УДК 621.391

ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС - МІЖНАРОДНІ ТА НАЦІОНАЛЬНІ ПРАВОВІ АСПЕКТИ

І.А. Кулик, *канд. техн. наук, доцент;*
В.Б. Чередниченко*, ст. викладач*,*
Сумський державний університет, м. Суми;
**Сумська філія Харківського національного університету внутрішніх справ, м. Суми.*

Застосування програмних засобів електронного цифрового підпису може досягти мети лише за дотримання вимог відповідних нормативно-правових актів. Розглянуто правову базу, встановлену документами ООН, а також законодавчими актами України, яка регламентує використання цифрового підпису документів.

Ключові слова: *цифровий підпис, електронний документ, ЮНСІТРАЛ, криптографія, посилений сертифікат ключа, засвідчувальний орган, центр сертифікації ключів.*

Применение программных средств электронной цифровой подписи может достичь цели только при соблюдении требований соответствующих нормативно - правовых документов. Рассмотрены правовая база, установленная документами ООН, а также законодательные акты Украины, регламентирующие использование цифровой подписи документов.

Ключевые слова: *цифровая подпись, электронный документ, ЮНСИТРАЛ, криптография, усиленный сертификат ключа, свидетельствующий орган, центр сертификации ключей.*

ВСТУП

Сьогодні все більшого поширення набуває обмін так званими „електронними документами" у банківській, економічній, правовій, технічній та інших сферах, що відкриває перспективи для прискорення розвитку та підвищення ефективності людської діяльності. Тому актуальним стає захист даних „цифровим підписом" (ЦП), що надає їм юридичної сили паперових документів, засвідчених підписом та печаткою відправника [1]. Цієї мети можна досягти за дотримання вимог низки законодавчих актів та інших нормативно – правових документів, а також при технічно коректному застосуванні легальних програмних засобів.

Глобальні мережі дозволяють вільно передавати інформацію через кордони, але у різних державах можуть застосовуватись неоднакові законодавчі підходи стосовно чинності електронних підписів. Тому важливими є юридична узгодженість міжнародних та національних правових актів. Фахівці у галузі ЦП звичайно досліджують науково – технічні аспекти у даній сфері, а правові засади привертають менше уваги науковців.

ПОСТАНОВКА ЗАВДАННЯ

Розгляд міжнародно-правових аспектів цифрового підпису та законодавства й інших нормативних документів України є завданням цієї роботи.

Міжнародні нормативні документи про цифровий підпис. Уперше ідея цифрового підпису була викладена У. Диффі (W. Diffie) та М. Хеллманом (M. Hellman) у 1976 р. з метою заміни звичайних паперових документів їх електронними аналогами, повноцінними з юридичної точки зору. Першим практичним рішенням став „електронний

підпис RSA", розроблений у 1977 р. співробітниками Масачусетського технологічного інституту (H. Rivest, A. Shamir, L. Adleman) [1]. У 1985 р. створено (El Gamal) криптографічну систему, на базі якої побудовано криптографічний стандарт США DSS (Digital Signature Standart). У 1990 р. розроблено (P. Zimmermann) на базі алгоритму RSA для застосування цифрового підпису програму PGP (Pretty Good Privasy) [1]. Вона має недорогі комерційні варіанти, а також спрощену безплатну версію. Програмне забезпечення PGP поклало початок активного використання ЦП у різних країнах. Альтернативою їй стала випущена у 1999 р. В. Кохом (Werner Koch) система GPG (GNU Privacy Guard), яка поширюється вільно. GPG дозволяє шифрувати та підписувати дані з метою їх безпечної передачі та зберігання, а також повністю сумісна з стандартом IETF OpenPGP, що дозволяє їй взаємодіяти з системою PGP.

Оскільки використання цифрового підпису досить поширене у багатьох країнах, були прийняті нормативні документи міжнародного рівня, які регламентують розроблення та застосування засобів ЦП. Одним із перших таких актів, призначених для узгодження підходів щодо надання електронній кореспонденції статусу документів, які мають юридичну силу, став „Правовий посібник з електронного переказу коштів" Комісії ООН з права та міжнародної торгівлі (ЮНСІТРАЛ) від 1987 р. [3]. У ньому було запропоновано спільні підходи до підписів у електронній формі та до сертифікаційних органів. Важливим етапом розвитку ЦП став Типовий закон ЮНСІТРАЛ «Про електронну торгівлю» від 1996 р., який сформулював фундаментальні принципи щодо використання електронних підписів, як засобу забезпечення однакового режиму для користувачів паперової документації й користувачів комп'ютеризованої інформації [4].

Одним з основних міжнародних документів у цій сфері є Типовий закон Комісії ООН з права та міжнародної торгівлі ЮНСІТРАЛ «Про електронні підписи», прийнятий у 2001 році [5]. Його призначення – надати державам допомогу зі створення уніфікованої законодавчої бази, яка регулює функції підпису в електронному середовищі. Крім того, Типовий закон встановлює зв'язок між технічною надійністю і юридичною чинністю, якою може володіти конкретний електронний підпис у "кіберпросторі".

У Типовому законі „Про електронні підписи" визначено, що цифрові підписи створюються і перевіряються шляхом використання криптографії, яка дозволяє перетворювати повідомлення у форму, що здається незрозумілою, і, навпаки, у первинну форму. При поставленні цифрових підписів застосовується метод, відомий як "криптографія з використанням публічного ключа", яка найчастіше ґрунтується на використанні алгоритмічних функцій для створення двох різних, але математично взаємозв'язаних "ключів" (тобто великих чисел, складених за допомогою ряду математичних формул). Один такий ключ - приватний (або закритий) використовується для накладення цифрового підпису або перетворення даних в удавану незрозумілу форму. Інший ключ - публічний (або відкритий) застосовується для посвідчення дійсності цифрового підпису та відтворення повідомлення в його первинній формі. Принцип створення пари ключів забезпечує режим, коли багато осіб може знати публічний ключ і використовувати його для перевірки дійсності електронного повідомлення, але вони не можуть установити приватний ключ відправника і використовувати цей ключ для підробки даних. Зауважимо, що застосування криптографії з метою посвідчення дійсності документа шляхом створення цифрового підпису необов'язково повинне забезпечити конфіденційність інформації в процесі передачі повідомлень, оскільки закодований цифровий підпис може бути доданий

до незакодованого (відкритого) повідомлення з метою підтвердження відсутніх змін у ньому [5].

У Типовому законі ЮНСІТРАЛ було рекомендовано з метою посвідчення чинності ЦП мати незалежну (третю щодо двох учасників електронного обміну) сторону, якій належить встановлювати зв'язок між особою, що підписала документ, та конкретним публічним ключем. У Типовому законі ця сторона названа „постачальник сертифікаційних послуг". Типовий закон визначив, що повинні існувати три функції (або ролі) стосовно пар ключів, а саме: у функція видачі ключа (чи функція абонування), сертифікаційна функція і функція приймаючої сторони (яка покладається на підпис). Для виконання таких функцій, як правило, створюється „Інфраструктура публічних ключів" (ІПК), яка складається з органів різної ієрархії, а саме: у державі створюється один „базовий орган", який видає сертифікати на діяльність у сфері ЦП та реєструє організації, уповноважені видавати пари ключів. Органи нижчого рівня (сертифікаційні) підтверджують відповідність публічного ключа до приватного ключа певної особи, його чинність та незмінність. Ще нижчими за рівнем є місцеві реєстраційні органи, які безпосередньо одержують запити користувачів ключів та надають їм відповіді.

Одержувач «електронного документа» для встановлення зв'язку між парою ключів одержує від постачальника сертифікаційних послуг (сертифікаційного органу) сертифікат, в якому в електронному вигляді підтверджується, що даному публічному ключу відповідає певна особа, яка користується відповідним парним приватним ключем. У такий спосіб технічно забезпечується гарантія того, що цифровий підпис був використаний саме особою, яка його підписала, та в одержаному повідомленні відсутні зміни порівняно з первинним змістом. Для забезпечення перевірки справжності цифрових підписів сертифікаційні органи створюють реєстри ключів (захищені електронні довідники), які звичайно функціонують у режимі он-лайн цілодобово [5]. Сертифікаційні органи можуть створюватися державними органами або приватними підприємствами. Визнання зарубіжних сертифікатів забезпечується методом „перехресної" сертифікації рівноправних органів у відповідних державах.

Як наслідок, усе більш широкого застосування цифрового підпису набули нові напрями суспільної діяльності: електронний бізнес, електронний уряд, електронне навчання, електронна охорона здоров'я, електронна наукова діяльність тощо.

У 2005 р. прийнято Конвенцію Організації Об'єднаних Націй про використання електронних повідомлень у міжнародних договорах [6]. Вона логічно завершує серію міжнародних актів щодо врегулювання питань цифрового підпису. До Конвенції включено всі основні напрацювання попередніх документів ООН із цього питання. Крім того, у Конвенції чітко фіксуються основні вимоги щодо чинності електронних документів, а саме: повідомлення чи договір не можуть бути позбавлені дійсності або позовної сили на тій лише підставі, що вони складені у формі електронного повідомлення. У випадках, коли законодавство вимагає, щоб повідомлення чи договір були представлені у письмовій формі, або передбачає настання певних наслідків у разі відсутності письмової форми, ця вимога вважається виконаною шляхом представлення електронного повідомлення, створеного з додержанням необхідних процедур. У випадках, коли законодавство вимагає, щоб повідомлення чи договір надавалися або зберігалися в їхній справжній (першоджерельній) формі, чи передбачає настання визначених наслідків у разі відсутності справжньої форми, ця вимога вважається виконаною у відношенні електронного повідомлення, створеного з додержанням визначених у Конвенції процедур. Також чітко визначені моменти

відправлення електронного повідомлення та його одержання, процедури виправлення помилок у таких документах тощо.

Ця Конвенція була відкрита для підписання всіма державами в центральних установах Організації Об'єднаних Націй, після чого вона підлягає ратифікації (прийняттю чи затвердженню) державами, що її підписали. Ратифікаційні грамоти чи документи про прийняття (приєднання) здаються на збереження Генеральному секретарю Організації Об'єднаних Націй. Це перший документ про цифровий підпис, дія якого має зобов'язальний характер на територіях держав, що її підписали, у повній відповідності з міжнародними правовими процедурами [6].

Нормативна база України про цифровий підпис. В Україні напрацьована певна законодавча база у сфері електронного підпису. Основними є два закони України: "Про електронні документи та електронний документообіг" від 22 травня 2003 року № 851-IV, та "Про електронний цифровий підпис" від 22 травня 2003 року № 852-IV [7]. У них знайшли відображення світові законодавчі засади щодо ЦП. У 2002 р. прийнято перший криптографічний стандарт України ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння", який набув чинності з 1 липня 2003 року. [8]. Крім нього, в Україні діє міждержавний стандарт ГОСТ 34.310-95 "Информационная технология. Процедура выработки и проверки цифровой подписи на базе асимметричного криптографического алгоритма".

Згідно із Законом України "Про електронний цифровий підпис" електронний цифровий підпис (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 [7].

Законодавство України встановило такі суб'єкти правових відносин у сфері послуг електронного цифрового підпису: центральний засвідчувальний орган; засвідчувальний центр органу виконавчої влади або іншого державного органу; контролюючий орган; центр сертифікації ключів; акредитований центр сертифікації ключів; підписувач; користувач. Цим Законом встановлено такі функції перелічених суб'єктів.

Функції центрального засвідчувального органу (ЦЗО) у Національній системі електронного цифрового підпису виконує Державний департамент з питань зв'язку та інформатизації Міністерства інфраструктури України [9]. Крім того, Кабінет Міністрів України за необхідності визначає засвідчувальний центр (з повноваженнями центрального засвідчувального органу) для центрального органу виконавчої влади та інших державних органів, які надають послуги електронного цифрового підпису цим органам і підпорядкованим ним підприємствам, установам та організаціям. Центральний засвідчувальний орган має такі основні функції: проводить акредитацію центрів сертифікації ключів; формує і видає посилені сертифікати ключів засвідчувальним центрам та центрам сертифікації ключів; блокує, скасовує та поновлює посилені сертифікати ключів засвідчувальних центрів та центрів сертифікації ключів; проводить електронні реєстри чинних, блокованих та скасованих посилених сертифікатів ключів засвідчувальних центрів та центрів сертифікації ключів; забезпечує цілодобово доступ засвідчувальних

центрів та центрів сертифікації ключів до посилених сертифікатів ключів та відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали тощо.

Контролюючий орган – це 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. Контролюючим органом в Україні встановлена Адміністрація Держспецзв'язку.

Центр сертифікації ключів (далі - ЦСК) безпосередньо надає послуги ЕЦП. Ним може бути юридична чи фізична особа – суб'єкт підприємницької діяльності, який надає послуги у сфері ЕЦП й засвідчує свій відкритий ключ у центральному засвідчувальному органі. Можуть функціонувати два типи надавачів послуг у сфері ЕЦП - центр сертифікації ключів й акредитований центр сертифікації ключів. Акредитованим центром сертифікації є такий, що пройшов добровільну процедуру акредитації на здатність виконувати функції щодо обслуговування посилених сертифікатів. Такий ЦСК використовує лише надійні засоби ЕЦП, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації [9].

Для втілення у практику вищеназваних законів протягом 2004 року Кабінетом Міністрів України прийнято ряд постанов, а саме: „Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу" (від 26 травня 2004 р. № 680); „Про затвердження Порядку акредитації центру сертифікації ключів" (від 13 липня 2004 р. № 903); „Про затвердження Положення про центральний засвідчувальний орган" (від 28 жовтня 2004 р. №1451); „Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності" (№1452 від 28 жовтня 2004 р.); „Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади" (№1453 від 28 жовтня 2004 р.); „Про затвердження Порядку обов'язкової передачі документованої інформації" (№ 1454 від 28 жовтня 2004 р.) [7]. Зміст цих постанов визначено в їхніх назвах, детальний аналіз урегульованих у них процесів не є метою цієї роботи.

Функціонування ЕЦП відбувається таким чином. Фізична або юридична особа, яка бажає стати учасником системи ЕЦП (підписувач), звертається у центр сертифікації ключів (або акредитований ЦСК), який здійснює ідентифікацію заявника і формування для нього сертифіката (посиленого сертифіката). Новий сертифікат переміщується до бази даних дійсних сертифікатів ЦСК та стає доступним для всіх користувачів по загальнодоступних телекомунікаційних каналах. Тепер підписувач при створенні електронного документа може додавати до нього власний ЕЦП. Отримувач, одержавши підписане повідомлення, звертається до бази даних сертифікатів, за ідентифікаційними даними відправника перевіряє статус сертифіката (чинний, заблокований, скасований). Якщо сертифікат дійсний на момент перевірки ЕЦП, за допомогою відкритого ключа відправника виконується перевірка його підпису.

Перший центр сертифікації ключів було акредитовано в Україні у січні 2006 р. На 01.03.2011 р. функціонує 14 таких центрів (один із них – державне підприємство "Центр автентифікації національної системи конфіденційного зв'язку" Державного підприємства "Українські спеціальні системи"). Більшість центрів має до 30 регіональних представництв. Також діє чотири неакредитованих ЦСК. Крім того,

зареєстровано також 16 засвідчувальних центрів та центрів сертифікації ключів [9].

Обслуговування сертифікатів відкритих ключів акредитованих ЦСК здійснює технологічний центр ЦЗО, створений на базі Державного підприємства "Державний центр інформаційних ресурсів України".

В Україні продовжується процес удосконалення законодавства про цифровий підпис.

ВИСНОВКИ

Поширення обміну „електронними документами" та підвищення вимог до достовірності отриманої банківської, економічної, правової, технічної та іншої важливої інформації розширюють сфери застосування цифрового підпису (ЦП). Використання комп'ютерних мереж для передачі даних через кордони потребує не тільки технічної сумісності процедур, але й їхньої правової узгодженості.

Рад міждержавних актів установлюють умови надання електронній кореспонденції статусу документів, що мають юридичну силу, а саме: „Правовий посібник з електронному переказу коштів" Комісії ООН з права та міжнародної торгівлі (ЮНСІТРАЛ) від 1987 р., Типовий закон ЮНСІТРАЛ «Про електронну торгівлю» від 1996 р., Типовий закон ЮНСІТРАЛ «Про електронні підписи», прийнятий у 2001 році, та Конвенція Організації Об'єднаних Націй „Про використання електронних повідомлень у міжнародних договорах" 2005 р. Остання має силу закону для держав, що її підписали, у повній відповідності з міжнародними правовими процедурами.

Порівняння змісту міжнародних та національних правових актів дозволяє зробити висновок, що в Україні створена законодавча база ЕЦП. У державі функціонує Національна система електронного цифрового підпису, а відповідні органи надають користувачам послуги ЕЦП.

SUMMARY

DIGITAL SIGNATURES - INTERNATIONAL AND NATIONAL LEGAL ASPECTS

I.A. Kulik, V.B. Cherednichenko,*
Sumy State University, Sumy,
**Sumy branch of Kharkiv National University of Internal Affairs, Sumy*

Application software digital signature can reach the goal only if the requirements of the relevant normative - legal documents. A legal framework set by the UN documents and laws of Ukraine, which regulates the use of digitally signed documents.

***Key words**: digital signature, electronic document, UNCITRAL, cryptography, key certificate, witness thick body, key certification center.*

СПИСОК ЛІТЕРАТУРИ

1. Фергюсон Н., Шнайер Б. Практическая криптография. [Текст] / Нильс Фергюсон, Брюс Шнайер. – М. : Вильямс, 2005. - 424 с. - ISBN 5-8459-0733-0.
2. Руководство по GnuPG. [Електронний ресурс]. – Режим доступу : http://www.gentoo.org/doc/ru/gnupg-user.xml - Загол. з екрана.
3. „Правовий посібник по електронному переказу коштів" Комісії ООН по праву та міжнародній торгівлі (ЮНСІТРАЛ) від 1987 р. [Електронний ресурс]. – Режим доступу : http://www.uncitral.org/uncitral/ru/ - Загол. з екрана.
4. Типовий закон «Про електронну торгівлю» Комісії ООН по праву та міжнародній торгівлі (ЮНСІТРАЛ), 1996 р. [Електронний ресурс]. – Режим доступу : http://www.uncitral.org/uncitral/ru/ - Загол. з екрана.
5. Типовий закон «Про електронні підписи» Комісії ООН по праву та міжнародній торгівлі (ЮНСІТРАЛ), 2001 р. [Електронний ресурс]. – Режим доступу : http://www.uncitral.org/uncitral/ru/ - Загол. з екрана.

6. Конвенція Організації Об'єднаних Націй „Об использовании электронных сообщений в международных договорах". [Електронний ресурс]. – Режим доступу: http://www.ifap.ru/pr/2005/051128aa.htm - Загол. з екрана.
7. Сайт Верховної Ради України „Законодавство". [Електронний ресурс]. – Режим доступу: http://www.rada. gov.ua - Загол. з екрана.
8. ДСТУ 4145-2002 "Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння". [Електронний ресурс]. – Режим доступу : http://www.dssu.gov.ua/ - Загол. з екрана..
9. Центральний засвсідчувальний орган. [Електронний ресурс]. – Режим доступу : www.czo.gov.ua - Загол. з екрана.

Надійшла до редакції 5 квітня 2011 р.