткої регуляторної бази щодо використання технології розподіленого реєстру, що ускладнює її інтеграцію у державні системи та процеси, зокрема антикорупційні інструменти.

По-четверте, існують ризики, пов'язані з людським фактором та якістю початкових даних. Навіть якщо блокчейн гарантує незмінність записів, він не може забезпечити достовірність інформації, якщо вона була введена неправильно або зловмисно (проблема «сміття на вході» — garbage in, garbage out).

Крім того, для підтримки дійсно високого рівня кібербезпеки необхідно враховувати питання управління приватними ключами та захисту кінцевих точок. Компрометація ключа користувача або адміністратора може звести нанівець всі переваги блокчейн-архітектури.

Таким чином, використання блокчейну у сфері захисту інформації потребує комплексного підходу, що поєднує технологічні, організаційні та правові заходи для мінімізації потенційних ризиків і повної реалізації переваг технології.

Висновок

Блокчейн-технології демонструють високий потенціал як інструмент забезпечення цілісності, незмінності та прозорості даних у різних сферах, де питання кібербезпеки та захисту інформації є критично важливими. Завдяки використанню механізмів розподіленого реєстру, криптографії та консенсусу блокчейн здатен істотно знизити ризики несанкціонованих змін і підробок даних, а також мінімізувати прояви корупційних схем у публічних і приватних процесах.

Разом із тим впровадження блокчейн-рішень не позбавлене викликів, зокрема проблем масштабованості, конфіденційності, регуляторних невизначеностей та людського фактора. Це підкреслює необхідність комплексного підходу, що має включати не лише технічні рішення, а й чітке правове регулювання, організаційні заходи та підвищення компетенцій користувачів.

Подальші дослідження у цьому напрямі мають бути зосереджені на поєднанні блокчейн-технологій з іншими інноваційними інструментами кіберзахисту — такими як штучний інтелект чи інтернет речей — для підвищення ефективності систем контролю даних і мінімізації ризиків. У довгостроковій перспективі це сприятиме зміцненню довіри до цифрових екосистем, зростанню прозорості процесів і посиленню кіберстійкості суспільства в цілому.

Література

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
2. Swan M. Blockchain: Blueprint for a New Economy. 2015.
3. Yli-Huumo J., Ko D., Choi S., Park S., Smolander K. Where Is Current Research on Blockchain Technology? A Systematic Review. 2016.

Головатюк К.В.
студент факультету Кібербезпека, спеціальність 125
Міжнародний гуманітарний університет
kostya93.06@gmail.com
Науковий керівник Йона Л.Г.

ФІШИНГ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ

Анотація. *Розглядається фішинг як одна з найпоширеніших і найнебезпечніших кіберзагроз сучасності, зокрема в контексті гібридної війни проти України. Аналізуються різновиди атак — spear-phishing, фармінг, вішинг — та їх цілі: викрадення даних, інфікування пристроїв, маніпуляція користувачем. Підкреслюється роль соціальних мереж у поширенні фішингових схем, а також економічна зацікавленість зловмисників. Окремо надано рекомендації для захисту користувачів і приклади дій українських кіберфахівців у виявленні та блокуванні фішингових ресурсів.*

У сучасному світі кіберзагроз фішинг вийшов на одне з перших місць за масштабами та наслідками. Це форма атаки соціальної інженерії, коли зловмисники вводять жертву в оману з метою викрадення даних або інфікування пристроїв шкідливим ПЗ. Зазвичай використовується електронна пошта, фальшиві сайти, повідомлення у месенджерах або навіть телефонні дзвінки.

Цей тип атаки побудований не лише на технічних уразливостях, а й на психологічному впливі. Атакуючі ретельно імітують комунікацію з надійним джерелом — банком, державною установою або знайомим контактом — аби викликати довіру та змусити користувача вчинити певну дію: перейти за посиланням, ввести паролі або завантажити заражений файл. Фішинг часто є першим етапом більш складної атаки, яка може завершитися повним контролем над пристроєм жертви або мережею організації.