УДК 681.518

ВИКОРИСТАННЯ КОРЕЛЯЦІЙНИХ ФУНКЦІЙ ПРИ РЕЄСТРАЦІЇ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Сегін А.І.[1)], Трач А.А.[2)], Вітрук В.В.[3)]
Тернопільський національний економічний університет
[1)]к.т.н., доцент; [2,3)] студент

I. Вступ

В сучасному суспільстві будь-яка діяльність супроводжується веденням документації, яка вимагає певних затрат часу і матеріальних ресурсів. Рівень затрат на роботу з документами залежить, від обсягу документації, кваліфікації персоналу, правильності організації роботи з документацією та інших факторів. Як і в інших сферах діяльності, роботу з документацією намагаються оптимізувати та автоматизувати [1].

З розвитком комп'ютерної техніки та її широким використанням актуальною стала задача переходу на системи електронного документообігу (СЕД). Оскільки, на даному етапі, в суспільстві використовується два типи документів: паперові і електронні, то СЕД повинні мати засоби автоматизованої обробки обох видів документів. Крім того, при переході на електронні типи документів, виникло ряд питань, одними з яких є підтвердження достовірності документу та захисту від навмисних чи ненавмисних змін.

Рішенням таких задач полягає у введені певного реєстраційного коду. Такий код, з одного боку, повинен формуватись на основі вмісту документу, і при зміні хоча б одного символу, таку зміну виявляти. А з іншого боку – ідентифікувати особу, яка несе відповідальність за цей документ.

II. Принцип формування електронного цифрового підпису та верифікація на його основі достовірності документу

На даний час, в якості такого коду є застосування електронного цифрового підпису (ЦЕП), який дозволяє убезпечити документ від несанкціонованих змін та підтвердити його достовірність. Проте відкритим залишається питання удосконалення методів формування такого цифрового підпису та його надійності, пошук альтернативних методів реєстрації електронних документів, які б були більш ефективними.

Електронний цифровий підпис – це реквізити електронного документу, які дозволяють встановити відсутність змін у електронному документі та перевірити приналежність підпису відповідній особі [2].

Принцип роботи електронного підпису досить простий (рис. 1).

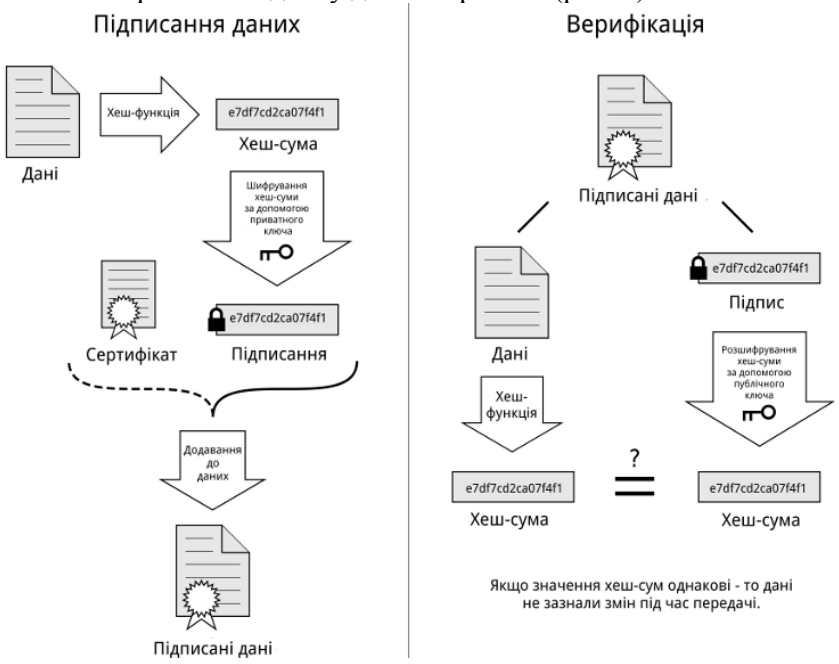

Рисунок 1 – Структурна схема процесу передавання повідомлення з електронним цифровим підписом та перевірка достовірності повідомлення

Кожному користувачеві, що бажає брати участь в електронному документообігу генеруються 2 ключі – відкритий і закритий. Підписант формує документ, який необхідно відправити. Потім, на основі закритого (приватного) ключа, вмісту документа і спеціального програмного забезпечення генерує послідовність символів, яка і є електронним підписом, і відправляє підписаний документ одержувачу. Одержувач документа за допомогою відкритого (публічного) ключа підписувача виконує зворотне криптографічне перетворення, тим самим перевіряє ЕЦП відправника та засвідчується в тому, що текст документа не був спотворений.

III. Використання кореляційних моделей для формування ідентифікатора електронного документу

В розглянутому на рис. 1 прикладі, кореляційні функції можуть бути використані для генерації унікального ідентифікатора документу – хеш суми. Якщо кореляційну модель побудувати таким чином, щоб всі символи документу приймали участь у формуванні його ідентифікатора, то крім унікальності цього номера, це ще забезпечить додатковий захист від фальсифікації документа, оскільки зміна в ньому хоча б одного символу приведе до зміни всього ідентифікатора.

Як показано в [3], існує цілий ряд кореляційних функцій і, в загальному, кореляційну модель для генерації, наприклад, шістнадцяти символьного номеру можна представити у наступному вигляді:

$$W_{xx}(j)=\frac{1}{M}\sum_{i=0}^{M} r(x_i, x_{i+j}), \qquad j=\overline{0,\ 15}, \tag{1}$$

де N – кількість символів в документі;

$M = N - 15$ – довжина вибірки для кореляції;

$r(x_i, x_{i+j})$ – одна з кореляційних функцій;

$W_{xx}(j)$ – значення вибраної кореляційної функції, що відповідає виразу $r(x_i, x_{i+j})$, які одночасно є символами ідентифікатора документу (хеш-суми). На основі досліджень в [3], для досягнення більшої швидкодії зручніше використовувати структурну, модульну або функцію еквівалентності.

Наприклад, ідентифікатор для тексту даної статті, обчислений на базі функції еквівалентності,

$$F_{xx}(j)=\frac{1}{M}\sum_{i=1}^{M} \overset{\vee}{z}[x_i, x_{i+j}], \tag{2}$$

де $\overset{\vee}{z}[x_i, x_{i+j}]=\begin{cases} x_i, & x_i \geq x_{i+j} \\ x_{i+j}, & x_i < x_{i+j} \end{cases}$ — функція «менше з двох»

буде мати вигляд: 18F42AED90B23F5D.

При цьому прийнято, що символи ідентифікатора документу представляються в шістнадцятковій системі числення.

Методика отримання ідентифікатора документу на базі кореляційних моделей можуть мати різні модифікації. Так ідентифікатор може обчислюватись на основі різних кореляційних функцій, мати різну довжину, представлятися може в різних системах кодування та системах числення, використовувати кореляцію тексту документу з наперед заданим кодом та ін.

Висновок

Запропонована методика реєстрації електронних документів має ряд переваг над існуючим електронним підписом, які полягають в тому, що при веденні внутрішнього електронного документообігу не потрібно звертатися в зовнішні сертифікаційні центри, можна вибирати зручну систему кодування документів найбільш оптимальну для організації, більшої захищеності документів завдяки нетрадиційній системі кодування та інші.

Список використаних джерел

1. Пітух І., Николайчук Я., Возна Н. Принципи побудови комп'ютерних мереж з глибоким розпаралелюванням інформаційних потоків на основі матричних моделей руху даних // Вісник НУ „Львівська політехніка". Радіоелектроніка та телекомунікації. – 2004.- № 508. – С. 263–268.

2. Николайчук Л.М., Возна Н.Я.. Реалізація цифрового підпису в телекомунікаційних системах та його правові аспекти. // Вісник Технологічного університету Поділля.-№ 3 Том. 1(51). - Хмельницький, 2003. – С. 125-128.

3. Николайчук Я. М., Сегін А. І. Моделі джерел інформації та методи їх представлення // Методи та прилади контролю якості. ІФДТУНГ, 1998, № 2. – С. 80 – 84.