Протокол розподіленого зберігання медичних даних

УДК 004.056

Микита Ціхоцький

Вінницький національний технічний університет, nik.tsikhotskiy15@gmail.com

Медичні інформаційні системи працюють з даними, для яких критичними є конфіденційність, цілісність, контрольований доступ і можливість відновлення. У розгалужених інфраструктурах зберігання повної копії медичного файлу на одному вузлі створює окрему точку компрометації, оскільки несанкціонований доступ до такого вузла може призвести до отримання всього об'єкта зберігання [1].

Метою роботи є розробка протоколу захищеного розподіленого зберігання медичних даних, який поєднує попереднє зашифрування файлу, пороговий розподіл зашифрованого вектору на частки та перевірку цілісності перед відновленням. Наукова новизна полягає у використанні порогової (*k*,*n*)-схеми з перекриттям блоків для контрольованого зберігання зашифрованого медичного файлу, за якого службові дані та контрольна частка залишаються у суб'єкта, що має право на відновлення.

У межах протоколу вхідний медичний файл F подається як послідовність байтів. У протоколі беруть участь уповноважений суб'єкт *M* та множина учасників зберігання $\mathbf{P} = \{P_1, P_2, \ldots, P_n\}$. Суб'єкт *M* готує файл до розподіленого зберігання, зберігає службові дані та має право на відновлення. Учасники P_i виконують роль вузлів, у яких розміщуються окремі частки розподіленого набору.

На першому етапі суб'єкт *M* виконує зашифрування файлу з використанням секретного ключа *K*: $\mathbf{C} = Enc_K(\mathbf{F})$, де C - зашифрований вектор медичного файлу [2]. Зашифрування виконується до розподілу, оскільки учасники зберігання не повинні працювати з відкритим медичним вмістом. У подальшій процедурі між вузлами розміщується не початковий файл, а частки його зашифрованого вектору.

Після зашифрування до вектору C застосовується порогова (*k*,*n*)-схема розподілу з перекриттям блоків [3]: $Share_{k,n}(\mathbf{C}) = \{\mathbf{S}, \mathbf{Q}, S_D, \mathbf{MB}\}$, де $\mathbf{S} = \{S_1, S_2, \ldots, S_n\}$ - множина часток, $\mathbf{Q} = \{Q_1, Q_2, \ldots, Q_n\}$ - множина порядкових номерів часток, S_D - частка, що зберігається у суб'єкта *M* та використовується під час відновлення, MB - службові дані розподіленого набору. Параметр *n* визначає загальну кількість сформованих часток, а параметр *k* - мінімальну кількість коректних часток, необхідну для відновлення зашифрованого вектору.

Для кожного учасника формується запис зберігання $\mathbf{R}_i = \{ID, q_i, \mathbf{S}_i\}$, де *ID* визначає належність частки до конкретного розподіленого медичного файлу, q_i задає її порядковий номер, а $\mathbf{S}_i$ є самою часткою. Розміщення часток у вузлах зберігання подається як $P_i \leftarrow \mathbf{R}_i, \quad i = 1, 2, \ldots, n$. Учасникам передаються лише

дані, необхідні для зберігання відповідної частки; ключ розшифрування, частка S_D і службові дані залишаються у суб'єкта *M*.

Службові дані MB формуються на етапі розподілу та містять ідентифікатор розподіленого набору *ID*, параметри *k* і *n*, таблицю відповідності між номерами часток і вузлами зберігання I_{SQ}, а також геш-значення часток і частки S_D. Таблиця I_{SQ} потрібна для перевірки відповідності отриманої частки очікуваному номеру та вузлу зберігання. Геш-значення фіксують стан часток у момент формування набору, тому під час відновлення дозволяють виявити пошкодження або підміну даних до їх об'єднання: $h_i = Hash(S_i)$, $h_D = Hash(S_D)$. Для відновлення суб'єкт *M* за ідентифікатором *ID* визначає потрібний розподілений набір і звертається до учасників зберігання. Отримані записи перевіряються за службовими даними: спочатку встановлюється відповідність *ID*, q_i та I_{SQ}, після чого перевіряється збіг геш-значень. До відновлення допускаються лише ті частки, для яких підтверджено належність до відповідного набору та цілісність. Після перевірки формується множина коректних часток $\mathbf{S}_{кор}$, і відновлення виконується лише за умови $\left|\mathbf{S}_{кор}\right| \geq k$.

Якщо порогова умова виконується, суб'єкт M відновлює зашифрований вектор з використанням множини коректних часток, частки S_D та службових даних [3]: $\mathbf{C} = \mathrm{Re}c_{k,n}(\mathbf{S}_{кор}, S_D, \mathbf{MB})$. Після цього виконується розшифрування зашифрованого вектору з використанням секретного ключа *K*: $F = Dec_K(\mathbf{C})$. У результаті відновлюється початковий медичний файл.

Запропонований протокол забезпечує зберігання медичного файлу без розміщення його повної копії на одному вузлі. Попереднє зашифрування обмежує доступ учасників зберігання до відкритого вмісту, порогова (*k*,*n*)-схема дозволяє відновити файл за наявності не менше ніж k коректних часток, а службові дані та частка S_D забезпечують контроль процедури відновлення. Використання порядкових номерів, таблиці відповідності та геш-значень дозволяє перевіряти належність і цілісність часток до запуску відновлення, що зменшує ризик використання пошкоджених або підмінених даних.

1. Лужецький В. Підходи до вирішення інструментальних завдань телемедицини. Матеріали III Всеукр. Медико-технічна наук.-практ. конф., м. Вінниця, 5–6 квіт. 2024 р. Вінниця: Едельвейс, 2024. С. 11–14.
2. Luzhetskyi V., Tsikhotskyi M. Image encryption and distribution method based on LFSR and counters. Information Technologies and Computer Engineering. 2025. Vol. 22, No. 3. P. 77-88.URL: https://doi.org/10.31649/vitce/3.2025.77 (дата звернення: 06.05.2026).
3. Лужецький В.А., Ціхоцький М.С. Розподіл секретного вмісту даних за (k,n)-схемою з використанням зашифрованих блоків. Вісник Вінницького політехнічного інституту. 2025. № 5. С. 113-120. URL: https://doi.org/10.31649/1997-9266-2025-182-5-113-120 (дата звернення: 08.05.2026).