УДК 004.056 + 004.658

Ю. В. Баришев, к. т. н., доц.; В. С. Ланова

МЕТОД ЗАХИЩЕНОГО ЗБЕРІГАННЯ МЕДИЧНИХ ДАНИХ НА ОСНОВІ РЕЛЯЦІЙНОЇ БАЗИ ДАНИХ ТА БЛОКЧЕЙНУ

В статті проведено аналіз відомих практик використання технології блокчейн в галузі охорони здоров'я. Розглянуто структури організації зберігання даних. Визначено задачі, які виникають при застосуванні технології блокчейн для зберігання конфіденційної інформації в критичних системах таких, як медицина. Наведено аналіз системи створення електронних направлень, яка використовується в Україні. Запропоновано метод зберігання медичних даних, який будується на основі використання гібридного середовища зберігання даних на основі блокчейну та реляційної бази даних. В основі методу покладено класифікацію даних відповідно до вимог щодо захисту властивостей інформації, відображенням якої є ці дані, для визначення способу їх зберігання. Для доведення застосовності методу наведено приклад його реалізації для задач в галузі сімейної медицини, а саме процесу видавання електронних направлень на додаткові обстеження спеціалістами. Наведено результати проєктування реляційної бази даних для цієї предметної області, в межах якого визначено основні сутності та атрибути цієї бази даних. Проведено аналіз вимог до безпеки цих даних, на основі якого здійснено їх класифікацію відповідно до запропонованого методу. Для можливості зберігання даних в блокчейні розроблено відповідний смарт-контракт, який забезпечує інтерфейс доступу до даних, що потребують підвищеного захисту цілісності, доступності та комбінації цих властивостей. Розроблено програмний модуль для об'єднання реляційної бази даних та блокчейну таким чином, щоб для клієнтських програм дані відображались інкапсульовано, незалежно від фактичного місця їх зберігання. Запропоновано механізм підвищення захисту цілісності даних в реляційній базі даних за рахунок їх верифікації в блокчейні, без розкриття вмісту цих даних. Визначено перспективи подальших досліджень.

Ключові слова: *кібербезпека, база даних, блокчейн, медична таємниця, персональні дані, сімейний лікар, смарт-контракт, критичні системи.*

Вступ

Потреба у захисті медичних даних очевидна: відповідно до законодавства вони належать до лікарської таємниці [1] та персональних даних [2 – 3]. Водночас ці дані можуть бути використані під час розслідуванні інцидентів, тому їх цілісність та доступність критична для успіху розслідування як помилок чи халатності лікарів, так і їх захисту від безпідставних звинувачень з боку пацієнтів чи державних органів. При цьому останнє вимагає прозорості медичних даних, що суперечить першому. Відповідно розв'язання задачі захисту медичних даних передбачає використання спеціальних методів їх зберігання та обробки, а також спеціальних структур даних, які дозволятимуть це здійснювати.

Можливим розв'язком цієї задачі може стати технологія блокчейн. Ця технологія пропонує нові підходи до моделей зберігання та управління даних, які застосовуються сьогодні в багатьох програмах охорони здоров'я. Це пов'язано зі здатністю сегментувати та захищати цілісність та доступність інформації. Водночас відкритість блокчейну для доступу породжує проблеми при захисті конфіденційності. Крім того використання лише технології блокчейн для зберігання даних вимагає більших ресурсів для створення та підтримки зберігання одиниці обсягу інформації порівняно з традиційними базами даних. Тому постає актуальна задача розробки методу зберігання, який дозволить поєднати переваги цих технологій для критичних систем таких як охорона здоров'я.

Метою цього дослідження є покращення захисту медичних даних шляхом розробки методу їх розподіленого зберігання на основі реляційної бази даних та блокчейну, що підтримує смарт-контракти.

Для того, щоб досягти поставленої мети, потрібно розв'язати такі задачі:

– виконати аналіз відомих методів застосування технології блокчейн для зберігання меди-

чних даних;

– розробити метод організації захищеного зберігання даних;

– проаналізувати предметну область;

– розробити модель даних;

– розробити смарт-контракти, які будуть зберігати дані в блокчейн.

У цій статті для доведення концепції обрано відомості, які обробляються під час процесу видачі пацієнтам направлень на додаткове обстеження сімейними лікарями.

Аналіз відомих методів застосування технології блокчейн для медичних даних

Природним станом для даних, які зберігаються в блокчейні є їх відкритість. Це обумовлюється розподіленістю технології та постійним обміном цією інформацією між вузлами. Тому ведуться дослідження в напрямку захисту конфіденційності даних. Зокрема в роботі [4] розглянуто механізм захисту приватності для розподілу даних між пацієнтами, лікарями і постачальниками медичних послуг. Запропонований авторами [4] підхід передбачає використання псевдонімів під час обміну даними для захисту приватності пацієнтів. Також цей метод враховує особливості медичної системи та законодавства Швеції, зокрема керування ухваленням рішень щодо обсягу даних, що ускладнює впровадження запропонованих методик отримання доступу в умовах законодавчої бази інших країн.

Широке поширення технології блокчейн в медицині відбулось в Естонії [5]. Так кожен громадянин цієї країни, який відвідав лікаря, має онлайн-запис в системі E-Health, який можуть відстежувати всі державні медичні установи [5]. Використання в системі технології блокчейн забезпечує цілісність даних і пом'якшує внутрішні загрози для даних. Однак, недоліком варто зазначити те, що для запису всіх даних потрібно багато ресурсів: необхідно виконати велику кількість транзакцій, що спричинить витрати обчислювальних ресурсів.

Автори [6] пропонують підхід до використання блокчейну для додавання медичних даних. Після того, як пацієнт звертається до лікарні, лікар ставить діагноз і створює медичну картку. Лікарю необхідно зберегти записи, щоб пацієнт в будь-який момент міг повернутись до своїх даних, а лікар міг дізнатись подробиці. Оскільки медичні записи, пов'язані з персональними даними пацієнта, тому перед збереженням передбачається їх шифрування. Лікар шифрує та підписує медичну документацію потім завантажує її в систему IPFS [7] для зберігання та генерує індекси для ключових слів. IPFS повертає геш-адресу збереженого файлу лікареві. Після, отримавши геш-адреси, лікар шифрує і гешує медичну документацію та її індекс за допомогою SHA-256, а потім зберігає геш-значення і зашифровану геш-адресу в блокчейні [6].

У джерелі [8] представлена архітектура системи контролю доступу до медичних даних, що зберігаються в блокчейні, на основі рольової моделі розмежування прав доступу. Зокрема в роботі передбачається державне регулювання щодо політики розмежування прав доступу та система зворотного зв'язку від пацієнтів та адміністраторів інформаційних систем (рис. 1).

Недоліком підходу, запропонованого в [8] є його зосередженість щодо зберігання даних виключно на блокчейні, що сповільнює швидкість доступу до даних. Крім того, відсутність захисту даних, інтегрованого безпосередньо в блокчейн, спричиняє підвищення впливу людського фактору на процес розмежування прав доступу.

Автори роботи [9] пропонують підхід до розв'язання задачі зберігання медичних даних в блокчейні на основі використання моделі розмежування прав доступу ABAC та шифрування даних. Основною перевагою цього підходу є застосування шифрування для захисту конфіденційності, але водночас шифрування ускладнює процедуру ключового транспорту. З урахуванням великої кількості залучених сторін (пацієнти, лікарі, органи державного регулювання, науковці-дослідники тощо) задача розподілу ключів поміж великою кількістю сторін породжує додаткові задачі, які вимагають подальших досліджень.

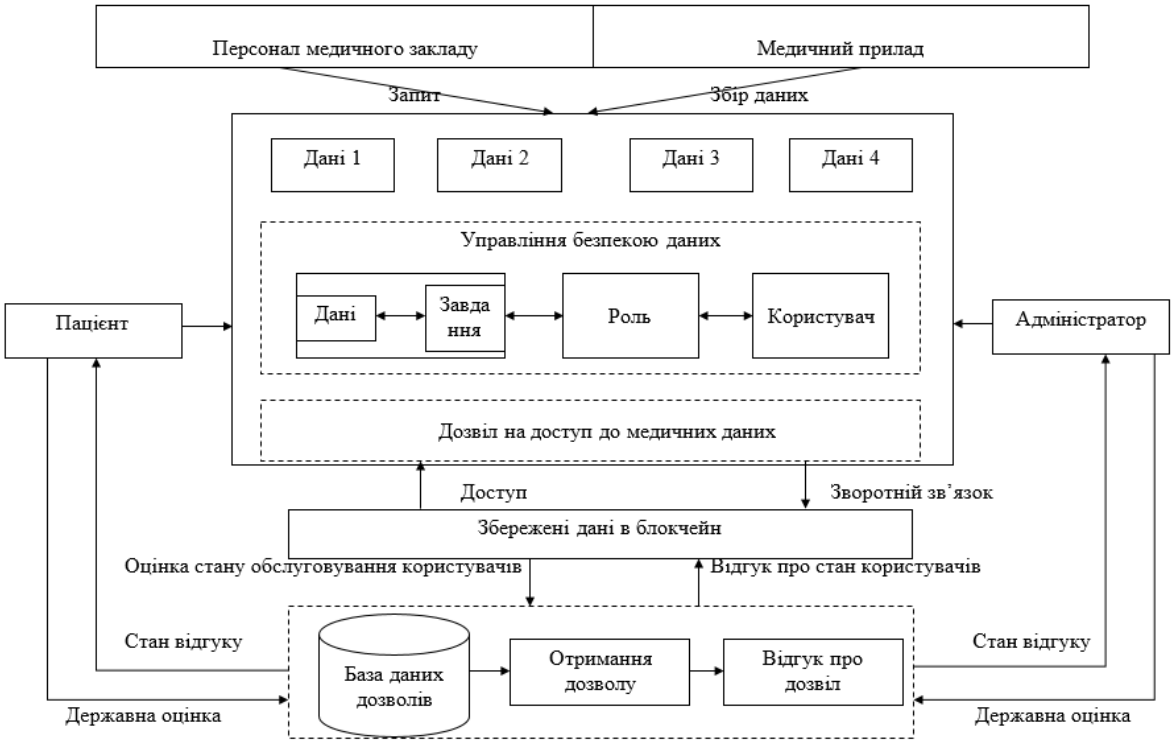

Рис.1. Архітектура системи контролю доступу до медичних даних на основі блокчейну

Робота [10] базується на розгортанні приватного блокчейну на основі кодової бази блокчейну Ethereum. Оскільки основною одиницею структурування даних в Ethereum є смарт-контракти, тому вони використовуються для зберігання відомостей електронної медичної карти пацієнта, яка містить персональні дані. При їх обробці необхідно враховувати безпеку. З цією метою автори розробили модель для обміну медичними даними між пацієнтами, лікарнями та будь-якою іншою організацією, яка бере участь у цьому процесі. Використовувані смарт-контракти забезпечують конфіденційність електронних медичних карт пацієнтів за допомогою криптографічних функцій і функцій контролю доступу. Застосування приватного блокчейну обмежує захист доступності даних, які в ньому зберігаються. При цьому в сфері медицини доступність інформації критична, наприклад, у випадках ургентної медицини.

В роботі [11] розглядається побудова блокчейну для зберігання медичних даних на основі смарт-контрактів та шардингу. Для захисту даних автори [11] пропонують технологію зашумлення даних та розробку смарт-контрактів, які керуватимуть процесом обробки даних. Відповідно системи в медичних закладах та клієнтські засоби будуть взаємодіяти зі смарт-контрактами для зміни стану блокчейну. Недоліком зашумлення даних є збільшення множини даних, які потрібно зберігати в блокчейні, для якого і так є загальним недоліком високій ступінь резервного копіювання даних.

Медична система України перебуває в процесі реформування та модернізації. Наказом МОЗ України від 9 червня 2017 р. № 17 затверджено Регламент функціонування електронної системи охорони здоров'я в рамках реалізації пілотного проєкту в частині забезпечення автоматизації обліку надання медичних послуг [12]. Одним з ключових напрямків є впровадження електронної системи охорони здоров'я eHealth, метою якої є підвищення ефективності та прозорості медичного обслуговування громадян.

Електронна система охорони здоров'я (ЕСОЗ) – двокомпонентна система, в якій користувач через медичну інформаційну систему взаємодіє з центральною базою даних [13].

ЕСОЗ складається з таких елементів [13]:

– центральної бази даних інформаційно-телекомунікаційної системи, яка містить реєстри,

програмні модулі, інформаційну систему Національної служби здоров'я України тощо;

– електронна медична інформаційна система — інформаційно-телекомунікаційна система, яка дає змогу автоматизувати роботу суб'єктів господарювання у сфері охорони здоров'я, створювати, переглядати, обмінюватися інформацією в електронній формі, зокрема з центральною базою даних.

Право доступу до персональних даних пацієнта в сфері охорони здоров'я мають: медичні працівники або інші особи закладу охорони здоров'я; фізичні особи-підприємці, які займаються медичною практикою на підставі ліцензії; особи, на яких поширюється дія законодавства про медичну таємницю; працівники центрального органу виконавчої влади, що реалізують державну політику в сфері державних фінансових гарантій медичного обслуговування населення [14]. Такий широкий спектр залучених осіб ускладнює задачу управління розмежуванням доступу, оскільки потребує визначення прав доступу для кожної зі сторін. Крім того наявність центральної бази даних породжує єдину точку відмови всієї системи, що породжує низку загроз цілісності та доступності інформації.

Таким чином, аналіз свідчить про потребу використання гібридизації блокчейну з іншими технологіями зберігання даних. Оскільки в критичних системах таких, як медицина, кількість користувачів та обсяги даних, які потребують обробки вимагають від інформаційних систем можливості масштабування. Водночас блокчейн за своєю природою є негнучким, а тому не може вважатись адекватним інструментом для зберігання всіх даних в таких задачах.

Метод організації захищеного зберігання даних

Як було показано в попередньому розділі – сучасний стан розробки методів для зберігання медичних даних у блокчейні неадаптований до реалій медичної практики та документообігу України. У зв'язку з тим, що наразі вже використовується система електронного документообігу запропоноване рішення повинно враховувати можливість поступового переходу до використання блокчейну. Крім того, властивість відкритості та низького рівня масштабованості блокчейну обумовлює разом із підвищеною захищеністю цілісності, втрату конфіденційності даних у випадку, якщо вони будуть опубліковані у відкритому вигляді. Саме тому пропонується метод до зберігання медичних даних, який базується на поєднання традиційних реляційних баз даних, які використовуються у поточній практиці, з блокчейном.

Метод, що пропонується передбачає такі кроки:

Крок 1. Аналіз предметної області, збір релевантних даних та їх подальша формалізація у вигляді атрибутів бази даних.

Крок 2. Нормалізація відношень бази даних.

Крок 3. Аналіз вимог до кожного з атрибутів в отриманій нормалізованій базі даних з точки зору конфіденційності та цілісності. Внаслідок виконання аналізу відбувається розбиття всіх даних на такі класи:

– дані, що не потребують підвищеного захисту;

– дані, що потребують підвищеного захисту цілісності (Ц);

– дані, що потребують підвищеного захисту доступності (Д);

– дані, що потребують підвищеного захисту конфіденційності (К);

– дані, що потребують підвищеного захисту декількох властивостей водночас (ЦД, КЦ, КД, КЦД).

Крок 4. Розробка смарт-контрактів для перенесення даних категорій Ц, Д та ЦД до блокчейну без внесення модифікації у них.

Крок 5. Розробка контейнерів захищеного зберігання даних категорії КЦ на основі методів виявлення та виправлення помилок.

Крок 6. Розробка контейнерів захищеного зберігання даних КД на основі методів шифрування.

Крок 7. Розробка контейнерів захищеного зберігання даних КЦД на основі методів шиф-

рування та виявлення і виправлення помилок.

Крок 8. Внесення до реляційної бази даних нових атрибутів з відомостями про посилання на смарт-контракти, до яких було перенесено дані.

Запропонований метод дозволяє розподілити дані поміж базою даних та блокчейном, використовуючи блокчейн виключно для захисту тих даних, які потребують підвищеного захисту цілісності та доступності. На відміну від відомих методів, зокрема, що були розглянуті в попередньому розділі статті, цей метод дозволяє одночасний доступ великої кількості різноманітних залучених сторін, як це притаманно сфері медицини. При цьому складність задачі управління розмежуванням прав доступу зменшиться через виділення саме тих даних, які потребують обмеження доступу, та їх зберігання в окремих контейнерах.

Застосування методу для медичних даних

Для доведення концепції предметною областю обрано сімейну медицину, а саме процес видавання направлень на додаткові обстеження в лікарні. Впровадження блокчейну може забезпечити високий рівень захисту даних пацієнтів, забезпечити автентичність та недопустимість змін до внесених записів, а також сприяти забезпеченню прозорості та відстежуваності медичних послуг. Такий підхід сприятиме покращенню ефективності управління медичними процесами в сфері сімейної медицини.

На основі виконаного аналізу предметної області було виділено основні сутності бази даних та їх атрибути. Для подальшого дослідження було взято реальне направлення до лікаря отоларинголога, видане 10.08.2022 у ЦПМСД №2 м. Вінниці, яке містить:

– № направлення – унікальний ідентифікатор направлення;
– спеціаліст – лікар, який створив направлення;
– назва обстеження – найменування обстеження чи процедури;
– ПІБ пацієнта – повне ім'я пацієнта;
– попередній діагноз – попередній медичний діагноз пацієнта;
– дата виписування направлення – дата, коли було створено направлення;
– пріоритет – ступінь важливості або терміновості обстеження;
– термін дії – термін, протягом якого направлення є дійсним;
– № медичної картки пацієнта – унікальний ідентифікатор медичної картки пацієнта;
– код послуги – уніфікований код для обстеження чи процедури;
– № паспорта лікаря – унікальний ідентифікатор лікаря, який створив направлення;
– найменування закладу охорони здоров'я – назва лікарні або медичного закладу;
– код за ЄДРПОУ/РНОКПП – ідентифікаційний код закладу охорони здоров'я відповідно до реєстрів.

Ці атрибути утворюють комплексну систему відстеження і контролю за наданням медичних послуг у сфері сімейної медицини в лікарні. Відповідно до попередньо виділених атрибутів, виконано аналіз наведених даних. Результати аналізу наведено в таблиці 1.

Таблиця 1

Аналіз наведених атрибутів

Атрибут	Захист конфіденційності	Захист цілісності	Захист доступності
№ направлення	-	+	+
Спеціаліст, до якого виписане направлення	+	+	+
Назва обстеження	+	+	+
ПІБ пацієнта	+	-	-
Попередній діагноз	+	-	-
Дата виписування направлення	-	-	-
Пріоритет	-	-	+
Термін придатності	-	-	+
№ медичної картки пацієнта	+	+	-
Код послуги	-	-	-
№ паспорта лікаря	+	+	-
Найменування закладу охорони здоров'я	-	+	-
Код за ЄДРПОУ/РНОКПП	-	-	+

Для цієї предметної області розроблено базу даних під назвою MedicalData. Основною таблицею бази даних є _MedicalRecords, що містить такі поля:

– patientName,
– previousDiagnosis,
– patientMedicalID,
– doctorPassport.

Поля зберігають в собі ПІБ пацієнта, діагноз, ідентифікаційний номер пацієнта (або № медичної картки) та № паспорту лікаря відповідно.

Ця таблиця створена з урахуванням вимог конфіденційності медичних даних та легкості доступу для медичного персоналу. Для її реалізації було розроблено запит (рис. 2).

```
USE MedicalData;
CREATE TABLE _MedicalRecords (
patientName NVARCHAR(255) NOT NULL,
previousDiagnosis NVARCHAR(255) NOT NULL,
patientMedicalID int NOT NULL,
doctorPassport CHAR(9) NOT NULL
);
```

Рис. 2. Запит для створення таблиці

Кожне з чотирьох полів таблиці є обов'язковим і не може бути порожнім. Це дозволяє уникнути неповних або некоректних записів. Такий обов'язковий характер полів таблиці MedicalRecords виключає можливість додавання неповних або некоректних записів у базу даних, забезпечуючи підвищення рівня їх захисту.

Окрім бази даних розроблено смарт-контракт, який є основою для зберігання даних, що потребують підвищеного рівня захисту цілісності та доступності інформації. Для реалізації смарт-контракту використано мову Solidity. Для розмежування доступу до даних з різними вимогами щодо захисту було розроблено окремі групи функції, які дозволяють читати і додавати такі дані категрій Ц, Д та ЦД. Для взаємодії з останньою групою функцій розроблено додаткову перевірку цілісності даних. Для цього використовується геш-функція keccak256,

яка природно підтримується блокчейнами сімейства Ethereum. Отримані геш-значення записуються до блокчейну, що дозволяє підвищити їх захист від підробки. В подальшому передбачається порівняння цих геш-значень із обчисленими геш-значеннями даних, які зберігаються в базі даних, що дозволяє виявити випадки несанкціонованої модифікації бази даних (рис. 3).

```
function verifyIntegrityData(
    string memory _patientName,
    string memory _previousDiagnosis,
    string memory _patientMedicalID,
    string memory _doctorPassport
) public view returns (bool) {
    IntegrityData memory data = integrityData[msg.sender];
    bytes32 expectedHash = keccak256(abi.encodePacked(
        _patientName,
        _previousDiagnosis,
        _patientMedicalID,
        _doctorPassport
    ));
    return keccak256(abi.encodePacked(
        data.patientName,
        data.previousDiagnosis,
        data.patientMedicalID,
        data.doctorPassport
    )) == expectedHash;
}
```

Рис. 3. Фрагмент коду виявлення несанкціонованої модифікації бази даних

Розроблений смарт-контракт розгорнуто в Ethereum-подібній мережі за допомогою середовища Ganache (рис. 4).

NAME	ADDRESS	TX COUNT	
MedicalData	0×18cbDa66Ac8Fce434232a4A70514b3Dc03eAFAa9	0	DEPLOYED

Рис. 4. Результат розгортання смарт-контракту

Наступною задачею є розробка програмного забезпечення, яке дозволить одночасно взаємодіяти із даними, які зберігаються в базі даних та в блокчейні, як з єдиним джерелом даних.

Приєднання бази даних до блокчейну

Для розробки програми інтеграції бази даних та блокчейну було використано бібліотеку ethers.js. Розроблено програмний модуль, який виконує приєднання бази даних до смарт-контракту. Для цього спочатку було виконано приєднання бази даних до програмного застосунку в середовищі node.js. Для цього виконано конфігурацію з'єднання, наведену на рис. 5.

```
var config = {
  database: 'MedicalData',
  server: 'DESKTOP-CSFCFTG\\SQLEXPRESS',
  driver: 'msnodesqlv8',
  options: {
      trustedConnection: true
  }
};
```

Рис. 5. Конфігураційний файл приєднання бази даних SQLServer

Інтеграція бази даних до розгорнутого смарт-контракту під час додавання даних виконується так:

– отримується адреса контракту;

– формується SQL-запит в середовищі node.js, який виконує запис до бази даних;

– відбувається запис до блокчейну.

Далі після успішного запуску та приєднання, можна побачити дані додані і в блокчейн, і в базу даних (рис. 6 – 7).

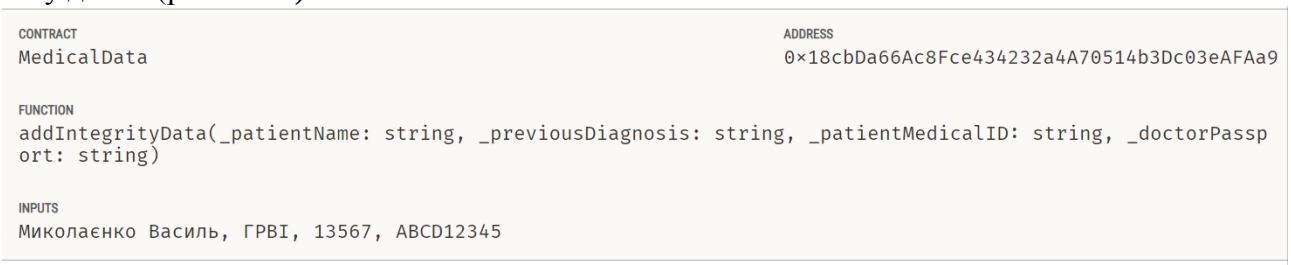

Рис. 6. Відображення успішного додавання даних в блокчейн

	patientName	previousDiagnosis	patientMedicalID	doctorPassport
1	Ланова Владислава	Астигматизм	12345	ABCD12345
2	Лановий Богдан	Бронхіт	23456	ABCD12345
3	Миколаєнко Василь	ГРВІ	13567	ABCD12345

Рис. 7. Відображення успішного додавання записів до бази даних

Читання інформації, відбувається за аналогічним принципом. При цьому під час читання даних з блокчейну не потрібно виконувати транзакції, що обумовлює більшу швидкість реалізації читання порівняно із записом.

Висновки

Аналіз відомих практик застосування блокчейну в медицині в різних країнах показав складність інтеграції цих методів в медичній сфері інших країн через відмінності законодавчих норм, що регулюють правила документообігу. Крім того, для сфери медицини важливо забезпечувати простоту архітектури та управління складністю розробки. Тому авторами було запропоновано метод, який дозволяє виконувати класифікацію даних відповідно до вимог щодо захисту конфіденційності, цілісності та доступності. Це дозволило створити різні контейнери (база даних або смарт-контракти) щодо яких застосовуються різні методи захисту залежно від властивостей інформації, для якої призначено відповідний контейнер. Таким чином, всі дані предметної області, які мають однакові вимоги до захисту інформації зберігаються в межах одного контейнеру. На відміну від відомих підходів, це дозволило не застосовувати методи захисту інформації до тих даних, які цього не потребують. Це сприяє більш ефективному розподілу обчислювальних ресурсів, а тому покращує масштабованість інформаційної системи на основі такого методу зберігання даних. Останнє особливо актуально для критичних систем таких, як медичні, оскільки цим системам притаманне тривале зберігання даних, а отже збільшення кількості цих даних разом зі збільшенням тривалості використання інформаційних систем для автоматизації бізнес-процесів в цих галузях.

Для доведення застосовності запропонованого методу наведено приклад його реалізації в галузі медичної практики сімейних лікарів, а саме реєстрації направлень на додаткові обстеження. Запропоновано механізм підвищення захисту цілісності бази даних за рахунок їх верифікації в блокчейні без розкриття вмісту цих даних.

СПИСОК ЛІТЕРАТУРИ

1. Закон України Основи законодавства України про охорону здоров'я [Електронний ресурс] : Закон від 19.11.1992 № 2801-XII: станом на 24 вер. 2023 р. (чинний) – Режим доступу: https://zakon.rada.gov.ua/laws/show/2801-12 (дата звернення: 24.09.2023). – Назва з екрана.

2. General Data Protection Regulation (GDPR) – Official Legal Text [Electronic resource] // General Data Protection Regulation (GDPR). – Mode of access: https://gdpr-info.eu/ (date of access: 04.09.2023).

3. Закон України Про захист персональних даних [Електронний ресурс] : Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481: станом на 24 вер. 2023 р. (чинний) – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 24.09.2023).

4. Accessing and sharing health information for post-discharge stroke care through a national health information exchange platform - a case study [Electronic resource] / N. Davoody, S. Koch, I. Krakau, M. Hägglund // BMC Medical Informatics and Decision Making. – 2019. – Vol. 19, № 95. – Mode of access: https://doi.org/10.1186/s12911-019-0816-x (date of access: 25.09.2023).

5. e-Health Record – e-Estonia [Electronic resource]. – Mode of access: https://e-estonia.com/solutions/healthcare/e-health-records/(date of access: 27.09.2023).

6. Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS [Electronic resource] / J. Sun, X. Yao, S. Wang [et al] // IEEE Access. – 2020. – Vol. 8. – P. 59389 – 59401. – Mode of access: https://doi.org/10.1109/access.2020.2982964 (date of access: 25.09.2023).

7. Design and Evaluation of IPFS: A Storage Layer for the Decentralized Web [Electronic resource] / D. Trautwein, A. Raman, G. Tyson [et al] – Mode of access: https://doi.org/10.1145/3544216.3544232 (date of access: 25.09.2023).

8. Data Access Control Based on Blockchain in Medical Cyber Physical Systems [Electronic resource] / F. Chen, J. Huang, C. Wang [et al] // Security and Communication Networks – Mode of access: https://doi.org/10.1155/2021/3395537 (date of access: 25.09.2023).

9. A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection [Electronic resource] / Y. Chen, L. Meng, H. Zhou [et al] // Wireless Communications and Mobile Computing. – 2021. – Vol. 2021. – P. 1 – 12. – Mode of access: https://doi.org/10.1155/2021/6685762 (date of access: 20.09.2023).

10. A Smart Contract Based Access Control Framework for Cloud Smart Healthcare System [Electronic resource] / A. Saini, Z. Qingyi, Y. Xiang // IEEE Internet of Things Journal. – 2020. – P. 1. – Mode of access: https://doi.org/10.1109/jiot.2020.3032997 (date of access: 25.09.2023).

11. Artificial Neural Network Blockchain Techniques for Healthcare System: Focusing on the Personal Health Records [Electronic resource] / Seong-Kyu Kim, Jun-Ho Huh // Electronics. – 2020. – Vol. 9, № 5. – P. 763. – Mode of access: https://doi.org/10.3390/electronics9050763 (date of access: 25.09.2023).

12. Регламент функціонування електронної системи охорони здоров'я в рамках реалізації пілотного проєкту в частині забезпечення автоматизації обліку надання медичних послуг [Електронний ресурс] : наказ Міністерства охорони здоров'я України від 09.06.2017 р. Режим доступу : https://www.apteka.ua/article/415112 (дата звернення: 25.09.2023).

13. Електронна система охорони здоров'я [Електронний ресурс]. – Режим доступу: https://ehealth.gov.ua/ (дата звернення: 25.09.2023).

14. Електронна система охорони здоров'я (e-Health): механізм упровадження та етапи розвитку [Електронний ресурс] / Н. В. Коробцова // Проблеми законності. – 2021. – Вип. 154. – С. 117 – 126. – Режим доступу : https://doi.org/10.21564/2414-990X.154.236921 (дата звернення: 25.09.2023).

Стаття надійшла до редакції 22.09.2023.
Стаття пройшла рецензування 28.09.2023.

Баришев Юрій Володимирович – к. т. н., доцент кафедри захисту інформації.

Ланова Владислава Сергіївна – студентка кафедри захисту інформації.
Вінницький національний технічний університет.