

## РОЗРОБЛЕННЯ БЕЗПЕЧНОЇ СИСТЕМИ ЕЛЕКТРОННИХ ОСВІТНІХ ЗАПИСІВ (EER SYSTEM) НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА ХМАРНИХ ОБЧИСЛЕНЬ

Шматко О. В., Кириченко О. В.

У традиційних системах управління електронними освітніми записами (EER) кожен навчальний заклад зберігає власні студентські записи незалежно, що ускладнює обмін або перевірку академічних даних між різними освітніми платформами. Останнім часом технологія блокчейн стала перспективним рішенням, яке забезпечує безпечний та ефективний обмін EER-записами між установами, що працюють на різних системах. Проте зберігання повних освітніх записів безпосередньо у блокчейні є недоцільним через обмежену ємність сховища та високі операційні витрати. Для розв'язання цієї проблеми використовується хмарна інфраструктура як додаткове рішення, що надає переваги у вигляді масштабованого зберігання та високої доступності. Об'єктом проведеного дослідження є система управління електронними освітніми записами (Electronic Education Record, EER), що призначена для зберігання, обробки, обміну та автентифікації освітніх даних між різними навчальними закладами, роботодавцями та студентами.

Для вирішення зазначених проблем у роботі запропоновано інноваційний підхід до побудови EER-системи, який базується на поєднанні технології блокчейн та хмарних обчислень. Основна ідея полягає у розподілі функцій між двома компонентами: блокчейн-мережа забезпечує цілісність, незмінність та контроль доступу до освітніх записів шляхом збереження хеш-ідентифікаторів транзакцій, журналів подій та смарт-контрактів, що регламентують взаємодію між учасниками. Хмарна інфраструктура використовується для масштабованого зберігання зашифрованих EER-даних, що дозволяє зменшити навантаження на блокчейн і уникнути обмежень його пропускну здатності та вартості. Для забезпечення безпечного обміну даними між користувачами застосовано еліптичну криптографію (Elliptic Curve Cryptography, ECC), яка забезпечує високий рівень захисту при мінімальних обчислювальних витратах. Для оцінки стійкості системи проведено моделювання у середовищі AVISPA (Automated Validation of Internet Security Protocols and Applications), яке підтвердило відсутність вразливостей до основних типів атак, таких як повторна, підміна повідомлень або атака "люди на посередині". Додатково застосовано BAN-логічний аналіз, який засвідчив наявність взаємної автентифікації між суб'єктами системи.

Розроблена система EER забезпечує захист від основних типів атак (повторної, підміни, перехоплення даних), гарантує взаємну автентифікацію учасників обміну та зменшує обчислювальні витрати порівняно з існуючими схемами. За результатами моделювання підтверджено стійкість протоколу до загроз, а також ефективність механізмів контролю доступу. Досягнення підвищеної безпеки та продуктивності пояснюється поєднанням переваг блокчейн-технології та хмарної інфраструктури. Блокчейн забезпечує довіру та незмінність даних, тоді як хмарні сервіси дозволяють масштабне зберігання освітніх записів без надмірних витрат ресурсів. Використання ECC робить систему придатною для практичного впровадження у навчальних закладах різного рівня, зберігаючи баланс між безпекою та ефективністю.

**Ключові слова:** блокчейн, хмарні обчислення, еліптична криптографія, автентифікація, безпека даних, смарт-контракт, AVISPA, BAN-логіка.

**Шматко Олександр Віталійович**, кандидат технічних наук, доцент, кафедра цифрових технологій та проєктно-аналітичних рішень, Технічний Університет "Метінвест Політехніка", Південне шосе, 80, м. Запоріжжя, Україна, 69008  
ORCID: <https://orcid.org/0000-0002-2426-900X>

**Кириченко Олег Володимирович**, аспірант, кафедра програмної інженерії та інтелектуальних технологій управління, Національний технічний університет «Харківський політехнічний інститут», вул. Кирпичова, 2, м. Харків, Україна, 61002  
ORCID: <https://orcid.org/0009-0006-4445-4057>