Грушко С.С.
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних наук
Таврійський державний агротехнологічний університет
імені Дмитра Моторного,
доцент кафедри комп'ютерних систем та мереж
Національний університет «Запорізька політехніка»
Тіменко А.В.
старший викладач кафедри комп'ютерних наук
Таврійський державний агротехнологічний університет
імені Дмитра Моторного,
старший викладач кафедри комп'ютерних систем та мереж
Національний університет «Запорізька політехніка»

СУЧАСНІ ПІДХОДИ ДО ВЕРИФІКАЦІЇ ТА ЗАХИСТУ ОСВІТНІХ ДАНИХ У ЦИФРОВИХ СИСТЕМАХ

Анотація. *У статті досліджується проблема забезпечення довіри до освітніх даних в умовах тотальної цифровізації навчального процесу. Проаналізовано загрози для цілісності академічних записів, включаючи технічні збої, кібератаки та людський фактор. Здійснено систематичний огляд наявних методів зберігання та верифікації освітніх даних – від традиційних централізованих баз даних до сучасних розподілених систем. Виявлено недоліки кожного підходу та визначено вимоги до надійних систем верифікації. Представлено порівняльний аналіз програмних та апаратних реалізацій криптографічних методів захисту. Запропоновано перспективні напрями розвитку систем верифікації на основі блокчейн-технологій та апаратного прискорення на мікросхемах FPGA.*

Ключові слова: *освітні дані, верифікація, цілісність інформації, криптографія, системи управління навчанням.*

Hrushko S., Timenko A. Modern approaches to verification and protection of educational data in digital systems. *The article examines the problem of ensuring trust in educational data in the context of total digitalization of the learning process. Threats to the integrity of academic records are analyzed, including technical failures, cyberattacks and human*

factors. A systematic review of existing methods for storing and verifying educational data is conducted – from traditional centralized databases to modern distributed systems. Critical shortcomings of each approach are identified and requirements for reliable verification systems are determined. A comparative analysis of software and hardware implementations of cryptographic protection methods is presented. Promising directions for the development of verification systems based on blockchain technologies and hardware acceleration on FPGA are proposed.

Key words: *educational data, verification, information integrity, cryptography, learning management systems.*

Актуальність. Цифрова трансформація освіти, що відбувається в Україні та світі упродовж останнього десятиліття, радикально змінила підходи до управління навчальним процесом. Електронні журнали успішності, системи дистанційного навчання, цифрові бази даних студентів поступово витісняють традиційні паперові форми документообігу.

Разом із незаперечними перевагами цифровізації – автоматизацією рутинних процесів, підвищенням доступності даних, зручністю аналітики – виникають нові труднощі у сфері інформаційної безпеки. Цифрові академічні записи стають об'єктом різноманітних загроз: від випадкових технічних збоїв до цілеспрямованих кібератак та внутрішніх зловживань. Проблема набуває особливої гостроти в контексті боротьби з академічною недоброчесністю, коли фальсифікація оцінок може здійснюватися не лише студентами, а й зацікавленими особами з адміністративним доступом [5].

Міжнародна академічна мобільність та інтеграція України в європейський освітній простір актуалізують питання міжнародного визнання документів про освіту. Роботодавці та іноземні університети потребують надійних механізмів верифікації українських дипломів [6]. Випадки фальсифікації академічних документів, які періодично розголошуються у ЗМІ, підривають довіру до системи освіти та створюють репутаційні ризики для добросовісних випускників.

У зв’язку з цим актуальним завданням є системний аналіз наявних підходів до зберігання та верифікації освітніх даних, виявлення їх вразливостей та пошук перспективних технологічних рішень, здатних забезпечити надійний захист академічних записів від несанкціонованих модифікацій.

Мета дослідження. Метою дослідження є комплексний аналіз сучасних методів зберігання та верифікації освітніх даних, систематизація їх переваг та недоліків, а також визначення перспективних напрямів розвитку систем забезпечення довіри до цифрових академічних записів.

Виклад основного матеріалу. Цілісність даних означає збереження точності, повноти та незмінності інформації впродовж усього її життєвого циклу. У контексті освітніх систем це надзвичайно важлива властивість, оскільки оцінки, дипломи та академічні довідки є основою для прийняття важливих рішень щодо продовження навчання, працевлаштування, отримання стипендій.

Технічні збої становлять першу категорію загроз. Апаратні несправності серверів або систем зберігання даних можуть призвести до втрати або пошкодження інформації. Програмні помилки в системах управління базами даних або освітніх платформах здатні спричинити некоректну обробку даних. Нестабільність мережевої інфраструктури під час синхронізації розподілених систем може викликати неузгодженість реплік даних. Зловмисні дії представляють найбільш небезпечну категорію загроз. Хакерські атаки типу man-in-the-middle дозволяють перехоплювати та модифікувати дані під час їх передачі. Програми-вимагачі можуть шифрувати бази даних оцінок, вимагаючи викуп за їх розблокування. Фішингові атаки спрямовані на отримання облікових даних адміністраторів системи. Особливо небезпечними є інсайдерські загрози, коли співробітники з легітимним доступом зловживають своїми повноваженнями для модифікації оцінок за винагороду або через особисту зацікавленість. Людський фактор також є джерелом численних інцидентів [1; 5]. Помилки при введенні даних, випадкове видалення записів, неправильне налаштування систем резервного копіювання – все це може призвести до порушення цілісності даних навіть за відсутності злого умислу. Фізичні фактори також відіграють роль. Пожежі, повені, інші стихійні лиха можуть знищити дата-центри. Відключення електроенергії без належних систем резервування може спричинити втрату несинхронізованих даних.

Ефективна система верифікації має відповідати низці критичних вимог. Цілісність даних є фундаментальною властивістю – будь-які несанкціоновані зміни оцінок повинні бути технічно неможливими або щонайменше легко виявлятися. Система має зберігати повну історію змін з фіксацією часу та автора модифікації.

Конфіденційність передбачає розмежування доступу на основі ролей. Здобувач освіти може бачити лише власні оцінки, викладач – оцінки своїх груп, адміністратор має ширші повноваження. Персональні дані повинні захищатися шифруванням як при зберіганні, так і при передачі. Багатофакторна автентифікація додає додатковий рівень захисту для доступу до чутливої інформації. Доступність системи означає її безперервну роботу цілодобово, сім днів на тиждень. Резервне копіювання, географічно розподілені сервери, балансування навантаження забезпечують стійкість до збоїв. Масштабованість дозволяє системі справлятися зі зростаючою кількістю користувачів та даних без втрати продуктивності. Швидкодія системи безпосередньо впливає на зручність роботи викладачів при масовому виставленні оцінок та своєчасне інформування студентів про результати.

Відповідність нормативним вимогам включає дотримання законодавства про захист персональних даних, освітніх стандартів, вимог акредитаційних органів. Система має підтримувати аудит та формування звітності для регуляторів.

Централізовані реляційні бази даних залишаються найпоширенішим рішенням в освітніх закладах [2]. Системи на основі MySQL, PostgreSQL або Microsoft SQL Server зберігають оцінки у структурованих таблицях з визначеними зв’язками між сутностями. Такий підхід забезпечує ефективні запити, підтримку транзакцій, зручність розробки та адміністрування.

Однак централізована архітектура має принципові вразливості. Компрометація головного сервера або облікових записів адміністраторів відкриває доступ до всієї бази даних, а відсутність вбудованих механізмів виявлення несанкціонованих змін дозволяє особам з підвищеними привілеями модифікувати навіть журнали аудиту. Крім того, єдина точка відмови робить всі дані недоступними при виході сервера з ладу, а відсутність стандартизованих механізмів взаємної перевірки між закладами ускладнює міжінституційну верифікацію достовірності даних.

Хмарні платформи, такі як Google Workspace for Education, Microsoft 365 Education або спеціалізовані системи управління навчанням типу Moodle, Canvas, Blackboard, переносять дані на сервери постачальника послуг. Це забезпечує високу доступність завдяки географічно розподіленій інфраструктурі, автоматичне резервне копіювання, захист від DDoS-атак, економію на власному обслуговуванні IT-інфраструктури. Проте виникають нові ризики.

Залежність від постачальника означає втрату контролю над власними даними. При виході постачальника з бізнесу або зміні умов обслуговування міграція даних може бути ускладненою. Потенційні вразливості в багатобічній інфраструктурі, де дані різних організацій зберігаються на спільному обладнанні, викликають побоювання щодо витоків.

Гібридні рішення намагаються поєднати переваги обох підходів. Найважливіші дані зберігаються локально під повним контролем організації, менш чутливі дані розміщуються в хмарі для зручності доступу. Резервні копії дублюються як на власних серверах, так і в хмарі. Така архітектура забезпечує баланс між контролем та зручністю, однак вимагає складнішого адміністрування, синхронізації між компонентами, вищих витрат на підтримку двох систем одночасно.

Базовим інструментом виявлення модифікацій є контрольні суми та криптографічні хеш-функції. Для кожного запису обчислюється хеш-значення – унікальний цифровий відбиток фіксованої довжини. Навіть мінімальна зміна вхідних даних радикально змінює хеш. При верифікації хеш обчислюється повторно та порівнюється зі збереженим еталонним значенням.

Прості контрольні суми типу CRC32 придатні лише для виявлення випадкових помилок, а криптографічні хеш-функції MD5 та SHA-1 вже зламані через виявлені методи створення колізій. Хоча сучасні стандарти SHA-256 та SHA-3 забезпечують надійний захист при адекватній обчислювальній вартості, зберігання хешів у тій самій базі даних, що й дані, дозволяє зловмисникові з адміністративним доступом модифікувати обидва компоненти одночасно.

Цифрові підписи на основі асиметричної криптографії додають властивість неспростовності. Викладач підписує оцінку своїм приватним ключем, який зберігається в захищеному сховищі та недоступний іншим. Будь-хто може верифікувати підпис за допомогою відкритого ключа викладача, але підробити підпис без знання приватного ключа практично неможливо.

Основним обмеженням є необхідність організації інфраструктури відкритих ключів – розподілу ключів, управління їх життєвим циклом, відкликання компрометованих ключів. Для великих університетів із сотнями викладачів це стає складним організаційним завданням.

Журнали аудиту фіксують всі операції з даними – створення, читання, модифікацію, видалення. Зберігається інформація про

користувача, часову мітку, IP-адресу, характер операції. Це дозволяє розслідувати інциденти постфактум, виявляти підозрілі патерни поведінки, забезпечувати підзвітність. Однак журнали ефективні лише для ретроспективного аналізу і не запобігають модифікаціям у реальному часі. Централізоване зберігання журналів створює можливість їх видалення або підробки зловмисником з адміністративним доступом.

Для систематизації інформації про різні підходи розглянемо їх порівняльні характеристики (Табл. 1).

Таблиця 1

Порівняльний аналіз систем верифікації

Характеристика	Централізо-вана БД	Хмарне рішення	Цифрові підписи	Блокчейн
Захист від модифікацій	Низький	Середній	Високий	Дуже високий
Стійкість до збоїв	Низька	Висока	Середня	Висока
Масштабованість	Обмежена	Висока	Середня	Середня
Складність впровадження	Низька	Низька	Середня	Висока
Вартість експлуатації	Середня	Низька	Середня	Висока
Прозорість верифікації	Низька	Низька	Висока	Дуже висока
Контроль над даними	Повний	Обмеже-ний	Повний	Розподіле-ний
Швидкодія	Висока	Висока	Середня	Низька

Блокчейн [7; 8] представляє радикально інший підхід до зберігання даних – розподілений незмінний реєстр, де записи об’єднані в блоки, криптографічно пов’язані один з одним. Кожен блок містить хеш попереднього блоку, створюючи ланцюг. Зміна даних в історичному блоці вимагатиме перерахунку всіх наступних блоків, що практично неможливо при достатній кількості учасників мережі.

Для освітніх застосувань перспективними є приватні або консорціумні блокчейни, де вузлами виступають довірені організації – університети, регіональні департаменти освіти, акредитаційні органи [3]. На відміну від публічних блокчейнів типу Bitcoin, вони не потребують

енергоємних механізмів консенсусу типу Proof of Work. Алгоритми Proof of Authority або Byzantine Fault Tolerance забезпечують швидке узгодження при збереженні децентралізації. Застосування блокчейн-технологій в освіті забезпечує чотири ключові переваги [4; 6]. Незмінність історичних записів робить практично неможливою модифікацію оцінок після їх додавання в систему. Прозорість верифікації дозволяє будь-якому учаснику мережі незалежно перевіряти достовірність записів без центрального органу. Міжінституційна сумісність стандартизованого блокчейну дає змогу різним університетам верифікувати документи один одного. Висока відмовостійкість досягається через реплікацію даних на всіх вузлах, що гарантує доступність інформації навіть при виході з ладу окремих компонентів.

Програмні реалізації криптографічних алгоритмів на центральних процесорах є гнучкими та простими у розробці, однак мають обмежену продуктивність. Процесори виконують інструкції послідовно, що обмежує паралелізм обчислень. Хоча сучасні CPU містять спеціалізовані інструкції для прискорення AES та SHA, їх застосовність обмежена конкретними алгоритмами. Графічні процесори забезпечують масовий паралелізм для однотипних обчислень. Для алгоритмів типу SHA-256 GPU можуть досягати на порядок вищої пропускної здатності. Однак архітектура GPU оптимізована для обробки графіки та наукових розрахунків, а не для криптографії. Висока латентність передачі даних між CPU та GPU може нівелювати переваги при обробці невеликих порцій даних. Програмовані логічні інтегральні схеми (FPGA) представляють компроміс між гнучкістю програмних рішень та продуктивністю спеціалізованих чіпів. FPGA складаються з масиву логічних блоків, які можна налаштувати для реалізації довільних цифрових схем. Криптографічний алгоритм реалізується безпосередньо на апаратному рівні, забезпечуючи справжній паралелізм.

Переваги FPGA включають високу пропускну здатність завдяки паралельній обробці, низьку латентність обчислень, енергоефективність порівняно з CPU та GPU, можливість переконфігурації для різних алгоритмів, фізичну ізоляцію криптографічних обчислень від загальної системи, що підвищує безпеку. Енергоефективність FPGA вища завдяки відсутності універсальної операційної системи та спеціалізованій архітектурі. Інтеграція блокчейн з апаратним прискоренням представляє перспективний підхід. FPGA можуть прискорити криптографічні операції блокчейн – хешування блоків, верифікацію цифрових підписів,

обчислення функцій консенсусу. Це дозволить підвищити пропускну здатність блокчейн-систем до рівня, прийнятного для масового використання в освіті. Гібридні архітектури поєднують різні підходи для досягнення оптимального балансу. Наприклад, поточні оцінки можуть зберігатися в традиційній базі даних для швидкого доступу, періодично фіксуючись в блокчейні для незмінності. Найважливіші документи типу дипломів одразу додаються в блокчейн, менш важливі дані залишаються в централізованій системі.

Як приклад практичної реалізації описаних підходів може слугувати система верифікації на базі приватного блокчейну з апаратним прискоренням хешування на FPGA. Архітектура передбачає кілька FPGA-вузлів, які обчислюють хеш-функції для оцінок перед додаванням у блокчейн. Використання навіть недорогих FPGA типу Cyclone IV дозволяє досягти суттєвого прискорення порівняно з програмними реалізаціями при прийнятній вартості обладнання. Блокчейн-компонент реалізується як приватна мережа, де вузлами є університети регіону або країни. Механізм консенсусу Proof of Authority забезпечує швидке підтвердження блоків без енергоємних обчислень. Кожна оцінка перед додаванням хешується на FPGA, хеш додається в блок разом з метаданими. Це забезпечує верифікацію цілісності без розкриття персональних даних студентів у публічному реєстрі.

Така архітектура поєднує переваги обох підходів – надійність та незмінність блокчейну з високою продуктивністю апаратного прискорення, залишаючись економічно доступною для освітніх закладів.

Висновки. Забезпечення довіри до освітніх даних є важливим завданням в умовах цифрової трансформації освіти. Систематичний аналіз загроз показує, що традиційні централізовані системи мають принципові вразливості до несанкціонованих модифікацій, кібератак та внутрішніх зловживань.

Огляд наявних підходів до зберігання та верифікації виявив, що кожне рішення має як переваги, так і суттєві недоліки. Централізовані бази даних забезпечують швидкодію та простоту, але страждають від єдиної точки відмови. Хмарні платформи підвищують доступність, але створюють залежність від постачальника. Цифрові підписи додають неспростовність, проте вимагають складної інфраструктури управління ключами.

Блокчейн-технології представляють найбільш перспективний підхід до створення незмінних реєстрів академічних досягнень.

Розподілена архітектура ліквідує єдину точку відмови, криптографічні зв'язки між блоками роблять практично неможливою модифікацію історичних записів, а механізми консенсусу типу Proof of Authority забезпечують ефективну роботу приватних освітніх мереж. Інтеграція блокчейн-технологій з апаратним прискоренням на FPGA представляє перспективний напрям розвитку систем верифікації освітніх даних. Такий гібридний підхід поєднує незмінність та прозорість розподіленого реєстру з високою продуктивністю спеціалізованих обчислювальних платформ.

Література

1. Ar M. The Use of Blockchain Technology to Enhance Security and Transparency in Educational Certification. *International Journal of Instructional Technology (IJIT)*. 2022. Vol. 01, No 02. Pp. 58–65.
2. Bawane D.H., Sudke Y.S., Pore P.Y. Educational Record Authentication Using Decentralized Consortium Blockchain Technology. *International Journal for Research in Applied Science and Engineering Technology*. 2023.
3. Grech A., Camilleri A. F. *Blockchain in Education*. JRC108255. Seville: Joint Research Centre, 2017.
4. Kolvenbach S., Ruland R., Gräther W., Prinz W. Blockchain 4 Education. *Proceedings of 16th European Conference on Computer-Supported Cooperative Work - Demos and Posters, Reports of the European Society for Socially Embedded Technologies*. 2018.
5. Nguyen M.D., Nguyen-Dinh C.H., Phuong L.A. BOCA: A novel semantic blockchain-based authentication system of educational certificates. *International Journal of Computers and Applications*. 2022. Vol. 44. Pp. 1074–1082.
6. Pinto Orellana D. F., Piedra N. Design of a data model for the decentralized management of digital educational credentials using blockchain in the framework of open digital badges. *12th International Conference On Software Process Improvement (CIMPS)*. 2023. Pp. 106–115.
7. Poorni R., Lakshmanan M., Bhuvaneswari S. DIGICERT: A Secured Digital Certificate Application using Blockchain through Smart Contracts. *2019 International Conference on Communication and Electronics Systems (ICCES)*. 2019. Pp. 215–219.
8. Prinz W., Kolvenbach S., Ruland R. *Blockchain for Education: Lifelong Learning Passport*. ERCIM News. 2020.