

УДК 681.3:002.651.028

**В.Ю. Горєлова**  
кандидат юридичних наук,  
доцент кафедри державно-правових дисциплін,  
Університет економіки та права «КРОК»

## **Поняття та правовий статус електронного цифрового підпису в Україні: проблемні питання**

*У статті досліджується поняття та правовий статус електронного цифрового підпису, а також здійснюється порівняльний аналіз деяких положень національного та міжнародного законодавства в межах даного питання.*

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

**В.Ю. Горєлова**  
кандидат юридических наук,  
доцент кафедри державно-правових дисциплін,  
Університет економіки та права «КРОК»

## **Понятие и правовой статус электронной цифровой подписи в Украине: проблемные вопросы**

*В статье рассмотрено понятие и правовой статус электронной цифровой подписи, а также проводится сравнительный анализ некоторых положений национального и международного законодательства в рамках данного вопроса.*

**Ключевые слова:** электронная цифровая подпись, информация, электронный документ, защита информации, собственноручная подпись.

**V. Horielova**  
PhD in Law,  
Docent of the Department of State and Legal Disciplines,  
«KROK» University

## **A concept and Legal Status of Electronic Digital Signature in Ukraine: Topical Issue**

*A concept and legal status of electronic digital signature are considered in the article , and also conducted a comparative analysis of some positions of national and international legislation within the framework of this question*

**Keywords:** electronic digital signature, information, electronic document, information protection, sign manual

### **Постановка проблеми**

У всьому цивілізованому світі на сьогодні приділяється значна увага питанню захисту інформації та вже визнана зручність та необхідність використання електронного цифрового підпису. Наша держава, обравши чіткий курс на євроінтеграцію та підписавши низку угод, узяла на себе зобов'язання у короткій строк максимально наблизити національне законодавство до європейського щодо послуг транскордонної сертифікації та створення умов для визнання взаємосумісності електронного цифрового підпису. Важливість цього кроку обумовлена активною співпрацею України з іноземними партнерами, а в епоху інформаційного суспільства питанню електронного діловодства та вирішення справ за допомогою новітніх засобів швидкого передання інформації у просторі надається велика увага. У зв'язку з цим вельми актуальним залишається питання правового регулювання сучасних засобів підпису документів «на відстані» та відносин, що виникають при використанні цифрового підпису як на державному рівні, так і між партнерами у сфері бізнесу, при оформленні будь-яких документів чи укладенні угод. Втім, аналіз правової бази вітчизняного законодавства дає підстави стверджувати: вона не відповідає світовим стандартам, а тому потребує переробки або розробки нових законодавчих актів задля мети технічної сумісності з міжнародними стандартами та утвердження довіри до України на світовій арені.

### **Аналіз останніх досліджень і публікацій**

Сучасні проблемні питання теорії та практики застосування електронного цифрового підпису в інформаційних та інформаційно-телекомунікаційних системах досліджено у монографії науковцями Ю.І. Горбенко та І.Д. Горбенко. Методи і алгоритми криптографічного захисту інформації в телекомунікаційних та інформаційних системах розроблено такими науковцями, як Г.В. Пухальська, А.А. Гринович, А.О. Мелашенко, О.Б. Кукарін та інші. Електронний цифровий підпис у правово-

му полі досліджували В.Б. Чередниченко, Н.В. Васильєва, О.А. Борисенко, О.О. Кузнецов, П.С. Клімушин та інші.

### **Не вирішені раніше частини загальної проблеми**

З розвитком інформаційно-комп'ютерних технологій вдосконалення набувають засоби, що дають можливість пов'язувати інформацію з конкретною фізичною або юридичною особою з метою забезпечення цілісності такої інформації, надання їй юридичного значення, в якості демонстрації авторських прав на інформацію та можливості встановлення правил доступу та її використання. Швидкість змін, що відбувається в комп'ютерних технологіях, з одного боку та зміни до вимог до якості електронного діловодства з іншого призводить до появи постійних неузгодженостей між правовими нормами та технічною реальністю. В деяких випадках чинне національне законодавство також не вкладається в площину міжнародно-правових вимог, що стає причиною різного кола проблем (невідповідності термінів у правових джерелах, рівнем експертних знань в цьому питанні тощо).

### **Формулювання цілей статті**

Основною ціллю статті є аналіз чинного національного законодавства України та міжнародних вимог в площині визначення поняття та умов застосування електронного цифрового підпису.

### **Вклад основного матеріалу дослідження**

Поняття «електронний цифровий підпис» визначено відповідно до п. 2 ст. 1 Закону України «Про електронний цифровий підпис» як вид електронного підпису, що отриманий в результаті криптографічного перетворення набору електронних даних і який додається до цього набору або логічно з ним поєднується та дає змогу підтвердити його цілісність та ідентифікувати підписувача [1]. Втім, для країн Євроспільноти фундаментальним для тлумачення поняття «електронний цифровий підпис» визнається положення ст. 2 Директиви «Про порядок використання електронних

підписів в Європейському співтоваристві» (1999) (далі – Директива), відповідно до якої електронний цифровий підпис – це данні в електронному форматі, що долучені до інших електронних даних, або логічно асоціюються з ними та служать в якості методу встановлення автентичності [2]. З цих визначень помічається певна розбіжність до підходу розуміння електронного цифрового підпису. Так, національне законодавство робить акцент на «ідентифікації (пізнюлат. *identifico* – ототожнюю) підписувача», що за загальним розумінням має два основних значення: усвідомлення чи розпізнання чогось або когось та ототожнення з кимось або чимось. Міжнародна ж спільнота використовує термін «автентичність» (від дав.-гр.  $\alpha$   $\theta$ εντικός – справжній, доказ походження), який стосується даних в електронному документі. Такі розбіжності передусім пов'язані з тим, що в міжнародно-правових документах в якості електронного цифрового підпису можуть служити біометричні дані людини, запис її голосу або фотографія чи будь-які «паролі», коди автентичності, що слугують для визначення особи, що створила документ та/чи яка його підписує. В Україні ж визнається лише один вид електронного підпису – криптографічного перетворення набору електронних даних. Слід мати на увазі ще таку специфіку: поняття електронного цифрового підпису як таке призначене не лише для використання в юридичному полі, воно також не прикріплене до будь-якої конкретної технології, оскільки для розпізнавання електронного підпису можуть бути використані не лише асиметричні системи, а й симетричні та такі, що взагалі не використовують криптографічні алгоритми.

Таким чином, виникає багато сумнівів щодо доцільності застосування терміна «підпис» до загальної конструкції «електронний підпис», оскільки вищезазначені методи можуть використовуватись не лише в якості обов'язкового реквізиту електронного документа – підпису, як це прийнято щодо паперових документів, а може використовуватись в якості паролю доступу (наприклад, до бази даних). Але

ж «пароль» не може бути в якості підпису, він виконує лише функцію використання його в якості надання особі певних повноважень, що мають бути закріплені за певною особою (хоча в реалії можуть бути і передані комусь іншому). Окрім того, хотілося б наголосити на неадекватності використання терміна «електронний цифровий підпис» у правовій сфері та його прирівнюванні до підпису людини від руки на папері. По-перше, конструкція «електронний цифровий підпис» – це «данні в електронному форматі» (основа механізму-криптографії), що покликані гарантувати цілісність електронного документа, тоді як рукописний підпис не може гарантувати незмінності змісту документа. По-друге, між електронним документом та електронним цифровим підписом простежується досить складна взаємодія, що залежить від строку дії сертифікатів, наявності секретного та відкритого ключів, до того ж місцезнаходження самого електронного цифрового підпису може бути не тільки наприкінці документа, а й на початку, та й взагалі у додатково прикріпленому файлі.

Відповідно до ч. 1. ст. 6 Закону України «Про електронні документи та електронний документообіг» електронний підпис може використовуватися в якості ідентифікації автора електронного документа [3]. Правові основи для застосування електронних документів регулюються також Цивільним кодексом України, відповідно до якого при здійсненні правочинів допускається застосування електронно-цифрового підпису (ст. 207) [4]. Законом також визначено, що тільки електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки), але з певними обмеженнями: електронний цифровий підпис повинно бути підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису; якщо під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису; особистий ключ підписувача повинен відповідати відкритому ключу,

зазначеному у сертифікаті. Також зазначено, що електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа [1, ст.3]. Втім, незважаючи на такі умови, Європейська модель застосування електронного цифрового підпису має в своєму правовому арсеналі та використовує на практиці три види кваліфікованих підписів, тоді як в Україні застосовується лише один найпростіший [5].

Для правового поля актуальним залишається питання використання електронного цифрового підпису в якості доказової інформації. Чіткі правила відносно документів – доказів – розраховані на те, що дотримання їх буде підвищувати надійність документа, надаватиме йому беззаперечності та слугуватиме в якості підвищення правової визначеності в суді. Визначальним в якості доказу по справі слугує питання достовірності документа. Існуючий ДСТУ 4145-2002 установлює механізм цифрового підписування, оснований на властивостях груп точок еліптичних кривих над полями, та правила застосування цього механізму до повідомлень, що пересилаються каналами зв'язку та/або обробляються у комп'ютеризованих системах загального призначення. Застосування цього стандарту гарантує цілісність підписаного повідомлення, автентичність його автора та неспростовність авторства [6]. Достовірність електронного документа визначається саме цифровим підписом, який може бути перевірений за допомогою сертифікатів та відкритого ключа. Втім, достовірність такого документа може бути втрачена, якщо на момент підписання спливає час дії сертифіката або сертифікат було анульовано.

Для досягнення такої мети, як використання електронного документа в якості доказу, на перший план мають виноситися питання цілісності даних в електронному документі, взаємна автентифікація сторін та автентифікація джерела інформації. При цьому має бути: 1) чітка відповідність правових положень можливостям науки та техніки; 2) можливість швидкої

перевірки у разі необхідності питань, що можуть стосуватися справи: «чи є підпис автентичним, тобто чи належить він саме конкретній людині?», «чи є документ достовірним?», «чи була можливість підробки?», «чи відповідають данні в електронному документі оригіналу та чи могли б вони бути змінені в наступному?» тощо.

На відміну від електронного цифрового підпису, в якості доказової інформації для власноручного підпису характерні такі доказові функції: 1) ідентифікації особи, що підписувала документ (а отже брала безпосередню участь у процесі підписання); 2) встановлення зв'язку особи зі змістом документа. Втім, наявність власноручного підпису особи на документі та ідентифікація особи, що його поставила, не завжди свідчать про достовірність самого документа, оскільки особа, до прикладу, може і не мати права засвідчувати оспорюваний документ. Таким чином, в Україні, як і в більшості цивілізованих країн, правом передбачено певні процедури, виконання яких надає безспірності або додаткової юридичної сили власноручному підпису (нотаріальне засвідчення документа, засвідчення факту свідками, обов'язковість печатки на підписі тощо). Такі юридичні процедури передбачають «неможливість відмови» від власного підпису в майбутньому. Разом з тим, чим більше ставиться вимог до надійності документа, тим полегшується для сторін можливість знаходити різні лазівки у випадках втрати інтересу до договору (наприклад, комерційного) заради мети ухилятися від виконання вимог за договором. Таким чином, прагнучи до підвищення надійності обмінних електронними документами, потрібно враховувати ймовірні ризики ухилення недобросовісними особами від перейнятих на себе зобов'язань. Пошук збалансованого підходу на основі норм і стандартів, визнаних на міжнародному рівні і придатних для трансграничного застосування, є важливим питанням у виробленні політики в галузі міжнародної електронної торгівлі. І для досягнення цієї мети в Україні вже відбулися помітні зрушення. Відповідно до Закону України «Про стандартизацію»

Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» були розроблені національні стандарти України, гармонізовані з міжнародними та європейськими нормативними документами (чинні з 1 січня 2016 року), серед яких вже діє стандарт ISO/IEC 10181-4, в якому визначається декілька типів сервісу «неможливість відмови від авторства» [7].

Відповідно до ч. 1 ст. 5 Закону України «Про електронний цифровий підпис» встановлено, що органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, державні реєстратори прав на нерухоме майно, державні реєстратори юридичних осіб, фізичних осіб – підприємців та громадських формувань, нотаріуси для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа [1]. Проте спеціального правового регулювання щодо посиленого сертифіката в Україні поки ще немає, тоді як європейською Директивою встановлені спеціальні вимоги до так званого «просунутого підпису»: такий підпис має бути унікальним чином пов'язаний з особою, що їм володіє (сигнатарієм); повинен створюватися на основі засобів, що знаходяться під одноосібним контролем сигнатарія; повинен бути пов'язаний з даними, до яких він відноситься таким чином, що будь-яка подальша зміна даних буде неминуче виявлена. Окрім того, у ст. 5 Директиви наголошено, що державичлени зобов'язані створювати такі умови, за яких «просунуті електронні підписи» разом із захищеним облаштуванням створення підпису і діючими сертифікатами відповідали б правовим вимогам, що пред'являються до підпису в електронній формі аналогічно підпису, зробленому на папері від руки. Рекомендації щодо надійного посвідчення підпису викладені також у Додатку IV до Директиви [2].

Відповідно до ч. 2 ст. 4 Закону України «Про електронний цифровий підпис» визначено, що електронним цифровим підписом можуть користуватися як фізичні,

так і юридичні особи – суб'єкти електронного документообігу для ідентифікації підписувача електронного документа та підтвердження цілісності даних в електронній формі [1]. В законі не йдеться про відповідальність провайдерів за розголошення особистих даних фізичної особи (сигнатарія), а також відомостей про переміщення чи знаходження особи. Відповідно до ст. 8 зазначеного вище закону на центр сертифікації ключів покладено зобов'язання лише «забезпечувати захист персональних даних, отриманих від підписувача» [1].

Загалом в Україні помітні позитивні зрушення щодо впровадження і розвитку електронного документообігу. Для прикладу, вже з 2014 року Державною фіскальною службою України впроваджено сервіс «електронний кабінет платника податків», який надає можливість підприємцям створити свій персональний кабінет, в якому фізична та юридична особа на безоплатній основі та використовуючи електронний цифровий підпис може надіслати електронним листом не лише податкову звітність, а й переглядати дані картки особового рахунка про стан розрахунків з бюджетом, формувати та заповнювати платіжні документи тощо [8], що додало чимало зручностей суб'єктам підприємницької діяльності: оперативність та можливість дистанційного опрацювання та накопичення інформації.

### **Висновки**

Україна обрала шлях успішного та надійного партнерства з державами, що входять до Європейського Союзу, і для успішної співпраці використовувани в країні технології і правові форми повинні відповідати уніфікованим загальноєвропейським вимогам, або не повинні їм суперечити. Правова неврегульованість електронного цифрового підпису є причиною відсутності сталої однакової понятійної бази і термінології в цій сфері. Насамперед, вбачається за необхідне ввести зміни до Закону України «Про електронний цифровий підпис», а саме:

1. Поняття «Електронний цифровий

підпис» сформулювати відповідно до Директиви – це дані в електронному форматі, які додаються до інших електронних даних або логічно асоціюються з ними і служать в якості методу встановлення автентичності.

2. Вести поняття «сигнатарій» – особа

що володіє засобом відтворення підпису і виступає або від свого імені, або від імені фізичної або юридичної особи, або ж організації, яку представляє.

Окрім того, важливим є юридичне визнання електронних цифрових підписів в якості доказів у судочинстві в усіх державах – членах Європейського Союзу.

### **Література**

1. Закон України «Про електронний цифровий підпис» від 22.05.2003 р. № 852-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 276 .
2. Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures // Official J. European Communities. OJ L 13. – 19.01.2000. – P. 12.
3. Закон України «Про електронні документи та електронний документообіг». [Електронний ресурс]. – Режим доступу: <http://zakon1.rada.gov.ua/laws/show/851-15>;
4. Цивільний кодекс України від 16.01.2003 № 435-IV // Відомості Верховної Ради України. – 2003. – №№ 40-44. – Ст. 356.
5. Кузнецов О.О. Захист інформації в інформаційних системах :навч.посіб. / О.О. Кузнецов, С.П. Євсєєв, О.Г. Король. – Х.: Вид-во ХНЕУ, 2011. – 512 с.
6. ДСТУ 4145-2002 «Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння» Державний комітет України з питань технічного регулювання та споживчої політики. – 28.12.2002. – № 31. [Електронний ресурс]. – Режим доступу: <http://www.dssu.gov.ua>.
7. Електронні підписи й інфраструктури (ESI). Алгоритми і параметри безпечних електронних підписів. Частина 2. Протоколи безпечних каналів і алгоритми засобів створення підписів (ETSI TS 102176-2:2005, IDT): ДСТУ ETSI TS 102 176 – 2. – [Чинний від 2011-07-01]. – К.: Держспоживстандарт України, 2011. – (Національний стандарт України).
8. Державна фіскальна служба України: офіційний веб-портал. [Електронний ресурс]. – Режим доступу: [sfs.gov.ua/elektronna-zvtnist](http://sfs.gov.ua/elektronna-zvtnist).