ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС ЯК ГОЛОВНИЙ ЕЛЕМЕНТ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Мінгальова Ю.І.
Україна, м. Житомир,
Житомирський державний університет ім. І.Франка

В статье проанализированы основные задачи, выделены свойства и методы построения схем электронной цифровой подписи. Рассмотрены наиболее распространенные программные средства работы с ЭЦП, а также законодательные и нормативные акты, которые определяют принципы использования ЭЦП в Украине.

Впродовж багатьох років документообігу підпис відповідальної особи або виконуючого обов'язки був неодмінною умовою визнання його статусу або беззаперечним свідоцтвом його важливості. Справжність різних паперових документів (юридичних, фінансових та ін) визначається наявністю або відсутністю авторизованого рукописного підпису. Щоб системи комп'ютерних повідомлень могли замінити фізичне переміщення документів, написаних чорнилом на папері, потрібно вирішити проблему підпису. Проблема впровадження заміни рукописного підпису досить складна [4, с. 853]. Вимагається система, за допомогою якої одна сторона могла б послати іншій стороні «підписане» повідомлення так, щоб виконувались наступні властивості підпису [5, с. 65]:

- підпис автентичний (за його допомогою одержувач міг перевірити оголошену особу відправника);
- підпис є доказом, що тільки та людина, чий автограф стоїть на документі, могла підписати цей документ, і ніхто інший не зміг би це зробити;
- підпис не можливо перенести (він є частиною документа, яку перенести на інший документ неможливо);
- документ з підписом є незмінним (тобто після підписання його неможливо змінити, залишивши даний факт непоміченим);
- підпис незаперечний (особа, яка підписала документ, у разі визнання експертизою, що саме вона засвідчила даний документ, не може оскаржити факт підписання);
- будь-яка особа, що має зразок підпису, може впевнитися в тому, що даний документ підписаний власником підпису.

Метою даної статті є аналіз основних схем та розгляд переваг практичного використання електронного цифрового підпису (ЕЦП), а також законодавчих та нормативних актів, які визначають організаційні принципи використання ЕЦП в Україні.

Розвиток глобальних комунікацій, науково-технічного прогресу та економіки, засвоєння нових районів, будування нових об’єктів, ускладнення процесів управління призвели до появи нової області взаємовідносин в діловому і повсякденному житті, предметом яких є електронний обмін даними. У такому обміні даними можуть брати участь органи державної влади, комерційні і некомерційні організації, а також громадяни в своїх офіційних і особистих стосунках. В електронному документі відомості, зафіксовані за допомогою електронних даних, мають включати обов’язкові реквізити документа, найголовнішим з яких є електронний підпис, в іншому випадку це документ в електронному вигляді. Тобто без електронного підпису за певних вимог документ не має юридичної сили і не може бути електронним документом.

Проблема збереження електронних документів від копіювання, модифікації та підробки вимагає для свого вирішення специфічних засобів і методів захисту. Одним з поширених в світі засобів такого захисту є електронний цифровий підпис (ЕЦП), який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документу, його реквізитів і факту підписання конкретною особою. Документи можуть бути засвідчені електронним цифровим підписом і передані до місця призначення протягом

декількох секунд, адже електронний документ передається за допомогою швидкісних телекомунікаційних систем, однією з яких є, наприклад, Інтернет [8]. За таких умов усі учасники обміну електронними документами незалежно від відстані мають однакові можливості в електронному інформаційному обміні.

Електронний підпис - дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації людини, яка підписала ці данні [3].

Електронний цифровий підпис - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати оголошену особу відправника. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа [3].

Програма електронного документообігу з використанням ЕЦП на сьогодні активно впроваджується в державних установах і органах державної влади, що істотно розширює можливості застосування ЕЦП і розвиток електронного документообігу в Україні.

Перший нормативний акт щодо ЕЦП прийнято в Україні у 2002 р. – це стандарт ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння" [3]. В Україні прийнято закони: "Про електронні документи та електронний документообіг" 2003 року № 851-IV, та "Про електронний цифровий підпис" 2003 року № 852-IV [6]. Згідно цих законів, ЕЦП за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо: електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису; під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису; особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті, який виданий в Україні [2]. Законами встановлено, що Національна система електронного цифрового підпису складається:

- центральний засвідчувальний орган (ЦЗО) веде акредитацію центрів сертифікації ключів та забезпечує цілодобово доступ до відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали, тощо;
- контролюючий орган – центральний орган виконавчої влади у сфері криптографічного захисту інформації, уповноважений перевіряти дотримання вимог Закону "Про електронний цифровий підпис“ центральним засвідчувальним органом, засвідчувальними центрами та центрами сертифікації ключів;
- центр сертифікації ключів (ЦСК) надає послуги ЕЦП. Можуть функціонувати два типи ЦСК - центр сертифікації ключів й акредитований центр сертифікації ключів [10].

Фізична або юридична особа, яка бажає стати учасником системи ЕЦП (підписувач), звертається у ЦСК, який здійснює ідентифікацію заявника, формування для нього сертифікату, переміщення останнього до бази даних дійсних сертифікатів ЦСК. З цього мометну підписувач при створенні електронного документу має можливість додавати до нього власний ЕЦП. Отримувач, одержавши підписане повідомлення, звертається по каналах зв’язку до бази даних про сертифікати та перевіряє статус сертифікату (чинний, заблокований, скасований). Для втілення у практику вищеназваних законів Кабінетом Міністрів України протягом 2004 року прийнято ряд постанов, серед яких: „Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу” (2004 р. № 680), „Про затвердження Порядку акредитації центру сертифікації ключів” (2004 р. № 903), „Про затвердження Положення про центральний засвідчувальний орган” (2004 р. №1451), „Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної

форми власності" (2004 р. №1452), „Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади" (№1453 2004 р.) [3].

Цифровий підпис дозволяє вирішити наступні завдання:

- здійснити аутентифікацію джерела повідомлення;
- встановити цілісність повідомлення;
- забезпечити неможливість відмови від факту підпису конкретного повідомлення [1, с. 365].

У практичній діяльності важливо не тільки захищати дані від незаконного користувача, але і мати можливість перевірити авторство даного повідомлення і щоб воно не було змінено сторонньою особою. Саме для вирішення цих проблем було розроблено ряд алгоритмів ЕЦП. В основі більшості з них лежить ідея використання деякої односторонньої функції з секретним ключем F_K для створення пари бінарних рядків (M, Q), де M – електронний документ, а Q - рішення рівняння $F_K(Q)=M$ [9, с. 264].

Виділимо наступні властивості ЕЦП:

1) при будь-якому K існує поліноміальний алгоритм обчислення значення $F_K(Q)$;
2) при невідомому K не існує поліноміального алгоритму для рішення рівняння $F_K(Q)=M$ відносно Q;
3) при відомому K існує поліноміального алгоритму для рішення рівняння $F_K(Q)=M$ відносно Q.

В силу першої властивості завжди легко перевірити, чи відповідає підпис до повідомлення, а в силу другої властивості підробити підпис при достатньо великому ключі практично неможливо. Доказ цієї властивості дозволив би надати підписаним повідомлення юридичну силу.

Секретний та відкритий ключі знаходяться у взаємно однозначній відповідності та в силу третьої вимоги не існує поліноміального алгоритму обчислення секретної компоненти по відкритій компоненті.

Існує кілька методів побудови схем ЕЦП, а саме [5, с. 66-68]:

1) шифрування електронного документа на основі симетричних алгоритмів. Дана схема передбачає наявність у системі третьої особи (арбітра), що користується довірою учасників обміну підписаними подібним чином електронними документами. Взаємодія користувачів даною системою проводиться за наступною схемою:

- учасник А зашифровує повідомлення на своєму секретному ключі K_A значення якого розділене з арбітром, потім шифроване повідомлення передається арбітру із зазначенням адресата даного повідомлення (інформація, що ідентифікує адресата, передається також у зашифрованому вигляді);
- арбітр розшифровує отримане повідомлення на ключі K_A, проводить необхідні перевірки і потім зашифровує на секретному ключі учасника В (K_B). Далі зашифроване повідомлення посилається учаснику В разом з інформацією, що воно прийшло від учасника А;
- учасник В розшифровує дане повідомлення і переконується в тому, що відправником є учасник А.

2) використання асиметричних алгоритмів шифрування. Фактом підписання документа в даній схемі є зашифрування документа на секретному ключі його відправника. Ця схема теж використовується теж досить рідко внаслідок того, що довжина електронного документа може виявитися критичною. У цьому випадку не потрібно наявності третьої сторони, хоча вона може виступати в ролі сертифікаційного органу відкритих ключів користувачів;

3) з розвитком попередньої ідеї стала найбільш поширена схема ЕЦП, а саме: зашифрування остаточного результату обробки електронного документа хеш-функцією за допомогою асиметричного алгоритму. Хеш-функцією називається математична або інша функція, яка для рядка довільної довжини обчислює деяке ціле значення або деякий інший рядок фіксованої довжини [7, с. 264]. Математично це можна записати так: $h = H(M)$, де

M - вихідне повідомлення, зване іноді прообразом, а h - результат, званий значенням хеш-функції (хеш-кодом або дайджестом).

Генерація підпису відбувається наступним чином:

1) учасник А обчислює хеш-код від електронного документа. Отриманий хеш-код проходить процедуру перетворення з використанням свого секретного ключа. Після чого отримане значення (яке і є ЕЦП) разом з електронним документом відправляється учаснику В.

2) учасник В повинен отримати електронний документ з ЕЦП та сертифікований відкритий ключ учасника А, а потім провести дешифрування на ньому ЕЦП, сам ЕД піддається операції хешування, після чого результати порівнюються, і якщо вони співпадають, то ЕЦП визнається істинною, в іншому випадку помилкової.

Криптографічна хеш-функція повинна забезпечувати: стійкість до колізій (два різні набори даних повинні мати різні результати перетворення) та необоротність (неможливість обчислити вхідні дані за результатом перетворення).

У більшості ранніх систем ЕЦП використовувалися функції з секретом, які за своїм призначенням близькі до односторонніх функцій. Такі системи уразливі до атак з використанням відкритого ключа, так як, вибравши довільний цифровий підпис і застосувавши до неї алгоритм верифікації, можна отримати вихідний текст. Щоб уникнути цього, разом з цифровим підписом використовується хеш-функція, тобто, обчислення підпису здійснюється не щодо самого документа, а щодо його хешу. У цьому випадку в результаті верифікації можна отримати тільки хеш вихідного тексту, отже, якщо використовується хеш-функція криптографічно стійка, то отримати вихідний текст буде обчислювально складно, а значить атака такого типу стає неможливою.

Крім цього, існують інші різновиди цифрових підписів (груповий підпис, незаперечний підпис, довірений підпис), які є модифікаціями описаних вище схем. Їх поява обумовлена різноманітністю завдань, що вирішуються за допомогою ЕЦП.

Засоби роботи з електронним цифровим підписом.

Пакет PGP (Pretty Good Privacy) - найпоширеніший програмний продукт, що дозволяє використовувати сучасні надійні криптографічні алгоритми для захисту інформації в персональних комп'ютерах .

Основні переваги:

- вихідний код доступний у відкритому вигляді;
- стійкість досягається шляхом використання кращих алгоритмів, при цьому для надійного захисту даних допускаються ключі великої довжини;
- підтримка централізованої (через сервери ключів) та децентралізованої (через «мережу довіри») моделі розподілу відкритих ключів;
- зручний програмний інтерфейс.

GNU Privacy Guard (GnuPG) (www.gnupg.org) - повна і вільно поширювана заміна для пакету PGP. Цей пакет не використовує патентований алгоритм IDEA, тому використовується без обмежень.

Пакет програм Криптон - призначений для використання електронного цифрового підпису (ЕЦП) електронних документів. У стандартному постачанні для зберігання файлів відкритих ключів використовуються дискети, смарт-карти, електронні таблетки Touch Memory.

Переваги електронного документообігу та цифрового підпису:

1) пришвидшення державних процесів, полегшення спілкування з державними органами;
2) зручна організація архівів електронних документів полегшить роботу працівникам як державних, так і недержавних органів;
3) заощаджені державні кошти за рахунок зменшення паперового документообігу;
4) спрощення та пришвидшення процесів аудиту та перевірки, за наявності відповідних дозволів, надасть простий доступ до інформації;
5) стане ефективнішим процес виявлення зловживань і незаконної діяльності [2].

Отже, електронний цифровий підпис спрямований на спрощення та прискорення документообігу між суб'єктами господарювання, що, в свою чергу, має зміцнити конкурентоспроможність вітчизняних підприємств, адже пришвидшиться процедура укладення цивільно-правових і господарських договорів, оформлення експортно-імпортних операцій, надання електронних банківських послуг. В Україні існує законодавча база ЕЦП, створена Національна система електронного цифрового підпису та функціонують органи, які надають користувачам послуги ЕЦП.

Список використаної літератури:

1. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие / 2-е изд., испр. И доп. – М.: Гелиос АРВ, 2002. – 480 с. ил.*
2. *Гринович А.А., Пухальська Г.В. Електронний цифровий підпис: особливості застосування, переваги та проблеми. – [Електронний ресурс]. – Режим доступу до ресурсу: http://www.nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2009_2/zmist.files/05.pdf*
3. *ДСТУ 4145-2002 "Криптографічний захист ін- формації. Цифровий підпис, що ґрунтується на еліптич- них кривих. Формування та перевіряння" Державний комітет України з питань технічного регулювання та споживчої політики. – 28.12.2002. – № 31. – [Електронний ресурс]. – Режим доступу до ресурсу: http://www.dssu.gov.ua.*
4. *Компьютерные сети. 4-е изд./ Э. Таненбаум. – СПб.: Питер, 2003. – 992с.: ил*
5. *Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.: ил.*
6. *Сайт Верховної Ради України „Законодавство”. – [Електронний ресурс]. – Режим доступу до ресурсу: http://www.rada.gov.ua.*
7. *Смарт Н. Криптография Москва: Техносфера, 2005. – 528с.*
8. *Спірін О.М., Ковальчук В.Н. Методика забезпечення он-лайн безпеки старшокласників у навчально-виховному процесі школи – [Електронний ресурс]. – Режим доступу: http://www.journal.iitta.gov.ua*
9. *Харин Ю.С. и др. Математические основы криптологии: Учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. – Мн.: БГУ, 1999.- 319с.: ил.*
10. *Чередниченко В.Б. Електронний цивровий підпис у правовому полі України [Електронний ресурс]. – Режим доступу до ресурсу: http://www.nbuv.gov.ua/portal/natural/soi/2009_7/Chered.pdf*