УДК 004.056 + 004.658

Інформаційна технологія захищеного зберігання результатів академічної успішності

Юрій Володимирович Баришев
к. т. н., доцент
доцент кафедри захисту інформації
Вінницький національний технічний університет
ORCID: 0000-0001-8324-8869

Владислава Сергіївна Ланова
студентка факультету інформаційних технологій та комп'ютерної інженерії
Вінницький національний технічний університет
ORCID: 0009-0007-4025-1866

Анотація. У статті визначено актуальність досліджень щодо захисту результатів академічної успішності в навчальних закладах. Проаналізовано нормативно-правову базу, що регулює вимоги до захисту цієї інформації. Наведено аналіз методів та засобів, що використовуються для захисту результатів академічної успішності. На основі аналізу визначено шляхи удосконалення відомих рішень, які стали підґрунтям для пропонування власного рішення такого захисту.

Наведено результати проєктування моделі даних предметної області. На основі цієї моделі проаналізовано вимоги до безпеки атрибутів сутностей, пов'язаних із академічною успішністю студентів. Для досягнення мети адаптовано метод захищеного зберігання даних для інформації щодо покращення його застосовності для захисту результатів академічної успішності. Запропоновано рішення, яке передбачає одночасне застосування централізованих та децентралізованих сховищ даних, що дозволяє покращити рівень захисту цілісності та доступності даних, порівняно з централізованими сховищами, та підвищити рівень захисту конфіденційності та зменшення надлишковості даних, порівняно з децентралізованими сховищами.

Для доведення концепції наведено одну з можливих архітектур програмного застосунку, який реалізує запропоновану інформаційну технологію. Цю архітектуру реалізовано як клієнт-серверний веб-застосунок, який надає інтерфейс користувачеві для захищеного зберігання даних в реляційній базі даних, розподіленому сховищі IPFS та блокчейні, який підтримує смарт-контракти. Наведено результати статичного тестування безпеки та юніт-тестування цього розробленого програмного застосунку для захищеного зберігання відомостей академічної успішності. Це дозволило довести безпеку розроблених смарт-контрактів, а також можливість використання запропонованого засобу в практичних ситуаціях в межах освітнього процесу навчальних закладів. Визначено перспективи подальших досліджень.

Ключові слова: кібербезпека, децентралізовані системи, реляційна база даних, критична інфраструктура, освіта, захист інформації.

DOI: https://doi.org/10.31649/1999-9941-2024-60-2-17-30

Information technology for secure storing of academic performance results

Yurii Baryshev

PhD (eng), Associated Professor,
Associated Professor of Information Protection Department
Vinnytsia National Technical University
ORCID: 0000-0001-8324-8869

Vladyslava Lanova

Student of Information Technology and Computer Engineering Faculty
Vinnytsia National Technical University
ORCID: 0009-0007-4025-1866

Abstract. The relevance of research on the protection of academic performance results in educational institutions is defined at the article. The legal framework regulating information protection requirements for the case was analyzed. The analysis of used mechanisms and tools of for the academic performance results protection used by known tools was presented. On the basis of the analysis, approaches for known solutions improvement were defined, that became the basis for proposing the solution for such protection. The results of data model designing are presented. On the basis of this model, the requirements for security attributes of the entities related to students' academic performance were analyzed. To achieve the goal, the method of secure data storing of the academic performance results was adapted in order to improve scalability for the information protection in the academic field. The solution is proposed that involves simultaneous utilizing of centralized and decentralized data repositories, which allows to improve the level of protection of data integrity and availability in comparison too centralized repositories, and to increase the level of privacy protection and reduce data redundancy in comparison to decentralized repositories. To yield proof-of-concept, one of the possible architectures of the software application that implements the proposed information technology is presented. This architecture is implemented as a client-server web application that provides a user interface for secure data storage utilizing the relational database, distributed storage IPFS and blockchain, which supports smart contracts. The testing results of this developed software application for secure storing of academic performance information were presented. This made it possible to prove the security of the developed smart contracts, as well as the possibility of the proposed technology utilization in practical situations within the business processes of educational institutions. The perspectives of further research were defined.

Key words: cyber security, decentralized systems, relational database, critical infrastructure, education, information security.

Вступ. Необхідність захисту персональних даних учасників освітнього процесу відзначається вимогами Закону України "Про захист персональних даних" (Law of Ukraine No. 2297-VI). Ця інформація вимагає належного забезпечення конфіденційності, цілісності і доступності. Зокрема, процес нарахування стипендій потребує одночасного дотримання цих трьох критеріїв для результатів академічної успішності. У випадку їх порушення подальше провадження освітньої діяльності у вищих навчальних закладах може бути зупинене, що негативно позначиться і на інших видах їх діяльності. Відповідно важливо запобігти цьому з урахуванням, що заклади вищої освіти часто належать до критичної інфраструктури (Resolution of the Cabinet of Ministers of Ukraine No. 1109).

Багато країн встановлюють суворі законодавчі вимоги, такі як Загальний регламент з охорони даних (GDPR) в Європейському Союзі, який не лише визначає вимоги щодо захисту даних, але й регламентує фіскальні наслідки для організацій, що не дотримуються цих вимог (Hjerppe et al., 2019). Таким чином, захист персональних даних є актуальним для закладів освіти і ця актуальність лише зростатиме з поглибленням інтегрування до Європейського Союзу.

Централізовані бази даних не забезпечують достатній рівень захисту доступності, оскільки передбачають локалізоване зберігання даних, що породжує єдину точку відмови в інформаційній системі. Крім того, вони поступаються децентралізованим сховищам даних у захисті цілісності даних. Тому використання децентралізованих технологій зберігання даних, таких як технологія блокчейн, може бути ефективним рішенням для покращення рівня захисту цілісності та доступності даних. Однак, слід враховувати, що відкритість блокчейну породжує проблеми конфіденційності, і сама технологія вимагає значно більших ресурсів, порівняно з традиційними базами даних, тому для досягнення адекватного рівня кібербезпеки актуально розробити модель даних, яка дозволить поєднати переваги обох технологій для захисту відомостей академічної успішності.

Таким чином постає актуальна задача поєднати сильні сторони бази даних та технологій розподіленого зберігання даних для забезпечення захисту цілісності, доступності та конфіденційності персональних даних, вимоги до яких регламентуються законодавством України та GDPR.

Метою є покращення рівня захищеності даних академічної успішності шляхом розроблення інформаційної технології, що дозволить поєднати технології розподіленого зберігання даних з реляційною базою даних.

Для досягнення мети необхідно розв'язати такі задачі:

- проаналізувати відомі рішення для захисту інформації освітнього процесу;
- розробити модель даних;
- проаналізувати вимоги до безпеки атрибутів в моделі даних;
- розробити інформаційну технологію для захисту результатів академічної успішності;
- реалізувати та протестувати розроблену інформаційну технологію.

Аналіз відомих рішень. Згідно із законами України «Про захист інформації в інформаційно-телекомунікаційних системах» (Law of Ukraine No. 80/94-VR, 2023) та «Про захист персональних даних» (Law of Ukraine No. 2297-VI, 2012), вимагається високий рівень захисту конфіденційності, цілісності та доступності освітніх даних. Зокрема, Єдина державна електронна база з питань освіти (ЄДЕБО) визначається як ключовий інструмент для зберігання та обробки інформації про систему освіти (info.edbo.gov.ua).

Забезпечення цілісності даних важливо для правильного нарахування стипендій та рішень про відрахування студентів. Недоступність ЄДЕБО може призвести до зупинки процесів у закладах вищої освіти, впливаючи на доступність інформації та процедур ухвалення таких рішень. При цьому удосконалення цієї системи потребує урахування необхідності у захисті конфіденційності відомостей, що там зберігаються, що істотно впливає на масштабованість цього рішення.

Одним із альтернативних засобів інформаційно-комунікаційних технологій є система «Moodle» – модульне об'єктно-орієнтоване навчальне середовище для управління контентом освітнього процесу (moodle.org). Для роботи системи «Moodle» необхідні три складові: веб-сервер, база даних і поштовий сервер. Використання декількох розподілених рішень породжує проблему захисту персональних даних, якими ці застосунки обмінюються під час експлуатації. У випадку витоку особистих даних, таких як імена, поштові адреси та дані облікового запису користувача, відкривається можливість для незаконного доступу до конфіденційної інформації. Це створює сприятливі умови для зловмисників, які можуть

використовувати різні методи, наприклад, фішингові атаки через електронну пошту або текстові повідомлення. Ці атаки спрямовані на отримання доступу до особистих даних на інших онлайн-ресурсах та можуть викликати серйозні наслідки для осіб, конфіденційна інформація яких стала доступною зловмисникам (Belov O., & Delembovskyi M.M., 2021).. Відповідно, в разі витоку персональних даних, записи, що стосуються здобувачів освітнього процесу та працівників, можуть бути втрачені або використані в незаконних цілях.

Серед відомих платформ для організації освітнього процесу варто відзначити Google Classroom, який розроблений компанією Google (classroom.google.com). За допомогою цієї інформаційної технології у викладача є можливість бачити статистику виконання лабораторних робіт студентами, планувати час розсилання завдань, визначати терміни складання завдань, надсилати інформацію одразу всім учасникам групи. Однак, Google Classroom має обмежені функціональні можливості, оскільки немає механізмів зберігання результатів академічної успішності, вести журнал викладачеві чи мати електронний щоденник студентові, які передбачені нормативно-правою базою освітнього процесу у вищій школі. Крім того, інформація, що зберігається на Google-диску доступна, як мінімум, компанії Google та потребує додаткових засобів захисту інформаційно-комунікаційних ліній, що заважає широко застосовувати цю платформу в освітньому процесу через згадане вище законодавче регулювання захисту інформації.

Серед платформ, що забезпечують захист персональних даних учасників освітнього процесу, відповідно до вимог трьох критеріїв захищеності є платформи з використанням децентралізованих сховищ зберігання даних.

Open Campus (opencampus.xyz) є децентралізованою технологією, яка спрямована на вирішення задач сучасної освіти. В її основі лежить інтегрована система, що об'єднує учнів, викладачів та навчальні заклади, забезпечуючи нові можливості для співпраці через використання блокчейн-технологій. Платформа також виступає як спільнота, сприяючи обміну знань, з метою покращення результатів для всіх учасників освітнього процесу.

Не зважаючи на зашифроване передавання даних, завжди існують ризики витоку особистої інформації при обміні даними між різними сторонами. Таким чином, використання виключно блокчейн технології, як зазначено в даному рішенні, може спричинити проблеми з конфіденційністю даних, які порушують закони та нормативно-правові акти (Laws of Ukraine No. 2297-VI, No. 80/94-VR). Ще одним недоліком є те, що не всі здобувачі та викладачі володіють знаннями та навичками в користуванні децентралізованими сховищами, тому необхідно провести тренінги та курси для навчання учасників освітнього процесу перед її впровадженням.

В роботі (Panagiotidis, 2022) розглянуто платформу для провадження освітнього процесу з використанням технології блокчейн – школу Голбертона. Їх інформаційна система на основі технології блокчейн зберігає всі види освітньої активності учнів: унікальний ідентифікатор учня, його поведінку під час навчання, досвід мікроакадемічних проєктів та макрорівень здобутої освіти.

Sony Global Education (sony.com) розробила технологію, яка застосовує блокчейн у сфері освіти, використовуючи безпечні властивості блокчейну для забезпечення зашифрованої передачі даних — таких як академічні досягнення та показники прогресу — між двома визначеними сторонами. Наприклад, після складання іспиту для демонстрації свого рівня академічної підготовки, особа може доручити організації, що проводить тестування, поділитися результатами іспиту з однією або кількома сторонніми організаціями, які проводять моніторинг якості освіти.

Не зважаючи на те, що блокчейн є децентралізованою технологією, у випадку Sony Global Education може виникнути ризик того, що компанія чи окремі організації, які керують платформою, можуть отримати надмірний контроль над даними. Це може призвести до ситуацій, коли дані учнів та їх академічні досягнення можуть бути використані в корисливих цілях або для маніпуляцій.

Можливість інтегрування розподілених сховищ даних, зокрема блокчейнів розглянута в роботах (Steiu, 2020). Однак попри покращення захисту цілісності недоліком цих систем є те, що блокчейн краще себе проявляє в задачах, де до нього записують невеликі за обсягом дані, адже їх потрібно копіювати на кожен вузол блокчейна. Таким чином масштабувати таку системах в межах вищого навчального закладу, а тим паче країни — невиправдано витратно та накладає обмеження на швидкість записування даних (Steiu, 2020). Крім того, зберігання даних на блокчейні, які не потребують підвищеного рівня захисту даних – є надлишковим.

Open Source University містить компонент навчання, а всі платежі постачальникам навчального контенту здійснюються за допомогою смарт-контрактів, що забезпечує безпеку. Ця платформа прагне використовувати блокчейн для користі усіх трьох ключових учасників освітнього процесу: студентів, академії та бізнесу (Steiu, 2020).

Однією з переваг використання блокчейну в освіті є можливість створення безпечного та зберігання результатів академічної успішності із підвищеною захищеністю до підробки відомостей. Кожен запис, такий як академічні досягнення, відомості про успішність виконання передбачених видів робіт та вивчені дисципліни, може бути зафіксований в блокчейні, що робить його стійким до зламу та відстежуваним.

Ще однією перевагою є те, що інформація про досягнення студентів та викладачів зберігається не на одному сервері, а на кількох вузлах мережі. Це знижує ризик втрати даних через технічні збої чи зломи центральної бази. Якщо блокчейни підтримують смарт-контракти (Kemmoe et al., 2020; Taherdoost, 2023), такі як Ethereum (Wood, 2024) чи Solana (Yakovenko). Для завдань освітнього процесу смарт-контракти можуть автоматично перевіряти виконання умов для отримання дипломів або сертифікатів. Наприклад, після успішного складання всіх іспитів система автоматично видавати сертифікат, без необхідності втручання людини. Здобувачі освіти можуть мати постійний доступ до своїх даних та кваліфікацій, незалежно від місця знаходження або навчального закладу (Taherdoost, 2023),. Це особливо важливо для міжнародних програм і академічної мобільності здобувачів.

Серед недоліків використання виключно децентралізованих сховищ зберігання даних можна зазначити проблему із захистом конфіденційності, яку породжує відкритість блокчейну. Оскільки блокчейн є розподіленою системою, всі транзакції, що проходять через нього, зберігаються на багатьох вузлах і можуть бути доступними для перегляду будь-якому користувачу мережі. Це створює ризики, що стосуються розкриття персональних даних студентів, таких як імена, академічні досягнення або інші конфіденційні відомості. У випадку академічних результатів це може призвести до того, що сторонні особи отримають доступ до чутливої інформації про успішність студентів, їх оцінки та інші академічні показники. Оскільки ці дані є персональними і підпадають під вимоги законів про захист персональних даних, таких як Загальний регламент про захист даних (GDPR) в ЄС та національні закони, такі як Закон України "Про захист персональних даних", їх публічність може стати серйозним порушенням законодавства, що відповідно може породити небажані наслідки такі, як фіскальні стягнення за недотримання вимог GDPR.

Таким чином, зважаючи на вищевикладене, можна зробити висновок, що наразі існує актуальна потреба в розробці інформаційної технології, яка забезпечить стійкий захист освітніх даних, зокрема відомостей, які пов’язані із академічною успішністю здобувачів освіти.

Матеріали та методи. Зважаючи на наведений вище аналіз, випливає, що при розробці інформаційної технології варто враховувати вимоги щодо захисту цілісності, доступності та конфіденційності даних. Крім того, аналіз показав, що застосування сховищ даних одного типу не забезпечує всі три вимоги природним чином, а тому доводиться вводити додаткові механізми щодо захисту. Виходом з цієї ситуації є рішення, де буде гібридно поєднано централізовані та децентралізовані сховища зберігання даних, такі як реляційна база даних (Harrington, 2016), яка є централізованим сховищем зберігання даних, а також

децентралізованими. До останніх належать блокчейн та розподілені сховища такі як внутрішньопланетна файлова система IPFS (docs.ipfs.tech) або фреймворк зберігання даних Storj (Storj Lab, 2024).

Централізовані сховища, як-от реляційні бази даних, забезпечують швидкий доступ і зручність управління даними. Вони добре підходять для зберігання великих обсягів інформації, яка не потребує надмірного рівня конфіденційності або може бути змінена в майбутньому. Наприклад, такі системи можна використовувати для зберігання допоміжних даних, що не мають чутливого характеру, або для зберігання даних, які можуть потребувати частого оновлення.

З іншого боку, децентралізовані сховища, такі як блокчейн та IPFS, мають переваги в захисті цілісності та доступності даних, оскільки вони зберігають дані на численних вузлах і є стійкими до атак. Децентралізовані технології особливо корисні для забезпечення прозорості і довіри, адже зміни в таких системах є незворотними, що забезпечує захист від маніпуляцій із даними. Проте, зберігання великих обсягів інформації в блокчейні може бути надто ресурсомістким та не завжди виправданим через високі витрати на обробку транзакцій.

Поєднання цих двох підходів дозволяє отримати баланс між безпекою, продуктивністю та ефективністю зберігання (Baryshev & Lanova, 2023). Децентралізовані системи можуть використовуватися для зберігання найважливіших або незмінних даних, таких як результати іспитів або сертифікацій, у той час як централізовані бази даних можуть бути використані для оперативного управління поточними даними, що потребують частого оновлення. В роботі (Baryshev & Lanova, 2023). наведено метод для зберігання даних на основі таких гібридних сховищ, який базується на класифікуванні інформації предметної області відповідно до вимог щодо захисту інформації та залежно від класу використовувати окреме джерело з-поміж реляційною базою даних (Wood, 2024), блокчейном, який підтримує смарт-контракти (Yakovenko; Harrington, 2016), та розподіленим сховищем даних, однак він орієнтований на іншу предметну область, тому не може бути застосований без модифікацій у цих дослідженнях.

Нехай D – множина даних предметної області, тоді вона, відповідно до метода (Baryshev & Lanova, 2023)., розбивається на такі підмножини залежно від вимог до інформації:

- множина даних, що не потребують підвищених вимог до захисту D_u;
- множина даних, що потребують підвищених вимог лише до захисту конфіденційності D_c;
- множина даних, що потребують підвищених вимог лише до захисту доступності D_a;
- множина даних, що потребують підвищених вимог лише до захисту цілісності D_i;
- множина даних, що потребують підвищених вимог до захисту конфіденційності та цілісності, але не мають таких вимог щодо захисту доступності D_{ci};
- множина даних, що потребують підвищених вимог до захисту конфіденційності та доступності, але не мають таких вимог щодо захисту цілісності D_{ca};
- множина даних, що потребують підвищених вимог до захисту цілісності та доступності, але не мають таких вимог щодо захисту конфіденційності D_{ia};
- множина даних, що потребують підвищених вимог щодо захисту і конфіденційності, і цілісності, і доступності D_{cia}.

Відповідно множина даних розглядається таким чином:

$$D = \{D_u, D_c, D_i, D_a, D_{ci}, D_{ca}, D_{ia}, D_{cia}\}. \quad (1)$$

Нехай S – множина сховищ даних, які використовуються в системі. Оскільки основною пропозицією є одночасне застосування декількох сховищ даних, тому ця множина представляється таким чином:

$$S = \{s_{DB}, s_{IPFS}, s_{bc}\}, \quad (2)$$

де s_{DB} – база даних, s_{IPFS} – розподілене сховище, s_{bc} – блокчейн.

Відповідно у загальному процедура зберігання даних з точки зору користувача формалізується таким чином:

$$storing: D \to S. \quad (3)$$

Однак наявність трьох сховищ даних вимагає відповідні три процедури зберігання з точки зору інформаційної системи:

- $storing_{DB}$ – процедура зберігання даних в базі даних s_{DB};
- $storing_{IPFS}$ – процедура зберігання даних в децентралізованому сховищі даних s_{IPFS};
- $storing_{bc}$ – процедура зберігання даних в блокчейні s_{bc}.

При цьому лише дані певних класів будуть зберігатись у цих сховищах залежно від того, захист яких саме властивостей інформації дозволяє забезпечувати те чи інше сховище. Оскільки бази даних дозволяють найкраще зберігати конфіденційності порівняно з іншими сховищами, тому s_{DB} буде використана для захисту конфіденційних даних. Крім того, дані, які не потребують підвищених вимог до захисту також доцільно зберігати в цьому сховищі, оскільки вартість операційних витрат та швидкість операцій зчитування/запису у цього сховища найвища поміж тих, що входять до *S*. Відповідно, процес записування даних до бази даних для задачі дослідження формалізується таким чином:

$$storing_{DB}: \{D_u, D_c, D_{ci}, D_{ca}, D_{cia}\} \to s_{DB}. \quad (4)$$

Запис до децентралізованих сховищ дозволяє забезпечити підвищений захист цілісності та доступності інформації. При цьому блокчейн дозволяє досягти кращих показників, але в силу технічних обмежень на розмір блока (Wood, 2024), цей носій не придатний для зберігання великого обсягу даних. Тому підмножини множини *D*, які не були залучені до процедури $storing_{DB}$, потребують подальшого поділу. Так множина даних, що потребують підвищених вимог лише до захисту цілісності D_i розбивається таким чином:

$$D_i = \{D^s{}_i, D^l{}_i\}, \quad (5)$$

де $D^s{}_i$ – множина даних малого обсягу, що потребують підвищених вимог лише до захисту цілісності, $D^l{}_i$ – множина даних великого обсягу, що потребують підвищених вимог лише до захисту цілісності.

Якщо розбити аналогічним чином D_a, та D_{ia}, тоді формалізація процесу записування даних до розподіленого сховища набуде такого вигляду:

$$storing_{IPFS}: \{D^l{}_i, D^l{}_a, D^l{}_{ia}\} \to s_{IPFS}. \quad (6)$$

Аналогічним чином визначається процес зберігання даних до блокчейну:

$$storing_{bc}: \{D^s{}_i, D^s{}_a, D^s{}_{ia}\} \to s_{bc}. \quad (7)$$

Таким чином отримано ідеалізований опис інформаційної технології захищеного зберігання даних. На практиці під час реалізації моделі необхідно передбачити додаткові механізми захисту, зокрема, додати механізми захисту цілісності для даних, що належать до множин D_{ci} та D_{cia}, адже вони також вимагають підвищеного рівня захисту цілісності. І при цьому то рівень захисту цілісності, який забезпечується засобами баз даних, є нижчим за

рівень, що забезпечується розподіленими технологіями, зокрема блокчейном. Відповідно адекватним рішенням буде частково залучити сховище s_{bc} для збереження технічних даних, які не містять конфіденційних відомостей, але які дозволять покращити контроль за цілісністю бази даних s_{DB}.

Модель даних. З математичного опису випливає, що для реалізації описаної технології необхідно попередньо виконати аналіз специфіки предметної області освітнього процесу, а саме обліку академічної успішності. З цією метою взято шаблон відомості обліку академічної успішності, а також дані освітнього процесу, які пов’язані із відомістю.

У результаті проєктування було побудовано реляційну модель даних, яка містить 6 основних сутностей:

- інформація про результати;
- інформація про освітню програму;
- інформація про відомість;
- інформація про дисципліну;
- інформація про студента;
- інформація про групу.

Доцільно буде навести діаграму зв’язків між цими сутностями та їх атрибутами. На основі аналізу цих сутностей та їх атрибутів розроблено модель даних (рис. 1).

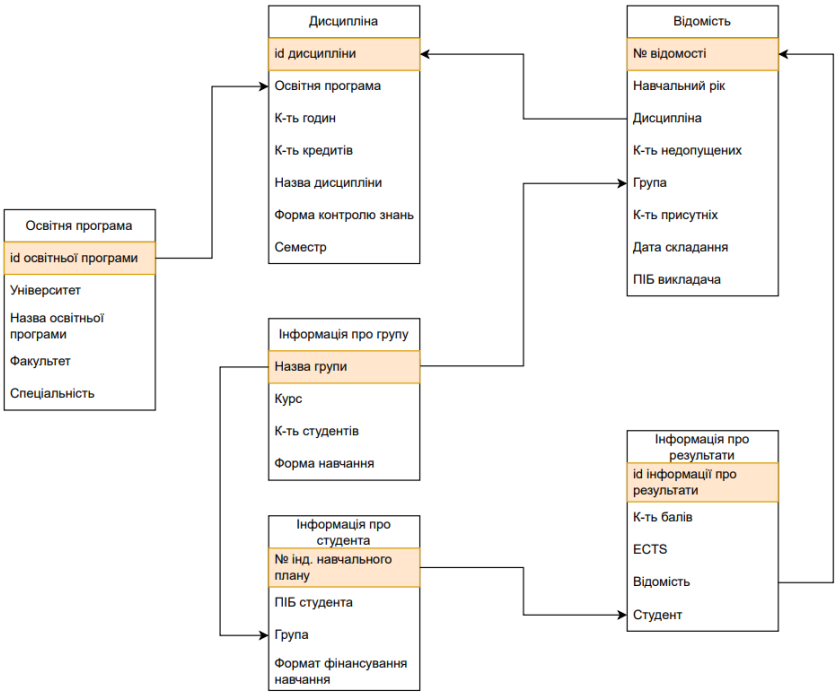


Рисунок 1. Вигляд реляційної моделі даних

Джерело: розроблено авторами.

Наведена на рис. 1 база даних є нормалізованою до нормальної форми Бойса-Кодда (Harrington, 2016; Lee, 1995). Відношення знаходиться в нормальній формі Бойса-Кодда, якщо вся надмірність на основі функціональної залежності була видалена, хоча інші типи надмірності можуть все ще існувати (Lee, 1995).

На основі розробленої моделі можна проаналізувати вимоги до безпеки кожного з атрибутів.

Для того, щоб визначити вимоги до безпеки атрибутів в моделі даних, було проаналізовано усі сутності та їх атрибути відповідно математичного опису, наведеного

вище, з урахуванням рівня вимог до захисту цілісності, доступності та конфіденційності. Приклад, отриманих результатів цього аналізу для атрибутів сутності "Відомість" наведено в таблиці 1.

Таблиця 1. Аналіз вимог до захисту інформації про відомість

Відомість	Захист цілісності	Захист доступності	Захист конфіденційності
№ відомості	+	-	+
Навчальний рік	-	-	-
Дисципліна	+	-	-
Назва групи	-	+	-
К-ть недопущених	-	-	-
К-ть присутніх	-	-	-
Дата складання	+	+	-
ПІБ викладача	+	+	-

Джерело: розроблено авторами.

Проаналізувавши вимоги до безпеки атрибутів кожної із сутностей аналогічним чином визначено найкращу технологію для їх зберігання відповідно до підходу, наведеного в математичному описі. Так записи, що є невеликими за обсягом та потребують підвищеного захисту цілісності та/або доступності, але не конфіденційності – зберігаються в блокчейні, записи, які містять конфіденційні відомості або не потребують підвищеного захисту взагалі – в базу даних, а великі за обсягом дані, які повинні були б за критеріями потрапити в блокчейн – помістити в іншу децентралізовану систему зберігання даних — IPFS.

Результати та Обговорення. З математичного опису випливає, що для реалізації описаної технології необхідно попередньо виконати аналіз специфіки предметної області освітнього процесу, а саме обліку академічної успішності. З цією метою взято шаблон відомості обліку академічної успішності, а також дані освітнього процесу, які пов’язані із відомістю. Інформаційна технологія передбачає використання клієнт-серверного веб-застосунку для надання інтерфейсу користувачам до обробки даних, а також інкапсуляції складності одночасної взаємодії із різними контейнерами для зберігання даних. Серверна частина цього веб-застосунку взаємодіє із базою даних (на основі програмного інтерфейсу служби управління базами даних), блокчейном та IPFS (рис. 2).

Запропонований підхід реалізує шаблон інформаційного брокера, але при цьому не зробить сервер, єдиною точкою відмови, адже у випадку атак на нього частина інформації, записаної до блокчейну та IPFS залишатиметься доступною, що дозволить досягти покращення порівняно із системами, які використовують лише централізовані бази даних.

Для доведення концепції було реалізовано запропонований підхід для зберігання результатів заліково-екзаменаційної сесії у ЗВО. Було створено реляційну базу даних під назвою MyUniversity, в якій будуть зберігатись дані, які потребують підвищеного захисту конфіденційності або не потребують підвищеного захисту даних взагалі (рис. 3).

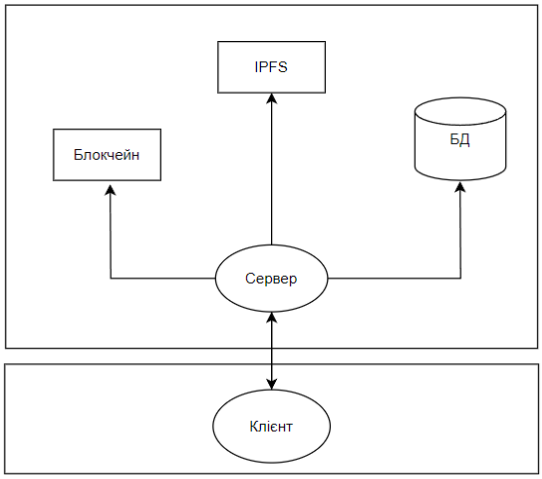


Рисунок 2. Схематичне зображення інформаційної технології

Джерело: розроблено авторами.

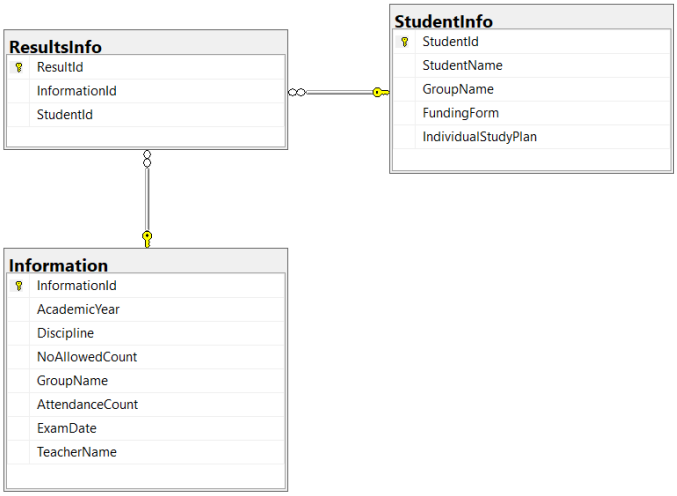


Рисунок 3. Вигляд діаграми зв’язків реляційної бази даних

Джерело: розроблено авторами.

Кожне із визначених полів таблиць не може бути порожнім, це дозволяє уникнути неповних або хибних записів. Для кожної із таблиць було визначено ключове поле.

Для даних, які, відповідно до вищевизначених критеріїв, необхідно зберігати в блокчейні, було розроблено окремі смарт-контракти під кожну із сутностей. Це забезпечить зручність взаємодії із кожною сутністю.

Варто розглянути для прикладу логіку смарт-контракту, який забезпечує зберігання інформації про освітню програму. Логіка смарт-контракту полягає в тому, що розроблений смарт-контракт дозволяє додавати та отримувати інформацію про освітні програми за допомогою унікальних ідентифікаторів, які формуються на основі внесених атрибутів, які стосуються цієї сутності. Розроблений смарт-контракт було розгорнуто в тестовій мережі Goerli (goerli.net).

Інші контракти, для інших сутностей, реалізовані за аналогічним принципом.

IPFS побудовано навколо децентралізованої системи користувачів-операторів, які зберігають частину загальних даних, створюючи стійку систему зберігання та спільного використання файлів.

IPFS доцільно використовувати для файлів порівняно великого обсягу. Зокрема у виконаній реалізації у файлову систему передбачається завантаження силабусів дисциплін та знеособлені дані з відомостей академічної успішності.

Інтерфейс веб-застосунку на прикладі форми створення відомостей наведено на рис. 4.

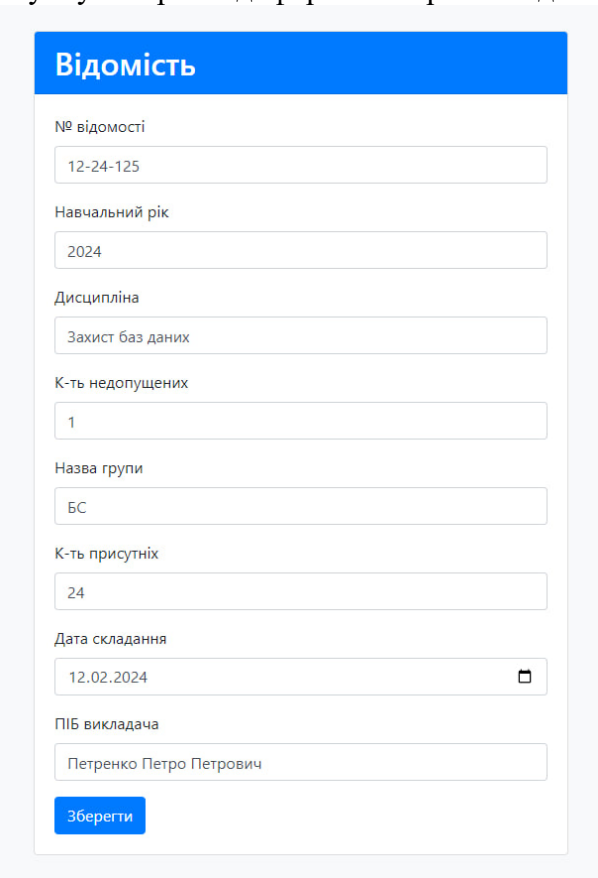
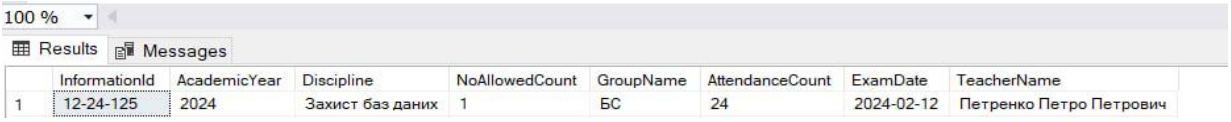


Рисунок 4. Вигляд заповненої форми з інформацією про академічну успішність

Джерело: розроблено авторами.

На рис. 5 наведено ту частину даних, які записались в базу даних, а на рис. 6 — ті дані, які записались в блокчейн за допомогою розгорнутого смарт-контракту [24].



	InformationId	AcademicYear	Discipline	NoAllowedCount	GroupName	AttendanceCount	ExamDate	TeacherName
1	12-24-125	2024	Захист баз даних	1	БС	24	2024-02-12	Петренко Петро Петрович

Рисунок 5. Фрагмент заповненої бази даних

Джерело: розроблено авторами.

Задля тестування безпеки в цій реалізації використано фреймворк Slither (Feist et al., 2019), який застосовувався для тестування безпеки смарт-контрактів, оскільки саме вони є критичним місцем з точки зору безпеки і через властивості блокчейнів не можуть бути змінені після розгортання.

Slither не лише виявляє вразливості, але й надає детальний аналіз та рекомендації щодо їх усунення, що дозволяє розробникам оперативно вносити зміни. Використання такого інструменту є необхідним кроком у розробці децентралізованих систем, оскільки помилки в смарт-контрактах можуть призвести до невідновних втрат даних або фінансових збитків. Зокрема, у разі реалізації смарт-контрактів для зберігання критичних даних, таких як

академічні результати, необхідність виявлення та усунення вразливостей є першочерговим завданням.

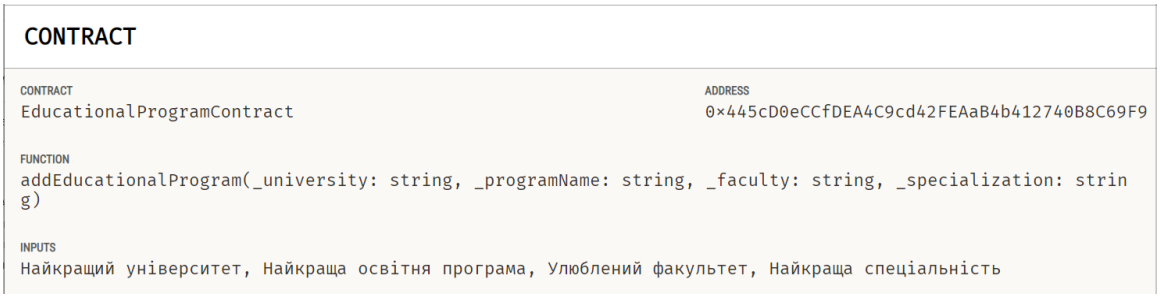


Рисунок 6. Вигляд доданих даних в блокчейн з форми “Інформація про освітню програму”

Джерело: розроблено авторами.

Результати тестування показали, що запропоновані смарт-контракти відповідають вимогам безпеки, що дозволяє інтегрувати їх в освітні процеси без ризику компрометації даних або збоїв у функціонуванні системи (рис. 7).

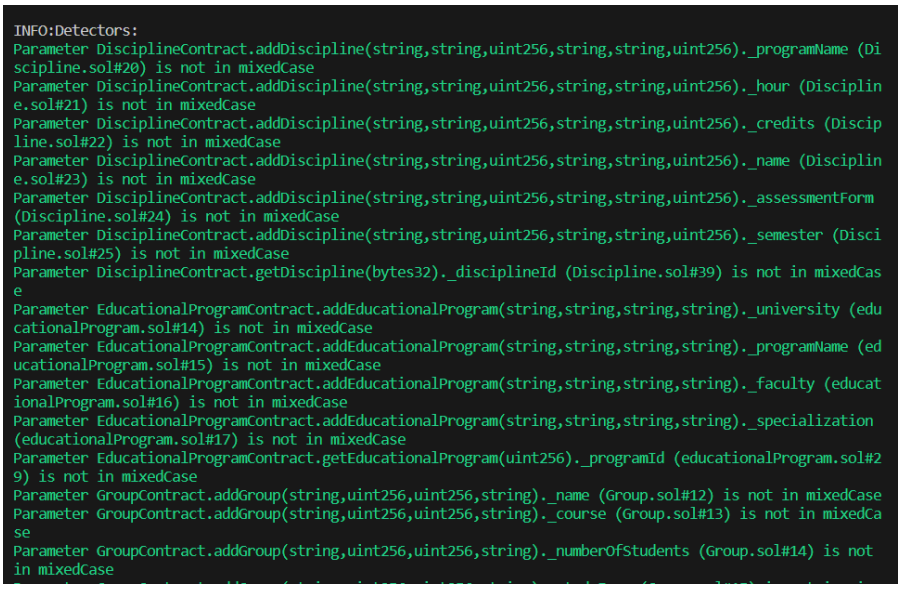


Рисунок 7. Вигляд результатів статичного тестування безпеки смарт-контрактів

Джерело: розроблено авторами.

Також було проведено юніт-тестування функцій та методів програмного коду. Юніт-тестування є важливим доповненням до статичного тестування безпеки, оскільки забезпечує динамічну перевірку функціональності коду**.** Хоча статичний аналіз, наприклад, за допомогою таких інструментів як Slither, може виявляти потенційні вразливості та помилки без запуску програми, юніт-тести надають можливість перевірити, як конкретні модулі або функції коду працюють під час виконання. Результати юніт-тестування підвердили коректність ухвалених технічних рішень під час розробки смарт-контрактів.

Таким чином вдалося експериментально довести концепцію запропонованої інформаційної технології та можливість її реалізації для розв’язання практичних завдань щодо захисту даних в освітньому процесі.

Висновки. Як показав аналіз інформаційних технологій для організації освітнього процесу традиційні інформаційні системи які використовують централізовані сховища даних такі як ЄДЕБО мають єдину точку відмови. І коли втрачається доступність до цієї системи зупиняється низка освітніх процесів. Водночас підходи, які базуються виключно на розподілених системах зберігання даних, мають недостатню масштабованість та потребують багато ресурсів. Саме тому в роботі запропоновано інформаційну технологію для захищеного зберігання результатів академічної успішності, яка пом'якшує ці недоліки завдяки класифікації інформації та відповідному розподілу її поміж різними сховищами залежно від потреб у захисті конкретного атрибуту в моделі даних.

Було проаналізовано відомі інформаційні технології обробки освітніх даних, в результаті чого аналіз показав, що платформи, які не використовують технологію блокчейн не є захищеними, не гарантують одночасний захист усіх критеріїв захисту та не забезпечують належний рівень захисту доступності та цілісності. Відповідно до вищезгаданих результатів аналізу було створено теоретико-множинний математичний опис інформаційної технології, що пропонується для захисту результатів академічної успішності студентів. На основі цього було спроєктовано модель даних, проаналізовано вимоги до безпеки кожного із атрибутів сутностей моделі даних та розроблено метод захищеного зберігання освітніх даних.

Практична реалізація інформаційної технології для закладу вищої освіти дозволила довести здійсненність запропонованого підходу. Тестування цієї технології дозволило довести можливість поєднання реляційних баз даних з розподіленими системами зберігання даних, які підвищують рівень захисту цілісності та доступності, що є критично важливим для забезпечення безперервності освітніх процесів. Крім того, завдяки використанню блокчейну для зберігання академічних досягнень студентів, було досягнуто суттєвого покращення в частині прозорості та відстежуваності даних, що сприяє підвищенню довіри до системи з боку як студентів, так й органів із забезпечення якості освіти та адміністрації закладу.

Перспективою розвитку є масштабування отриманих результатів на інші процеси обробки освітніх даних, а також для взаємодії з іншими освітніми процесами. Також перспективним буде створення спеціалізованого блокчейна для завдань освітнього процесу.

Подяки. «Немає».

Конфлікт інтересів. «Немає».

Стаття надійшла: 04.06.2024.

References.

Baryshev, Y., & Lanova, V. (2023). Method of the Protected Storage of Medical Data, Based On The Relational Database And Blockchain. *Scientific Works VNTU, 3*, 9 p. Retrieved from https://works.vntu.edu.ua/index.php/works/article/view/638/633.

Belov O., & Delembovskyi M.M. (2021). Organization of Protection and Security in the Moodle System. In *IX international scientific and practical conference "Theory and practice of using the Moodle learning management system"*, Retrieved from https://2021.moodlemoot.in.ua/course/view.php?id=23. [in Ukrainian]

Blockcerts. The Open Standard for Blockchain Credentials. Retrieved from https://www.blockcerts.org/guide/.

EDBO About. Accessed: Jul. 1, 2024Retrieved from https://info.edbo.gov.ua/about/.

Feist J., Grieco G., & Groce A. (2019). Slither: a static analysis framework for smart contracts. In *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*. IEEE, 8-15.

Goerli Testnet: A cross-client proof-of-authority testing network for Ethereum Accessed: Jul. 1, 2024. Retrieved from https://goerli.net/#about

Google Classroom – Management Tools & Resources. Accessed: Jul. 1, 2024. Retrieved from https://classroom.google.com/.

Harrington, J. L. (2016). *Relational Database Design and Implementation*. Fourth Ed. Elsevier.

Hjerppe, K., Ruohonen, J., & Leppanen, V. (2019). The General Data Protection Regulation: Requirements, architectures, and constraints. In *Proceedings of the 2019 IEEE 27th International Requirements Engineering Conference (RE)*. doi: 10.1109/re.2019.00036.

IPFS documentation. Accessed: Jul. 1, 2024. Retrieved from https://docs.ipfs.tech/.

Kemmoe, V. Y., Stone, W., Kim, J., Kim, D. & Son, J. (2020). Recent Advances in Smart Contracts: A Technical Overview and State of the Art. *IEEE Access*, vol. 8, pp. 117782-117801, Retrieved from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9125932.

Law of Ukraine No. 2297-VI “Law on the Protection of Personal Data”. (2012, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text. [in Ukrainian]

Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunication Systems" (2023). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-vr#Text. [in Ukrainian]

Lee, H. (1995). Justifying database normalization: a cost/benefit model. *Information Processing & Management*, Volume 31, Issue 1, Pages 59-67. Retrieved from https://www.sciencedirect.com/science/article/pii/030645739580006F.

Moodle - *Learning Management System*. Accessed: Jul. 1, 2024. Retrieved from https://moodle.org/.

Open Campus Whitepaper: Overview (n.d.). *User documentation*. Retrieved from https://userdocs.opencampus.xyz/.

Panagiotidis, P. (2022). Blockchain in education: The case of language learning. *European Journal of Education, 5*(1), 66. doi: 10.26417/443gjm83.

Resolution of the Cabinet of Ministers of Ukraine No. 1109 "Some Issues of Critical Infrastructure". (2020, October 9; amended January 16, 2024). Retrieved from https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF. [in Ukrainian]

Smart contract. (2024). *Etherscan*. Retrieved from https://goerli.etherscan.io/address/0xfa3db68927ade71daae8f1b78b51b369d6d23aad.

Sony Global Education. Accessed: Jul. 1, 2024. Retrieved from https://www.sony.com/en/SonyInfo/News/Press/201602/16-0222E/.

Steiu, M.-F. (2020). Blockchain in education: Opportunities, applications, and challenges. *First Monday, 25*(9). doi:10.5210/fm.v25i9.10654.

Storj Lab Inc (2024). Storj: A Decentralized Cloud Storage Network Framework v.3.1. 90 p. Retrieved from https://www.storj.io/storjv3.pdf.

Taherdoost, H. (2023). Smart Contracts in Blockchain Technology: A Critical Review. *Information 14, 117.* Retrieved from https://doi.org/10.3390/info14020117

Wood, G. (2024). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Shanghai Version. Retrieved from https://ethereum.github.io/yellowpaper/paper.pdf

Yakovenko A., Solana Foundation. Solana: A new architecture for a high performance blockchain. Accessed: Jul. 1, 2024. Retrieved from https://solana.com/solana-whitepaper.pdf.