Іванов В.Г.
Доктор технічних наук, професор кафедри криміналістики
Національний Юридичний Університет імені Ярослава Мудрого.
м. Харків,Україна.

ТЕХНОЛОГІЧНІ І ПРАВОВІ АСПЕКТИ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Електронний цифровий підпис (ЕЦП) – це набір двійкових знаків (біт), отриманий за спеціальними алгоритмами зі змісту електронного документа що дозволяє встановити авторство документа, а так само несанкціоновані зміни цього документа. ЕЦП застосовується в електронному державному документообігу та електронної комерції для ідентифікації підписувача та підтвердження цілісності даних в електронній формі. Електронний документ, підписаний ЕЦП має таку ж юридичну силу, як і паперовий документ підписаний власноручним підписом [1,2].

Одним з основних реквізитів звичайних документів є рукописний підпис. Він підтверджує факт взаємозв'язку між відомостями, що містяться в документі, і особою, що підписала документ. В основу використання рукописного підпису як засобу ідентифікації покладена гіпотеза про унікальність особистих біометричних параметрів людини. Однак його ступінь захисту зовсім недостатній. Наприклад, на фінансових документах необхідна наявність двох рукописних підписів, а також печатки юридичної особи. Якщо й цього недостатньо, то засвідчують у нотаріуса чи використовують спеціальні бланки, що мають особливі засоби захисту.

Рукописний підпис можливий тільки на документах, що мають матеріальну природу. Сторони – учасники угоди повинні при її складанні знаходитися поруч або в опосередкованому контакті через матеріальний носій та послуги сторонніх організацій (служб доставки). Звідси випливає необхідність розходження між оригіналом та копіями документів, одержаними засобами копіювально-множної техніки. Ще один недолік рукописного підпису, що не дозволяє використовувати його в електронної комерції – функціональний. Він пов'язаний з тим, що рукописний підпис забезпечує тільки ідентифікацію документа, тобто підтвердження його відношення до особи, яка поставила підпис, але ніякою мірою не забезпечує аутентифікації документа, тобто його цілісності та незмінності. Без спеціальних додаткових заходів захисту рукописний підпис не гарантує того, що документ не піддався змістовим змінам під час збереження чи транспортування.

Електронний цифровий підпис має не фізичну, а логічну природу – це послідовність символів, що дозволяє однозначно зв'язати автора документа, зміст документа та власника електронного цифрового підпису [3]. Електронний цифровий підпис має наступні позитивні властивості: 1) співставлення захисних властивостей. Можливість порівняти захисні властивості різних типів алгоритмів електронних цифрових підписів на строгому математичному аналізі; 2) масштабованість. Можливість застосування найпростіших засобів електронного цифрового підпису в цивільному документообігу, а в випадках важливих та секретних документів – застосування інших, складних і спеціальних, засобів електронного цифрового підпису; 3) дематеріалізація документа. Незалежність електронного цифрового підпису від носія. Ця властивість лежить в основі електронної комерції; 4) рівнозначність копій. Будь-яка копія документа без додаткових заходів рівнозначна оригіналу. 5) можливість аутентифікації документа. В електронний документ, підписаний ЕЦП, не можна внести зміни, не порушивши підпис.

Засоби ЕЦП (комп'ютерні програми) використовують методи і способи криптографії (шифрування) [4,5]. Ці методи поділяють на два класи: симетричні і несиметричні. Метод шифрування – це формальний алгоритм, що описує порядок перетворення повідомлення в зашифроване. Ключ шифрування – це набір даних, необхідних для застосування методу шифрування. Симетричні методи шифрування мають високий рівень безпеки и прийнятну

швидкість обробки даних. При симетричному шифруванні обидві сторони використовують той самий ключ. Яким ключем повідомлення шифрувалося, тим же ключем і дешифрується. Це недолік, бо для використання симетричного алгоритму сторони повинні попередньо обмінятися ключами, а для цього потрібно пряме фізичне спілкування либо захищений канал зв'язку. Тому алгоритми симетричного шифрування прямо не використовуються в електронній комерції та сучасному урядуванню.

Електронний документообіг та електронний цифровий підпис зокрема заснований на методах несиметричної криптографії. Несиметрична криптографія використовує спеціальні математичні методи, на основі яких створено програмні засоби, які називаються засобами електронного цифрового підпису. Після застосування одного з таких засобів утворюється пара взаємозалежних ключів з унікальною властивістю: те, що зашифровано одним ключем, може бути дешифровано тільки іншим, і навпаки. Власник пари ключів залишає один ключ собі, а інший ключ поширює, тобто розсилає своїм адресатам. Публікація ключа може відбуватися прямим розсиланням, наприклад, електронною поштою або розміщенням ключа на своєму сайті, де його зможе одержати кожен бажаючий. Ключ, залишений для себе, називається закритим чи особистим ключем. Опублікований ключ називається відкритим чи публічним. Час обробки даних несиметричними методами істотно більше (на один-два порядки), ніж з використанням симетричних методів. У найпростішому випадку ЕЦП – це деякі дані про себе, зашифровані особистим (закритим) ключем. Кожен, хто володіє відкритим ключем, зможе ці відомості прочитати і переконатися, хто є автором повідомлення.

Для виявлення несанкціонованих змін в тексті повідомлень використовують дайджест повідомлення. Це унікальна послідовність символів, що однозначно відповідає змісту повідомлення. Зазвичай дайджест має фіксований розмір 128 чи 168 бітів, що не залежить від довжини самого повідомлення. Дайджест вноситься до складу електронного цифрового підпису разом з відомостями про автора та зашифровується разом з ними.

Найпростіший прийом створення дайджесту – контрольна сума символів. Наприклад, якщо букві "а" відповідає в таблиці ASCII число 192, букві "б" – число 193, а букві "в" – 194, то контрольна сума тексту "абв" – 1*192+2*193+3*194=1160. Для великого за обсягом тексту це буде величезне число, тому, щоб одержати контрольну суму в 128 бітів, її переводять у двійковий вигляд, тобто який вона і має у комп'ютері, та беруть останні 128 знаків.

Зрозуміло, що при зміні змісту, навіть однієї букви, зміниться і контрольна сума. Множення на 1, 2, 3 і так далі у формулі для підрахунку контрольної суми необхідно для того, щоб не можна було переставити букви без зміни контрольної суми. Про правильну контрольну суму користувач довідається з підпису і, порівнявши їх, виявить стороннє втручання.

Запевняємо підписом повідомлення може бути абсолютно довільного розміру: від кілобайтних текстових повідомлень й до мегабайтних графічних файлів. Тому для формування ЕЦП в якості вихідного значення береться не саме повідомлення, а його хеш (результат обробки повідомлення спеціальною хеш-функцією). Завдання хеш-функції – з повідомлення довільної довжини швидко обчислити цифрову послідовність потрібного розміру (скажімо, 128 або 168 Обробка таких повідомлень безпосередньо методом несиметричного шифрування (закритим ключем) потребує дуже великого обсягу обчисленьЦю послідовність ще називають дайджест або контрольна сума. Хеш-функція повинна відповідати певним вимогам. Перш за все необхідно, щоб результат (хеш повідомлення) однозначно відповідав вихідному повідомленню і змінювався при будь-якій модифікації останнього, навіть незначною. Тобто хеш повідомлення має залежати від кожного символу вихідного повідомлення і від порядку їх слідування. Хеш повідомлення повинне обчислюватися таким чином, щоб по хешированій версії повідомлення не можна було ніякими способами відновити саме повідомлення. Крім того, дуже важко відшукати два набори даних, що володіють одним і тим же значенням хеш-функції. Отримана через хеш-функцію контрольна сума повідомлення шифруються закритим ключем відправника і разом з листом і відкритим ключем (сертифікатом) відправляються одержувачу. Комп'ютерна програма адресата за допомогою отриманого відкритого ключа розшифровує отриману

контрольну суму. Потім програма генерує контрольну суму для тексту листа і звіряє обидві контрольні суми. Якщо суми збіглися, то це гарантує одночасно справжність змісту документу та його авторство.

У відкритому ключі наводяться дані про власника, але в ньому нема засобів, які б засвідчили, що ці дані не підмінені. Без вирішення цього питання механізм електронного цифрового підпису не може бути використаний ні в електронній комерції, ні в електронному документообігу. Тому Закон України "Про електронний цифровий підпис" та ще деякі державні законодавчі акти присвячені механізму підтвердження особи власника відкритого ключа. Це – сертифікації відкритих ключів. В усіх випадках вказаний механізм заснований на тому, що вводиться (призначається) додаткова сторона, яка засвідчує належність відкритого ключа конкретній юридичній чи фізичній особі[3].

У статті 3 Закону зазначено, що "електронний цифровий підпис 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".

Основне поняття тут –"посилений сертифікат ключа" – визначено в статті 1:

"посилений сертифікат відкритого ключа (далі – посилений сертифікат ключа) – сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом".

В статті 6 Закону перераховані необхідні дані, що повинен містити сертифікат ключа, а в статтях 8, 9, 10 та 11 вказані вимоги до центрів сертифікації ключів та інших уповноважених на це органів, а також їх права та обов'язки.

Таким чином особа, яка створила собі пари ключів, повинна звернутися в орган, уповноважений виконати сертифікацію, та отримати сертифікат ключа. Центр сертифікації перевіряє належність відкритого ключа заявнику і засвідчує цей факт додаванням до відкритого ключа свого підпису, зашифрованого власним закритим ключем. Будь-який партнер, бажаючи вступити в контакт із власником відкритого ключа, може прочитати запис, що засвідчений, за допомогою відкритого ключа центру сертифікації. Якщо цілісність запису не порушена і він довіряє центру сертифікації, то може використовувати відкритий ключ іншого партнера для зв'язку з ним.

Додаткові можливості при роботі з ЕЦП: фіксування точного часу підписання документа, який згодом неможливо змінити навіть особою, яка наклала підпис. Можливо лише повторне підписання з фіксацією нового часу. Шифрування з використанням Сертифікату відкритого ключа одержувача. Це дозволяє зміст документа прочитати тільки тому, кому воно адресоване.

ЛИТЕРАТУРА

1. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 року № 851-IV. [Електронний ресурс] // Офіційний веб-сайт Верховної Ради України. – Режим доступу до матеріалу http://zakon3.rada.gov.ua/laws/main/851-15.

2. Матвиенко А. Основы организации электронного документооборота: Учебное пособие. / А. Матвиенко, М. Цывин. – К.: Центр учебной литературы, 2008. – 112 с.

3. Про електронний цифровий підпис : Закон України від 22 травня 2003 року № 852-IV. [Електронний ресурс] // Офіційний веб-сайт Верховної Ради України. – Режим доступу до матеріалу http://zakon3.rada.gov.ua/laws/main/852-15.

4. Задірака В. К. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: навч. посіб. / Задірака В. К., Кудін А. М., Людвиченко В. О., Олексюк О. С. Київ – Тернопіль: Підручники і посібники, 2007. – 272 с.

5. Правова інформація та комп’ютерні технології в юридичній діяльності : навч. посіб. / В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін., за заг. ред. В. Г. Іванова. – Х.: Право, 2010. – 240 с.

Ключевые слова: Електронний цифровий підпис, технологічні і правові аспекти, дайджест повідомлення, сертифікація відкритих ключів.

Анотація: Розглянуто технологічні та правові аспекти електронного цифрового підпису. Показано, що для виявлення несанкціонованих змін в тексті повідомлень використовуються дайджест повідомлення. Наводиться поняття хеш-фукції, а також призначення центру сертифікації відкритих ключів.

Іванов В. Г. Технологічні і правові аспекти електронного цифрового підпису / В. Г. Іванов // Права та обов’язки людини у сучасному світі : Матеріали міжнародної науково-практичної конференції (м. Одеса, Україна, 11-12 листопада 2016 р.) – Одеса: ГО «Причорноморська фундація права», 2016. – С. 125–128.