УДК 351.755.5:[005.92:004.63](477)

Лютенко К. Т., Яковлєв С. В.

ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ В УКРАЇНІ: ПРОБЛЕМНІ АСПЕКТИ

Ця стаття – короткий огляд юридичних і технічних передумов для ефективного впровадження електронного документообігу. Особливу увагу приділено практичним проблемам правового регулювання електронно-цифрового підпису як повноцінного аналогу власноручного підпису. Недоліки процесу впровадження електронного документообігу в Україні проілюстровано освітнім експериментом «Електронний вступ 2011».

Ключові слова: електронний документ, електронний цифровий підпис, власноручний підпис, захист інформації, сертифікат.

Схвалюючи Концепцію розвитку електронного урядування в Україні [1], Кабінет Міністрів, по-перше, визнав необхідність упровадження технологій електронного урядування у діяльність органів державної влади та органів місцевого самоврядування і, по-друге, задекларував, що одним із пріоритетів розвитку нашої держави є розвиток високотехнологічного інформаційного суспільства, яке дасть змогу кожному громадянинові створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися та обмінюватися ними. Етапи реалізації згаданої Концепції передбачають, зокрема, створення єдиної загальнодержавної системи електронного документообігу, забезпечення передачі електронних документів до державних архівів, музеїв, бібліотек, їх довгострокове зберігання, підтримка в актуалізованому стані та надання доступу до них, а також створення Національного депозитарію електронних інформаційних ресурсів.

Автори не є прихильниками позиції, що електронний документообіг повинен повністю витіснити паперовий; ці дві форми мають ефективно співіснувати і давати можливість вільно застосовувати будь-яку із них, враховуючи доцільність у конкретних умовах. Проте, на відміну від паперового діловодства, процес упровадження електронної документації повинен подолати певні проблеми, основні з яких і буде висвітлено у цій статті.

Законодавство визначає електронний документ як документ, інформація в якому зафіксована у вигляді електронних даних, у тому числі обов'язкові реквізити документа [2].

З одного боку, переваги даних, що існують в електронній формі, над паперовими носіями очевидні: зменшення витрат на архівацію, підвищення рівня захисту даних, прозорий та ефективний документообіг, можливість організації колективної синхронної роботи над документом, стандартизоване введення даних та автоматизація процесу їх обробки тощо [3]. З іншого боку, на практиці виникають труднощі щодо порядку надання доступу до документа та керування внесенням змін, навчання персоналу основам користування комп'ютерами та певною інформаційною системою, проблема одночасного існування паперового та електронного документообігу, відсутність як визначених норм щодо здійснення електронного діловодства, так і уніфікованих технічних форматів створення електронних архівів й алгоритмів генерації та підтвердження електронних цифрових підписів (далі – ЕЦП) тощо [4].

ЕЦП не лише замінює традиційні печатку та підпис, він також забезпечує достовірність і цілісність інформації – гарантію того, що дані існують у їхньому початковому вигляді і під час їх зберігання та передачі не було внесено несанкціонованих змін з боку третіх осіб [5]. UNCITRAL Model Law on electronic signatures (2001) наділяє ЕЦП такою характеристикою, як функціональна еквівалентність – здатність виконувати усі функції паперового документа: фіксування інформації, особи, яка підписала, умов складання (час, дата, місце), розрізняє оригінал і копію документа, може бути доказом у суді [6].

Математичне підґрунтя використання цифрового підпису зводиться до двох процедур: генерація цифрового підпису та його перевірка. Під час генерації з вхідних даних, випадкових даних та ключа формується деяке значення – цифровий підпис. Перевірка ЕЦП полягає у перевірці визначених залежностей між даними, підписом та ключем, на підставі чого робиться висновок щодо поставлення ЕЦП саме підписувачем та щодо можливого пошкодження чи модифікації даних. В основі алгоритму роботи з ЕЦП, що належить до так званої асиметричної криптографії, – принцип ключової пари: один ключ, особистий, слу-

гує для генерації підпису під даними та доступний тільки підписувачу; другий ключ, відкритий, публікується підписувачем у загальнодоступних джерелах, тож кожен суб'єкт у сфері використання ЕЦП за допомогою цього відкритого ключа може перевірити підпис. Математичний апарат, що використовується, дає змогу швидко обчислювати відкритий ключ за значенням секретного, але обернена операція вкрай складна. Таким чином, публікація відкритого ключа ніяк не може зашкодити власникові, але зникають витрати, пов'язані з захищеним транспортуванням ключів між користувачами.

Однак асиметричній криптографії в цілому притаманний суттєвий недолік: з математичного погляду відкриті ключі – це звичайні числа, без будь-якої прив'язки до конкретної особи. Отже, є можливість фальсифікації ЕЦП та порушення конфіденційних даних шляхом видавання згенерованих будь-ким ключових пар за ключі законних користувачів. Математично цей недолік принципово не усувається, тому для боротьби з ним застосовують організаційно-адміністративні заходи, найпоширенішими з яких є використання інфраструктур відкритих ключів, завдання яких – організація роботи із відкритими ключами користувачів, їх зберігання, транспортування та, найголовніше, встановлення довіри до ключів у інших користувачів. Джерелом довіри до ключів є так звана третя довірена сторона; в нашому випадку це спеціальний орган – Центр сертифікації ключів (ЦСК). Центри сертифікації за заявами користувачів виконують необхідні перевірки та видають так звані сертифікати ключів, що містять сам відкритий ключ, відомості про його власника, термін дії, можливі сфери використання тощо; сертифікати підписуються власним ключем ЦСК, і цей підпис вважається гарантією коректності наведених відомостей. Отже, новому користувачу необхідно встановити довіру одному лише ЦСК (зазвичай окремими організаційними процедурами), щоб потім автоматично встановлювати довіру до всіх інших користувачів цього ЦСК.

Незважаючи на понад десятирічну історію національної системи ЕЦП, вона і досі перебуває у зародковому стані, що зумовлене у першу чергу відсутністю адекватної нормативно-правової бази, необхідної для її сталого розвитку. Наприклад, факт схвалення Кабінетом Міністрів Концепції розвитку електронного урядування в Україні не мав наслідком розроблення деталізованого плану конкретних заходів щодо впровадження основних засад цієї Концепції. Крім того, сфера електронного документообігу перебуває у компетенції різних державних установ (Держкомінновації, СБУ, Держспецзв'язку, Держкомпідприємництва, Мінюст тощо); в результаті маємо ситуацію «семи няньок» та низку проблем.

По-перше, немає загального формату електронного документа та подання його реквізитів, через що різні реалізації систем електронного документообігу несумісні між собою. За нашими підрахунками, наразі державні органи та установи, що приймають звітність в електронній формі, використовують до дванадцяти різних форматів документів. По-друге, вже два роки залишаються незатвердженими формати подання електронного цифрового підпису та протокол фіксування часу, без яких системи документообігу просто не можуть повноцінно функціонувати. Те саме стосується й інших необхідних специфікацій більш технічного характеру. По-третє, немає пакета нормативних вимог до Центрів сертифікації ключів, що містили б обов'язкові та рекомендовані політики сертифікації, типовий Регламент роботи тощо.

Та найголовніша проблема, на нашу думку, – це відсутність порядку визначення чинності сертифікату. Надання ЕЦП статусу аналога власноручного підпису створює правову основу для застосування електронних документів під час вчинення юридично значущих дій [7]. Стаття 207 ЦК України [8], по суті, зрівнює паперові та електронні документи, застерігаючи, що використання електронно-числового підпису допускається у випадках, встановлених законом, іншими актами законодавства, за домовленістю сторін. Спеціалізований щодо ЕЦП Закон України «Про електронний цифровий підпис» позиціонує ЕЦП як обов'язковий реквізит електронного документа, який використовується для ідентифікації автора документа іншими суб'єктами документообігу. Проте не встановлено на законодавчому рівні, за яких умов ЕЦП буде валідним. Перевірка валідності ЕЦП вимагає попередньої перевірки чинності сертифіката ключа підписувача. Така перевірка, описана у міжнародних стандартах (так званий Certificate Path Validation), – доволі складна процедура із одинадцятьма вхідними параметрами та багатьма внутрішніми нюансами; у вітчизняній нормативній базі її просто немає. Таким чином, парадокс: хоча нині в Україні активно надаються послуги із сертифікації ключів, а цифровий підпис дедалі більше проникає у різні сфери, легітимні основи використання ключів та сертифікатів залишаються неврегульованими.

Окрім нормативних проблем, на заваді розвитку національної системи ЕЦП та електронного документообігу стоїть і низка проблем організаційного характеру: проблема створення загальнодержавної інтегрованої мережі для забезпечення зовнішнього документообігу між державними органами та взаємодії державних органів і недержавних (у тому числі комерційних) структур; проблема забезпечення всього циклу електронного документообігу, аналогічного звичайному; забезпечення держслужбовців надійними засобами

ЕЦП та іншими необхідними засобами криптографічного захисту інформації; проблема створення електронних архівів, зокрема переведення документів із паперової форми в електронну.

Весь спектр проблем (нормативних, організаційних та технічних), що існують у сфері електронного документообігу, можна проілюструвати на прикладі програми «Електронний вступ 2011» (далі – «ЕВ 2011») [9], впровадженої у 2011 році. Нагадаємо, що система «ЕВ 2011» була посередником між абітурієнтами та приймальними комісіями ВНЗ та надавала послуги з електронної дистанційної реєстрації заявок абітурієнтів. Охочі швидко та без черг подати документи до обраного вишу повинні були подати електронну заяву із необхідними документами через «ЕВ 2011», яка, своєю чергою, передавала її до відповідної приймальної комісії на опрацювання нарівні з заявами, поданими особисто.

Опишемо спочатку, як мала функціонувати подібна система електронної реєстрації (СЕР) в режимі, наближеному до ідеального.

1. Абітурієнт формує та надсилає до СЕР належним чином оформлену електронну заяву з усіма необхідними документами. Заяву абітурієнт повинен скріпити власним ЕЦП на ключах, що пройшли сертифікацію в будь-якому Центрі сертифікації ключів (акредитованому або зареєстрованому). Час створення заявки повинен бути зафіксований за допомогою служби фіксування часу; такі служби фіксування часу функціонують у складі ЦСК, отже, абітурієнт може звертатись до свого Центру.
2. СЕР одержує заяву абітурієнта та (після необхідних перевірок) надсилає йому підтвердження про одержання заявки або її відхилення. Підтвердження повинно бути підписане ключами СЕР, час його створення також повинен бути зафіксований.
3. Заяву абітурієнта СЕР надсилає до відповідної приймальної комісії.
4. Приймальна комісія (після необхідних перевірок) реєструє заяву та надсилає СЕР та безпосередньо абітурієнту підтвердження про реєстрацію, також із власним підписом та зафіксованим часом створення. Після цього приймальна комісія вже працює безпосередньо з абітурієнтом.
5. У разі відсутності підтверджень на кожному із зазначених кроків у визначений термін сторони повинні використовувати резервні засоби зв'язку (наприклад, особисте або телефонне звернення) для подолання труднощів, що виникли.

У цій схемі кожна зі сторін є організаційно захищеною від недобросовісних дій інших. Абітурієнт, маючи на руках власну заяву та підтвердження про її реєстрацію у СЕР, може довести, що він подав заяву належним чином, і тоді, у випадку її втрати, відповідальність нестиме СЕР. І навпаки, не надсилаючи заяву до СЕР, неможливо отримати підтвердження та доводити факт реєстрації. Аналогічно і щодо приймальної комісії: вона не може відмовитися від власного підтвердження (а тому несе відповідальність за зареєстровані заявки), однак без цього підтвердження СЕР та абітурієнт не можуть стверджувати, що заява взагалі потрапила до приймальної комісії.

Наведена схема може бути розширена та мати певні відмінності під час реалізації на практиці (наприклад, абітурієнт може використовувати шифрування для захисту персональних даних, що передаються через СЕР).

Проте під час впровадження «ЕВ 2011» виникла низка проблемних моментів.

1. Громадяни України (та переважна більшість приймальних комісій) не мають засобів ЕЦП і власних ключів, сертифікованих в акредитованих ЦСК. Більше того, наразі вони і не зможуть придбати відповідні засоби, оскільки не існує пропозиції для окремих громадян. Виробники засобів криптографічного захисту та ЦСК пропонують свої послуги для корпоративних клієнтів. Утім, у програмі «ЕВ 2011» взагалі не передбачено можливість додавати ЕЦП до заявок абітурієнтів, що ставить під великий сумнів доцільність такої системи взагалі, беручи до уваги факт закріплення у законодавстві ЕЦП як обов'язкового реквізиту електронного документа.
2. Внаслідок відсутності ЕЦП в «ЕВ 2011» загалом був низький рівень ідентифікації особи, що давало змогу не тільки відправляти заявки від чужого імені, а й поширювати завідомо неправильні відомості про особу, від імені якої така заява подається, – зокрема, спотворювати бали атестату та додаткові бали; можливості перевірки цих даних більш ніж обмежені, оскільки не впроваджена уніфікована база даних, через яку можна було б автоматично перевіряти такі відомості.
3. За відсутності служби фіксації часу не може бути юридично завірений час створення (або, точніше, існування) тієї чи іншої заявки. Отже, всі сторони процесу можуть вільно модифікувати відомості про реєстрацію. Теоретично факт подання заявки можна зафіксувати шляхом складання протоколу у присутності свідків та нотаріального посвідчення «скріншоту» екрану, проте такі дії видаються занадто громіздкими і не виправдовують задекларовану зручність «ЕВ 2011».
4. Інтерфейс «ЕВ 2011» давав змогу не зазначати контактні дані абітурієнтів, що не сприяло вирішенню робочих питань приймальною комісією стосовно абітурієнта. Крім того, в «ЕВ 2011» не передбачено функцію моніторингу заявок.

5. Електронна реєстрація заяви відбувалась через Інтернет-портал «Єдине інформаційне освітнє вікно», власником сайту якого була комерційна структура [10], а отже, необхідна документована згода абітурієнтів на обробку персональних даних [11]. Крім того, передбачалося створення Єдиної державної електронної бази з питань освіти [12], Положення про яку передбачає необхідність отримання від фізичних осіб – учасників освітнього процесу їхньої згоди на обробку відповідних даних у Єдиній базі. Наказ МОНмолодьспорту № 291 передбачав занесення даних із заяв до цієї бази, в тому числі і підстав, що надають пільги (наприклад, дані медичних довідок). Тут взагалі починається сфера права на приватність (як зазначив Європейський суд з прав людини у рішенні «Amann v. Switzerland», поняття «приватне життя» не можна тлумачити звужено, тож автоматична обробка персональних даних цілком підпадає під цю категорію) [13]. І якщо у випадку особистого подання документів письмову згоду отримати можна, то відповідність такій вимозі Закону України «Про захист персональних даних», як «документованість згоди», в умовах електронної реєстрації знову забезпечує наявність ЕЦП.
6. Відсутність електронних форм атестата, медичних довідок тощо передбачає необхідність сканувати їхні паперові аналоги, що створює певний простір для внесення модифікацій у «скани» оригіналів за допомогою графічних редакторів тощо. Відсутність можливості автоматизовано перевіряти достовірність відомостей призводить до втрати часу іншими абітурієнтами.

Розглядаючи твердження у позові одного з абітурієнтів про невідповідність Наказу МОНмолодьспорту № 291 ст. 6 ЗУ «Про електронні документи та електронний документообіг», Окружний адміністративний суд м. Києва зазначив, що «на сьогоднішній день не створено дієвих механізмів використання електронного документообігу з застосуванням електронного підпису, що утруднює доступ користувачам для використання новітніх технологій. Проте вказана обставина не позбавляє можливості проведення експерименту щодо вдосконалення механізму подачі заяв в електронному вигляді» [14]. Сподіваємось, що експеримент «Електронний вступ 2012» буде успішнішим [15].

Список літератури

1. Розпорядження Кабінету Міністрів Укриаїни від 13 грудня 2010 р. № 2250-р «Про схвалення Концепції розвитку електронного урядування в Україні».
2. Ст. 5 Закону України «Про електронні документи та електронний документообіг».
3. Sprague R. H. Jr. Electronic document management : challenges and opportunities for information systems managers / R. H. Jr. Sprague // MIS Quarterly, 1995. – № 19 (1) – P. 29–49.
4. Komito L. Paper “work” and electronic files : defending professional practice / L. Komito // Journal of Information Technology. – 1998. – № 13. – P. 235.
5. Вишневський А., Кучеров М. Запровадження електронного документообігу в органах влади : досвід Головдержслужби України [Електронний ресурс] // Вісник Державної служби України. – 2009. – № 4. – Режим доступу: http://www.center.gov.ua/elektronne-uryaduvannya/zaprovadzhennya-elektronnogo-dokumentoobigu-v-organah-vladi-dosvid-golovderzhsluzhbi-ukrayini.html. – Назва з екрана.
6. Хінінський А. Електронний цифровий підпис (у запитаннях і відповідях) / А. Хінінський // Секретар-референт. – 2011. – № 1. – С. 38–42.
7. Apollònia Martínez-Nadal, Josep Lluís Ferrer-Gomila. Comments to the UNCITRAL Model Law on Electronic Signatures – Universitat de les Illes Balears, 2002. – P. 229–243.
8. Пантюхін В. О. Впровадження системи електронного документообігу : сучасні тенденції / В. О. Пантюхін, О. Г. Севостьянова // Вісник Східноукраїнського національного університету ім. В. Даля. – 2011. – № 17 (171). – С. 122.
9. Цивільний кодекс України від 16.03.2003 року № 435-IV // Відомості Верховної Ради. – 2003. – № 40–44. – С. 356.
10. Наказ Міністерства освіти і науки, молоді та спорту України від 28.03.2011 р. № 291 «Про запровадження у 2011 році у вищих навчальних закладах експерименту «Електронний вступ 2011» [Електронний ресурс]. – Режим доступу: www.zakon1.rada.gov.ua. – Назва з екрана.
11. URL: www.osvita.ua/vnz/news/17963.
12. Ч. 1 ст. 11, ст. 2 ЗУ «Про захист персональних даних» від 01.06.2010 року № 2297-VI [Електронний ресурс]. – Режим доступу: www.zakon1.rada.gov.ua. – Назва з екрана.
13. Постанова КМУ від 13.07.2011 № 752 «Про створення Єдиної державної електронної бази з питань освіти» [Електронний ресурс]. – Режим доступу: www.zakon1.rada.gov.ua. – Назва з екрана.
14. Amann v. Switzerland, para. 65
15. Постанова Окружного адміністративного суду м. Києва № 2а-8785/11/2670 від 04.08.2011
15. Наказ Міністерства освіти і науки, молоді та спорту України № 1179 від 12.10.2011 р. «Про затвердження Порядку подання та розгляду заяв в електронній формі на участь у конкурсному відборі до вищих навчальних закладів» [Електронний ресурс]. – Режим доступу: www.zakon1.rada.gov.ua. – Назва з екрана.

K. Liutenko, S.Yakovlev

ELECTRONIC DOCUMENT MANAGEMENT: PROBLEMATIC ISSUES

This article is a brief review of legal and technical framework for electronic document management. The practical problems of electronic signatures, together with public key certificates, as a substantive solution of hand-written signatures regarding to the legal effect that may result from use of electronic signatures are issued. The paper concludes with some observations that show the non-effectiveness of «Electronic apply 2011».

Keywords: electronic document, electronic document management, electronic signatures, hand-written signatures, asymmetric cryptography.

Матеріал надійшов 30.05.2012