УДК 004:657

ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС: СУТНІСТЬ, ПРИНЦИП ДІЇ ТА ПОРЯДОК ОТРИМАННЯ

Волинець В.І. – к.т.н., доцент
Вінницький навчально-науковий інститут економіки ТНЕУ

В сучасних умовах все більшого поширення набуває електронний документообіг електронних документів [1], застосування якого надає ряд суттєвих переваг в порівнянні з традиційним документообігом паперових документів. Обов'язковим реквізитом кожного електронного документа є електронний цифровий підпис, який використовується для ідентифікації підписувача та підтвердження цілісності даних електронного документа [2].

Окремі питання, пов'язані з електронним документообігом та електронним цифровим підписом, розглядались в працях таких науковців як Білуха М.Т., Гринович А.А., Кукарін О.Б., Мельник Т., Новицький А.М., Шпірко А. [3-5]. Однак, в зв'язку з можливим значним зростанням кількості користувачів електронного документообігу, зокрема в сфері бухгалтерського обліку та звітності, існує нагальна потреба комплексного висвітлення основних питань, пов'язаних з електронним цифровим підписом.

Метою даної роботи є дослідження сутності, принципу дії та порядку отримання електронного цифрового підпису.

Електронний цифровий підпис (ЕЦП) – це вид електронного підпису, отриманого в результаті криптографічного перетворення даних електронного документа, який додається до цих електронних даних або логічно з ними поєднується і дає змогу підтвердити цілісність електронного документа та ідентифікувати підписувача [2].

ЕЦП накладаються (створюються) за допомогою особистого (закритого) ключа (електронних даних фіксованого розміру), відомого лише підписувачу електронних документів, а перевіряються за допомогою відкритого ключа (електронних даних фіксованого розміру), доступного всім отримувачам електронних документів.

Процес накладання ЕЦП здійснюється наступним чином:

- на першому кроці визначається хеш-функція (контрольна сума невеликого фіксованого розміру) електронного документа, яка ідентифікує його зміст;
- на другому кроці хеш-функція шифрується особистим ключем ЕЦП підписувача та в зашифрованому вигляді додається до даних електронного документа.

Процес перевірки ЕЦП здійснюється наступним чином:

- на першому кроці визначається хеш-функція отриманого електронного документа (даних електронного документа, не включаючи дані ЕЦП);
- на другому кроці здійснюється розшифрування зашифрованої хеш-функції, яка міститься в отриманому електронному документі, за допомогою відкритого ключа ЕЦП підписувача;
- на третьому кроці здійснюється порівняння хеш-функцій, визначених на попередніх кроках. Їх співпадіння підтверджує справжність змісту документу та його авторство.

Окрім накладання та перевірки підпису, відкритий та особистий ключі також використовуються для шифрування та розшифрування електронних документів в цілому. Електронні документи шифруються відправниками за допомогою відкритих ключів отримувачів електронних документів, а розшифровуються отримувачами за допомогою їх особистих ключів.

Отже, накласти ЕЦП на електронні документи, що відправляються, та розшифрувати отримані електронні документи можуть лише користувачі особистих ключів, а перевірити ЕЦП підписувачів та зашифрувати електронні документи, які відправляються, можуть всі користувачі, які мають відкриті ключі тих, від кого вони отримують та кому відправляють електронні документи.

Відкритий ключ міститься у посиленому сертифікаті відкритого ключа – електронному документі, який формується, розповсюджується (за згодою власників), обслуговується (блокується, скасовується, поновлюється) акредитованим центром сертифікації ключів (АЦСК) та підписується його особистим ключем.

Для отримання посиленого сертифікату відкритого ключа необхідно:

1. Подати до одного з АЦСК заповнену і підписану реєстраційну картку та комплект документів, склад яких залежить від виду заявника (юридична особа, відокремлений підрозділ юридичної особи, фізична особа – підприємець (ФОП), фізична особа, інше), з інформацією про осіб та установу, для яких необхідно отримати сертифікати відкритих

ключів.

2. Сформувати усі особисті ключі та запити на формування сертифікатів відкритих ключів (відповідні файли), використовуючи програмне забезпечення для генерації ключів та запитів, в АЦСК або за місцем роботи. При створенні кожного особистого ключа задати пароль захисту.

На підставі запитів на формування сертифікатів відкритих ключів сертифікати формуються у АЦСК, після чого передаються власникам ключів та/або публікуються на сайті АЦСК.

Станом на 01 січня 2017 року в Україні функціонує 28 АЦСК, серед яких до АЦСК, сертифікати яких підтримуються, зокрема програмним забезпеченням електронного документообігу, належать АЦСК Інформаційно-довідкового департаменту Державної фіскальної служби України (АЦСК ІДД ДФСУ), АЦСК органів юстиції України (АЦСК ОЮУ), АЦСК «Цент сертифікації ключів «Україна» (АЦСК «Україна»), АЦСК ПрАТ «Інфраструктура відкритих ключів» (АЦСК «ІВК»), АЦСК ТОВ «Ключові системи» (АЦСК «КС»), АЦСК державного підприємства «Українські спеціальні системи» (АЦСК «УСС»), АЦСК «Masterkey» ТОВ «Арт-майстер» (АЦСК «Masterkey»), АЦСК державного підприємства «Головний інформаційно-обчислювальний центр Державної адміністрації залізничного транспорту України» (АЦСК «Укрзалізниця»), АЦСК ринку електричної енергії (АЦСК РЕЕ).

Вартість формування та обслуговування сертифікатів відкритих ключів в різних АЦСК наведена в табл. 1.

Таблиця 1

Вартість формування та обслуговування сертифікатів відкритих ключів за один рік, грн. (станом на 01.01.2017 року)

АЦСК	Фізичні особи	ФОП	Юридичні особи
АЦСК ІДД ДФСУ	Безкоштовно		
АЦСК ОЮУ	48		
АЦСК «Україна»	74	74 (без печатки) 92 (з печаткою)	116
АЦСК «ІВК»	96	96	132
АЦСК «КС»	115	132	161
АЦСК «УСС»	150		
АЦСК «Укрзалізниця»	210		
АЦСК «Masterkey»	214		
АЦСК РЕЕ	Безкоштовно (для членів оптового ринку електричної енергії)		

Таким чином, в роботі розглянуто сутність, принцип дії та порядок отримання ЕЦП, що дозволить потенційним користувачам електронного документообігу отримати відповіді на основні питання, пов’язані з використанням ЕЦП.

Література

1. Про електронні документи та електронний документообіг: Закон України від 22.05.03 р. № 851-IV, зі змінами та доповненнями [Електронний ресурс] // Верховна Рада України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/851-15.

2. Про електронний цифровий підпис: Закон України від 22.05.03 р. № 852-IV, зі змінами та доповненнями [Електронний ресурс] // Верховна Рада України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/852-15.

3. Гринович А.А., Пухальська Г.В. Електронний цифровий підпис: особливості застосування, переваги та проблеми // Вісник Хмельницького національного університету. Серія: Економічні науки. – 2009. – № 2, Т. 1. – С. 19-21.

4. Кукарін О.Б. Електронний документообіг та захист інформації: навч. посіб. / За заг. ред. д.держ.упр., професора Н.В. Грицяк. – К.: НАДУ, 2015. – 84 с.

5. Мельник Т. Електронний документообіг та електронний підпис // Бухгалтерський облік і аудит. – 2008. – № 7. – С. 47-53.