УДК: 004.04

Васильченко Д. Н., здобувач вищої освіти
Загоруйко Л. В., канд. техн. наук, доцент,
доцент кафедри прикладної математики та кібербезпеки,
Донецький національний університет імені Василя Стуса

АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕДИЧНІЙ ХМАРНІЙ СИСТЕМІ E-HEALTH

Анотація. У роботі було проведено аналіз методів забезпечення захисту персональних даних у медичній хмарній системі e-Health, що пов'язано зі стрімким розвитком інформаційних технологій загалом, зміною форматів збереження і зростанням об'єму даних, та з процесами їх перетворень, редагувань тощо у контексті хмарних медичних даних.

Ключові слова: інформаційні технології, інформаційна система, e-Health, медичні інформаційні системи, протокол, секрет.

Вступ. В умовах швидкого впровадження цифрових технологій у різні сфери діяльності людини питання безпеки під час обробки та зберігання інформації стає критично важливим завданням. Особливо це стосується сфери охорони здоров'я, де використання медичних інформаційних систем (МІС) як частини електронної системи охорони здоров'я e-Health стає необхідністю.

Мета цього дослідження полягає в аналізі методів, що гарантують безпеку обробки, передачі та зберігання особистих даних (ОД) пацієнтів, які використовують МІС для зв'язку з центральною базою даних e-Health, побудованих на засадах розподіленої хмарної архітектури.

Основний текст. Для забезпечення безпеки обміну медичними файлами обстеження також можна використовувати схему Шаміра. Ця схема дає змогу створити (k, p) порогову систему обміну секретом, де тільки будь-які k чи більше сторін $(k \leq p)$ можуть відновити секрет. Це означає, що, наприклад, якщо встановлено поріг $k = 3$ і загальна кількість сторін $p = 5$, то будь-які три або більше сторін можуть відновити секрет, але будь-які менше ніж три сторони не матимуть достатньої інформації для розкриття секрету. Це дає змогу забезпечити конфіденційність медичної інформації шляхом обміну файлами між довіреними сторонами, забезпечуючи водночас високий рівень захисту навіть у випадку, якщо деякі ключі потраплять у руки несанкціонованих осіб (рис. 1, 2).

У вказаному підході абоненти, тобто користувачі, виступають у ролі серверів, які зберігають фрагменти секрету, що в цьому контексті є медичними файлами обстеження. Протокол розподілу секрету Шаміра – це криптографічний метод, призначений для розподілу секретної інформації серед кількох учасників так, що лише підмножина з них, відома як поріг, необхідна для відновлення секрету. У центрі протоколу знаходиться інтерполяція полінома над скінченними полями. Секрет представлений як сталий член полінома, водночас кожен учасник утримує частку, що відповідає точці на кривій полінома. Поліном будується так, що знання будь-якої підмножини меншої, ніж поріг, не надає жодної інформації про секрет. Отже, поєднуючи частки від достатньої кількості учасників,

можна відновити початковий секрет. Ця основна властивість протоколу розподілу секрету Шаміра забезпечує стійкість та безпеку під час розподілу конфіденційної інформації серед кількох сторін.

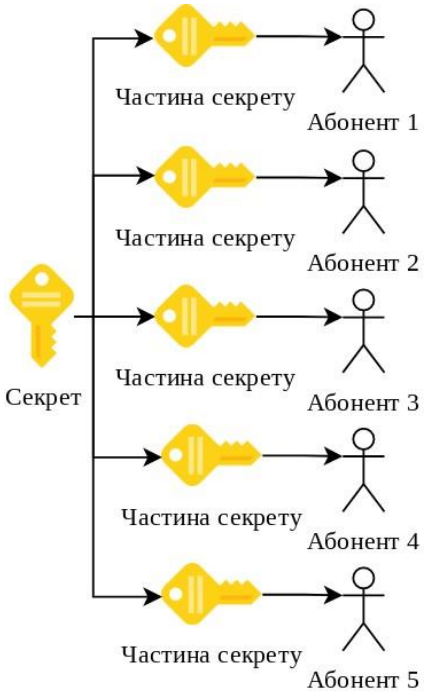

Рисунок 1 – Розділення секрету на частини за схемою Шаміра

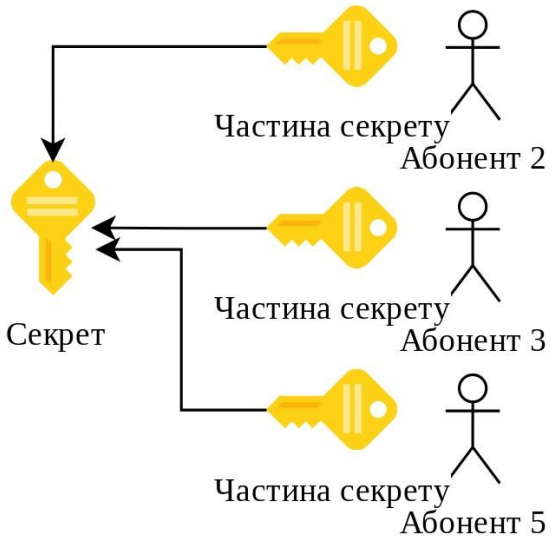

Рисунок 2 – Збирання частин секрету в один фрагмент за схемою Шаміра

З математичного погляду, поділ секрету виглядає так:

1. Ініціалізація:

a. Учасники домовляються про просте число p:

$$p \in P,$$
$$p > s,$$

де P – множина простих чисел.

s – секретний ключ (значення).

b. Кожен учасник незалежно вибирає випадкові коефіцієнти $a_1, a_2, \ldots, a_{t-1}$ з множини цілих чисел за модулем p:

$$a_i \in Z_p,$$
$$0 \leq i \leq t-1,$$

де Z_p – множина цілих чисел за модулем p;

t – поріг.

c. Обчислити поліном:

$$f(x) = s + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \text{ за модулем } p.$$

2. Розподіл:

Учасники обирають різні ненульові значення x для своїх часток та обчислюють відповідні значення y $(f(x))$ за допомогою узгодженого полінома.

3. Відновлення:

a. Учасники збирають принаймні t часток від інших.

b. Відновлення секрету s за допомогою інтерполяції Лагранжа:

$$s = \sum_{i=1}^{t} \left(y_i \cdot \prod_{j \neq i, j=1}^{t} \frac{x - x_j}{x_i - x_j} \right),$$

де (x_i, y_j) – це частки, зібрані від учасників [1–2].

Протокол розподілу секрету Асмута–Блума розподіляє секрет серед учасників, представляючи його як пару цілих чисел за модулем відмінних простих чисел. Використовуючи китайську теорему залишку, учасники обчислюють частки, що конгруентні секрету за модулем різних простих чисел. Ці частки розподіляються серед учасників, і будь-яка підмножина з необхідною кількістю часток може відновити секрет, використовуючи теорему. Цей підхід забезпечує надійний розподіл і відновлення секрету серед кількох сторін.

Опис протоколу з математичного погляду:

1. Ініціалізація:

a. Учасники кількістю n колективно узгоджують набір різних простих чисел $p_1, p_2, \ldots, p_n$, кожне з яких більше за секрет s:

$$p_1, p_2, \ldots, p_n,$$
$$p_i > s,$$
$$p_i \in P,$$

де P – множина простих чисел.

b. Використовуючи китайську теорему залишку, кожен учасник обчислює свої відповідні значення $u_1, u_2, \ldots, u_n$, такі, що:

$$u_i \equiv s \bmod p_i,$$

де u_i – частина секрету.

2. Розподіл:

a. Учасники розподіляють свої відкриті ключі (p_i, u_i) іншим для забезпечення секретного розподілу.

3. Відновлення:

a. Збираючи t або більше часток, учасники використовують китайську теорему залишку для відновлення секрету s:

$$s = \sum_{i=1}^{n} u_i \cdot \left(\prod_{j \neq i, j=1}^{n} p_j \right) \cdot \left(\prod_{j \neq i, j=1}^{n} (p_j)^{-1} \bmod p_i \right) \bmod,$$
$$P = p_1 \cdot p_2 \cdot \ldots \cdot p_i,$$
$$t \leq n,$$

де t – поріг кількості часток секрету для відновлення початкового секрету [3–4].

За допомогою протоколу розподілу секрету Карніна–Гріна–Хеллмана учасники можуть безпечно розділити конфіденційну інформацію шляхом генерації часток, які обмінюються між собою. Кожна частка обчислюється на основі випадкового числа, яке кожен учасник обирає незалежно, і загальних параметрів p та g.

Після розподілу часток учасники можуть використовувати зібрані частки для відновлення початкового секретного значення за допомогою визначеного методу відновлення. Цей протокол забезпечує безпечний та ефективний спосіб розподілу й відновлення секретної інформації між довіреними сторонами.

1. Ініціалізація:

a. Учасники колективно домовляються про просте число p та генератор g так, щоб $p > s > 0$, де s – секретне значення.

b. Кожен учасник незалежно вибирає випадкові числа $s_1, s_2, \ldots, s_t$ як їх частки.

c. Частки обчислюються за допомогою:

$$x_i \equiv g \ mod \ p_i.$$

2. Розподіл:

Учасники розподіляють свої частки x_i іншим учасникам.

3. Відновлення:

a. Збираючи принаймні t часток від учасників.

b. Використовується визначений метод відновлення для обчислення секретного значення s [5–6].

Висновки. Результатом виконання цієї роботи є аналіз методів забезпечення захисту персональних даних у медичній хмарній системі E-health у вигляді протоколів розподілу секретної інформації, а саме за схемами Шаміра, Асмута–Блума, Каріна–Гріна–Хеллмана.

Протокол розподілу секретів Шаміра з його методом поліноміальної інтерполяції надає надійний та ефективний спосіб розподілу секретів серед учасників, забезпечуючи те, що для відновлення оригінального секрету потрібна лише певна кількість часток.

Протокол розподілу секретів Асмута–Блума використовує китайську теорему залишку теореми для розподілу часток на основі різних простих чисел, що пропонує гнучкість і безпеку в розподілі секретів серед учасників.

Протокол розподілу секретів Карніна–Гріна–Хеллмана використовує модульні піднесення до степеня та генераторні елементи для ефективного розподілу й відновлення секретів серед учасників, забезпечуючи конфіденційність та цілісність.

Загалом ці протоколи являють собою важливі інструменти у галузі криптографії, надаючи універсальні та надійні методи розподілу й захисту чутливої інформації у різних застосуваннях та сценаріях. Розуміючи їх принципи та механізми, практики можуть приймати обґрунтовані рішення щодо вибору протоколу, що найкраще відповідає їх конкретним вимогам безпеки.

Наступним етапом досліджень буде визначення найефективнішого протоколу розподілу секретної інформації для системи e-Health через створений програмний модуль.

Список використаних джерел

1. Поділ секрету Шаміра. URL: https://exbase.io/uk/wiki/podil-sekretu-shamira (дата звернення: 22.10.2024).

2. Shamir’s Secret Sharing: Explanation and Visualization. URL: https://evervault.com/blog/shamir-secret-sharing (дата звернення: 22.10.2024).

3. On the asymptotic idealness of the Asmuth-Bloom threshold secret sharing scheme. URL: https://www.sciencedirect.com/science/article/abs/pii/S0020025518304869 (дата звернення: 22.10.2024).

4. Constructing Ideal Secret Sharing Schemes based on Chinese Remainder Theorem. URL: https://eprint.iacr.org/2018/837.pdf (дата звернення: 22.10.2024).

5. On Secret Sharing Systems. URL: https://www-ee.stanford.edu/~hellman/publications/45.pdf (дата звернення: 22.10.2024).

6. Revisiting the Karnin, Greene and Hellman Bounds. URL: https://www.win.tue.nl/~berry/papers/icits08kgh.pdf (дата звернення: 22.10.2024).