КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

УДК 004.056.55

УПРАВЛІННЯ ДОСТУПОМ ДО ПЕРСОНАЛЬНИХ ДАНИХ З ВИКОРИСТАННЯМ ДОВІРЕНОГО ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

А. Джоші
студент 6 курсу, група КНІТ-61м, навчально-науковий інститут автоматики, кібернетики та обчислювальної техніки
Науковий керівник – д.т.н., професор П. М. Мартинюк

Національний університет водного господарства та природокористування, м. Рівне, Україна

В статті наведено огляд протоколів довіреного цифрового підпису та розглянуто спосіб використання довіреного цифрового підпису на основі еліптичних кривих для управління доступом до персональних даних.
Ключові слова: довірений цифровий підпис, еліптичні криві, управління доступом, персональні дані.

В статье представлен обзор протоколов доверенной цифровой подписи и рассмотрен способ использования доверенной цифровой подписи на основе эллиптических кривых для управления доступом к персональным данным.
Ключевые слова: доверенная цифровая подпись, эллиптические кривые, управление доступом, персональные данные.

In the article review of proxy signature protocols has been done, using of elliptic curves proxy signature for access control of personal data is described.
Keywords: proxy signature, elliptic curves, access control, personal data.

Останнім часом питання збереження та управління персональними даними стало одним з найважливіших у сфері інформаційних технологій. У 2018 році Європейським Союзом було прийнято постанову щодо захисту персональних даних осіб в межах Європейського Союзу – загальний регламент про захист даних, основною метою якого є посилення та уніфікація захисту персональних даних [1]. Зважаючи на зовнішню орієнтованість, цей документ має безпосередній вплив і на український ринок надання послуг з розробки програмного забезпечення.

До ключових принципів регламенту про захист даних належать:

- цілісність та конфіденційність – при обробці даних необхідно забезпечити захист персональних даних від несанкціонованої чи незаконної обробки, знищення чи ушкодження;
- точність – неточні персональні дані мають бути видалені або виправлені;
- обмеження збереження – особисті дані повинні зберігатися у формі, що дозволить ідентифікувати суб'єкти даних на термін не більше ніж це необхідно для цілей обробки.

Однією з ключових проблем забезпечення конфіденційності даних є управління доступом до них. Вивчення методів та інструментів, здатних забезпечити надійне управління доступом до персональних даних та інформаційних ресурсів, в цілому є актуальною задачею в умовах підвищення вимог до обробки та збереження конфіденційної інформації.

В Україні широкий попит на методи і засоби захисту інформації почав виявлятися у другій половині 80-х років XX століття. З часом виникла нагальна потреба використання

криптографічних та технічних методів захисту і в приватному секторі. На теперішній час велика кількість конфіденційної інформації передається в електронному вигляді, на електронних носіях, в інформаційно-комунікаційних системах звичайними лініями зв'язку. Термін збереження секретності може коливатися від декількох годин до багатьох десятиліть. Тому знання криптографічних, технічних та комплексних методів захисту та їх застосовність у програмних та апаратних забезпеченнях є надзвичайно важливими для гарантування таємності та цілісності конфіденційної інформації. Криптографічні методи вважаються одними з найбільш надійних та ефективних для досягнення поставленої мети [2].

У 70-х роках минулого сторіччя було прийнято і опубліковано перший стандарт шифрування – DES, а також американські математики У. Діффі та М. Хелман заклали основи *криптографії з відкритими ключами.* Одразу після цього з'явилася перша реальна шифрсистема RSA з відкритим ключем, створена Райвестом, Шаміром та Адамаром. Поряд з ідеєю відкритого шифрування, Діффі та Хелман запропонували ідею відкритого розподілу ключів, що дозволила б використовувати незахищений канал зв'язку при розсилці криптографічних ключів [2].

В 1985 році було запропоновано використання еліптичних кривих в криптографічних цілях. Роль основної криптографічної операції виконує множення точки еліптичної кривої на ціле число, що визначається через операції додавання та подвоєння точок кривої. Характерними перевагами криптографії на еліптичних кривих є швидкість алгоритмів та невелика довжина ключа. Стійкість криптосистем на еліптичних кривих базується на складності обрахування дискретного логарифму в групах точок.

Методика досліджень. Для управління доступом до персональних даних було обрано використання довіреного цифрового підпису на основі еліптичних кривих як основного механізму розподілу криптографічних ключів доступу до інформаційних ресурсів.

Для перевірки доцільності використання довіреного цифрового підпису на основі еліптичних кривих для управління доступом до персональних даних було поставлено наступні завдання: огляд теоретичних відомостей з криптографії на основі відкритих ключів; пошук алгоритмів довіреного цифрового підпису; створення варіанту використання довіреного цифрового підпису на основі еліптичних кривих для управління доступом до персональних даних.

У системах електронного документообігу часто використовується електронний цифровий підпис як механізм забезпечення аутентифікації джерела, цілісності повідомлення та неможливість відмови від факту підпису. Надійність цього механізму визначається складністю підробки підпису, створення підписаного документу або його підміни. Традиційні протоколи цифрового підпису дозволяють користувачу виконати підпис під документом самостійно і будь-який учасник електронного інформаційного обміну зможе переконатися в коректності підпису. Проте, такі протоколи не дозволяють одному учаснику делегувати свої права іншому учаснику, що зміг би підписувати повідомлення чи документи від його імені. Для вирішення подібної задачі використовуються протоколи довіреного цифрового підпису.

Засновниками теорії протоколів довіреного цифрового підпису та розробниками першого такого протоколу є M. Mambo, K. Usuda та E. Okamoto. Саме ними вперше було сформульовано вимоги до безпеки протоколів довіреного цифрового підпису. Згідно їх теорії, безпечний довірений цифровий підпис повинен задовольняти наступні вимоги [3]:

- можливість перевірки – перевіряючий може бути переконаний, що підпис поставлений з дозволу довірителя;
- стійкість до фальсифікації – тільки визначена довірителем сторона може створити вірний довірений цифровий підпис від імені довірителя. Іншими словами, не повинно бути можливості створення підпису від імені довіреної особи без її відома;
- ідентифікація – кожен повинен мати можливість ідентифікувати відповідну довірену

сторону з довіреного підпису;

 неможливість відмови – якщо довірений підписник створює підпис під документом, то в майбутньому він не зможе довести, що підпис був виконаний кимось іншим;

 протистояння ескалації дозволів – довірена сторона не повинна використовувати ключ підписання для цілей, що не вказані довірителем в інформації про дозволи.

Основна ідея, що використовується при створенні довірених цифрових підписів полягає в створенні схеми розподілу ключової інформації таким чином, щоб можна було використовувати вже існуючі алгоритми цифрового підпису.

Кожен учасник інформаційного обміну має свою пару ключів – відкритий та закритий. Для створення довіреності, довіритель повинен передати інформації про повноваження, термін дії по відкритому чи захищеному каналу учаснику – довіреній особі. Довірений учасник, в цілях ідентифікації довірителя, перевіряє вхідні дані та, на основі отриманої інформації, створює пару довірених ключів – закритий та відкритий. Закритий ключ надалі використовуватиметься для створення цифрового підпису, а відкритий – для його перевірки іншими учасниками інформаційного обміну.

Загальна схема довіреного цифрового підпису, що реалізує наведену ідею, виглядає наступним чином [3]:

Дії довірителя **A**:

1. Створює випадкове зобов'язання k та обраховує його свідоцтво $K = f(k)$, де f – деяка одностороння функція.
2. Створює s_A, що залежить від величин $\{x_A, y_B, k, K, w\}$, де x_A – закритий ключ А, y_B – відкритий ключ В, k – зобов'язання, K – свідоцтво, w – повноваження, та відправляє їх довіреній особі В.

Дії довіреної особи **B**:

1. Перевіряє виконання певної ідентифікаційної умови, що залежить від y_A, y_B, s_A та K з метою ідентифікації А.
2. Якщо умова з попереднього кроку виконана, то В обраховує довірені ключі x_p, що повинні залежати від s_A, x_B, y_A, y_B та w, та $y_p = f(x_p)$.
3. За допомогою існуючого алгоритму цифрового підпису підписує деякий документ М, використовуючи x_p в якості ключа для підпису. Створений підпис позначається $Sign(M, x_p)$. Довірений підпису формується під M як $\sigma = (Sign(M, x_p), K, y_A, y_B, w)$.

Дії перевіряючого:

1. Обраховує y_p, застосовуючи певний алгоритм до K, y_A, y_B, w, що містяться в σ.
2. За допомогою ключа y_p перевіряє підпис $Sign(M, x_p)$ під документом M, використовуючи процедуру верифікації відповідного алгоритму цифрового підпису.

Пропонується використовувати довірений цифровий підпис для підпису запитів на інформаційні ресурси або, в розглянутому прикладі – персональних даних. В даному випадку M є не власне документом, а запитом на інформаційний ресурс. Довірителем ***A*** виступає власник персональних даних, а довіреною стороною ***B*** – третя сторона або зовнішній сервіс, що використовує персональні дані в цілях обробки або збереження. В такому варіанті кожен учасник інформаційного обміну, зможе перевірити дозвіл власника персональних даних на їх використання зовнішнім сервісом в рамках обмежень, встановлених w.

Зважаючи на переваги криптосистем на основі еліптичних кривих, пропонується наступний протокол довіреного цифрового підпису з використанням особливостей групи точок еліптичної кривої.

Еліптичною кривою називається крива, координати точок якої задовольняють залежності

$$y^2 = x^3 + ax + b.$$

В криптографічних цілях використовуються лише криві, що не мають особливих точок – точок зламу або точок само перетину. Параметри таких кривих повинні задовольняти наступній умові:

$$4a^3 + 27b^2 \neq 0.$$

Точки еліптичної кривої утворюють групу, елементами якої є точки, що належать кривій; в якості одиничного елемента виступає точка на нескінченності; оберненим елементом до точки P є точка, симетрична їй відносно осі x; операція групи задана наступним правилом: сума точок, що лежать на одній прямій дорівнює точці на нескінченності – нулю групи. Криптосистеми на еліптичних кривих використовують поняття породжуючого елемента – генератора циклічної групи. Генератор групи – це елемент, всі степені котрого пробігають всі елементи групи.

Пропонується наступний протокол довіреного цифрового підпису з використанням еліптичних кривих. В ньому використовується n – велике просте число, що є загальновідомим для всіх учасників інформаційного обміну. Кожен учасник інформаційного обміну також має пару ключів (d, H) – відкритий та закритий, що пов'язані наступним співвідношенням: $H = d \cdot G$, де G – загальновідомий генератор групи точок еліптичної кривої. w описує список прав та доступів, що надаються довіреній особі. h – криптографічна геш-функція.

Дії довірителя **А**:

1. Генерує випадкове число $k \in (1, n)$.
2. Обраховує значення точки $P = k \cdot G = (x_P, y_P)$. $r = x_P$.
3. Обраховує довірений підпис
$$s = d_A + k \cdot w \cdot r.$$
4. Величини (P, s, w) довіритель **А** надсилає довіреній особі **В**.

Дії довіреної особи **В**:

1. Перевіряє ідентифікаційну умову:
$$s \cdot G = H_A + P \cdot w \cdot r.$$
2. Створює ключ підписання:
$$l = d_B + s.$$
3. Відповідний відкритий ключ для перевірки:
$$u = l \cdot G = H_B + H_A + P \cdot w \cdot r.$$

Підписання повідомлення (запиту на інформаційний ресурс):

1. M – повідомлення, $h(M)$ – його геш.
$$sign = l \cdot h(M) + d_B.$$
2. Величини $(M, sign, P, w)$ передаються перевіряючому.

Дії перевіряючого:

1. Перевіряє вірність довіреного цифрового підпису з загальновідомих величин H_B, H_A, P, w:
$$sign \cdot G = h(M) \cdot [H_B + H_A + P \cdot w \cdot r] + H_B.$$

Отже, проблема управління доступом до персональних даних може бути вирішена за допомогою використання протоколів довіреного цифрового підпису. Взявши в якості повідомлення, що підписується, запит на документ, кожен учасник інформаційного обміну має можливість бути переконаним, що довірена особа має необхідні повноваження, що можуть бути обмежені довірителем. Запропоновано протокол довіреного цифрового підпису на основі криптографічних властивостей груп точок еліптичної кривої.

Список використаних джерел:

1. Regulation of the European parliament and of the council of on the protection natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016. **2.** Завадська Л. О., Савчук М. М. Математичні методи захисту інформації : курс лекцій для студентів напрямів підготовки 0802 «Прикладна математика», 0804 «Комп'ютерні науки», 1601 «Інформаційна безпека». К. : НТУУ «КПІ», 2008. 127 с. **3.** Толюпа Е. А. Некоторые протоколы доверенной цифровой підписи. *Прикладная дискретная математика*. № 1 (11). 2011. С. 70–77.