УДК 34.096
DOI https://doi.org/10.32782/2524-0374/2021-11/114

АКТУАЛЬНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ПІДПИСУ

THE CURRENT STATE OF THE LEGAL REGULATION OF THE USE OF ELECTRONIC SIGNATURE

Крикавська І.В., к.ю.н.,
старший викладач закладу вищої освіти
кафедри адміністративного та інформаційного права
Інститут права, психології та інноваційної освіти
Національного університету «Львівська політехніка»

Ткачук Л.В., студентка IV курсу
Інститут права, психології та інноваційної освіти
Національного університету «Львівська політехніка»

Стаття присвячена висвітленню однієї з актуальних проблем інформаційного права щодо питання використання електронного підпису. Основна мета застосування електронного підпису – це спрощення та прискорення документообігу між суб'єктами господарювання, органами державної влади й місцевого самоврядування та громадянами в широкому розумінні. Масове використання електронного підпису дасть змогу створити сприятливі умови для функціонування бізнесу, налагодити безконтактний спосіб спілкування між фізичними та юридичними особами й державними органами та звести нанівець роль людського фактору, а отже, уникнути корупції. Перелік документів, необхідних для отримання електронного цифрового підпису юридичною особою, ФОП і фізичними особами, є різним. Для отримання електронного цифрового підпису необхідно звернутися до Акредитованого центру сертифікації ключів. У статті проаналізовано тлумачення поняття «електронний підпис» у міжнародних нормативно-правових актах, національному законодавстві й досліджено підходи до його тлумачення науковцями та юристами-практиками. Проаналізовано нормативно-правове регулювання цифрового підпису Законами України «Про електронні документи та документообіг», «Про електронні довірчі послуги». Детально досліджено процедуру отримання цифрового підпису в Акредитованого центру сертифікації ключів і за допомогою Bank ID. На прикладі додатку Приват24, що є сервісом надання онлайн послуг Акціонерного товариства комерційного банку «Приватбанк», розглянуто процедуру надання електронного підпису банком.

Розглянуто такі проблемні питання, як захист закритих ключів від пошкодження, модифікації, зміни; відсутність чіткої нормативно-правової бази регулювання системи електронного документообігу та стандартизації процесу накладення й перевірки електронного підпису.

Ключові слова: електронний підпис, електронні документи, електронні довірчі послуги, сертифікація ключів.

The article is devoted to one of the current issue of information rights on the use of electronic signature. The main purpose of the use of electronic signatures is to simplify and accelerate the flow of documents between business entities, public authorities and local governments and citizens in a broad sense. Mass use of electronic signatures will create favorable conditions for business, establish a contactless way of communication between individuals and legal entities and government agencies and nullify the role of the human factor, and thus avoid corruption. The list of documents required to obtain an electronic digital signature by a legal entity, private individual and individuals is different. To obtain an electronic digital signature necessary apply to Accredited center of key certification. The article is analyzed interpretation the concept of "electronic signature" in international regulations, national legislation and researched approaches to its interpretation by scholars and legal practitioners. It is analyzed the normative regulation of digital signature in laws "On electronic documents and document flow", "About electronic trust services". The procedure for obtaining a digital signature is possible with Accredited center of key certification and with BankID. On the example of the application Privat24, which is a service for providing online services of the Joint-Stock Company of the commercial bank "Privatbank", the procedure for providing an electronic signature by the bank is considered.

Such problematic issues as: protection are consideredprivate keys from damage, modification, change; lack of clear regulatory framework for regulating the system of electronic document management and standardization of the process of overlay and verification electronic signature.

Key words: electronic signature, electronic documents, electronic trust services, key certification

Постановка проблеми. Глобалізаційні процеси, розвиток інформаційного суспільства й інформаційно-комунікативних технологій створюють нові виклики перед суб'єктами публічного управління. Сьогодні розвиток суспільства характеризується постійним збільшенням обсягів інформації, яка потребує оперативної та якісної обробки, оскільки є основою для прийняття обґрунтованих управлінських рішень. Ефективним вирішенням цієї проблеми є застосування інформаційних технологій і перехід до електронного урядування. Разом із переходом до використання ІТ виникає необхідність легалізації документів, що подаються он-лайн.

Широкого застосування електронний підпис набув у період карантинних обмежень у зв'язку з необхідністю дистанційної роботи. Вагомий вплив на масове використання електронного підпису здійснила програма діджиталізації публічних послуг і портал «Дія» – інформаційно-телекомунікаційна система, яка організаційно та функціонально складається з реєстру адміністративних послуг, електронного кабінету, мобільного додатка порталу «Дія (Дія)», інших підсистем і програмних модулів.

Мета статті – дослідження актуальних питань правового регулювання використання цифрового підпису й виявлення питань, що потребують удосконалення інструментів нормативного забезпечення безпроблемного використання цифрового підпису.

Аналіз останніх досліджень і публікацій. Проблему електронного підпису в працях досліджували Т. Мельник «Електронний документообіг та електронний підпис», А. Спірко, А. Прокопенко «Впровадження та ефективне використання електронного документообігу та електронного підпису в Україні: проблеми, нові можливості, шляхи розвитку», С. Рудзілевич «Нове у використанні електронного цифрового підпису» та ін.

Виклад основного матеріалу. З метою глибшого розуміння сутності поняття електронного підпису першочергово варто розглянути його тлумачення в міжнародних нормативно-правових актах, національному законодавстві й дослідити підходи до його тлумачення науковцями та юристами-практиками.

Комісією ООН з права міжнародної торгівлі, ЮНСІТРАЛ затверджено у 2001 році Типовий закон ЮНСІТРАЛ про електронний підпис. У цьому міжнародному нормативному документі визначено, що електронний підпис – це дані в електронній формі, які містяться

в комунікаційному повідомленні, приєднані до нього або логічно пов'язані з ним, і які можуть бути використані для ідентифікації підписанта, так указуючи на його згоду з повідомленням даних [1].

Ще одним серед міжнародних нормативних документів, що регулюють питання електронного підпису, є Регламент 910/2014 Європейського парламенту та Ради від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку і скасування Директиви 1999/93/ЕС, який набув чинності 1 липня 2016 року. У вказаному акті зазначено, що електронні підписи – це дані в електронній формі, які логічно пов'язані з іншими дійсними в електронній формі й використовуються як підпис підписантом [2].

На національному рівні питання електронного підпису регулюється низкою нормативно-правових актів, зокрема в Законі України «Про електронні довірчі послуги» .

Теоретично електронні підписи, які практично застосовуються, поділяють за рівнем довіри на прості, удосконалені і кваліфіковані. Однак лише кваліфікований електронний підпис здійснює електронну ідентифікацію підписанта, виявляє порушення цілісності електронних даних і дає можливість підписати електронні документи, оскільки документи з накладенням лише такого електронного підпису мають таку саму юридичну силу, як і підписані власноруч.

Законом України «Про електронні довірчі послуги» кваліфікований електронний підпис визначено як удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису й базується на кваліфікованому сертифікаті відкритого ключа.

Серед науковців немає єдиного підходу до тлумачення поняття електронного цифрового підпису.

Наприклад, І. Свидорук зазначає, що електронний підпис у найзагальнішому розумінні – це низка символів, які дають змогу точно ідентифікувати носія цього «підпису» та забезпечити те, щоб інформація, що міститься в документі, не змінювалася [3].

М. Дутов уважає, що термін «електронний цифровий підпис» означає дані, надіслані разом із текстом повідомлення, отримані шляхом певних алгебраїчних перетворень тексту, надісланого «приватним ключем» відправника, який може бути відомий лише йому [4].

Застосування електронного підпису для легалізації правочинів прямо передбачено в законодавстві України.

Частиною 1 ст. 205 Цивільного кодексу України передбачена можливість укладання договору за допомогою підписання його електронним підписом. Відповідно до ч. 1 ст. 205 Цивільного кодексу України, правочин може бути вчинений усно або письмово (електронно). Правочин уважається вчиненим у письмовій формі, якщо його зміст зафіксовано в одному або кількох документах (у тому числі в електронній формі), у листах, телеграмах, якими обмінюються сторони [5].

Відповідно до ст. 6 Закону України «Про електронні документи та документообіг», створення електронного документа завершується накладенням електронного підпису. Згідно зі ст. 7 цього Закону, оригінальним електронним документом є електронна копія документа з обов'язковими реквізитами, у тому числі електронним підписом автора або підписом, прирівняним до власноручного підпису [6].

Використання електронного цифрового підпису означає, що для кожного підпису існують унікальні ключі (паролі), один із яких може лише шифрувати документ – закритий ключ, а інший – лише розшифрувати – відкритий ключ. При підписанні електронного документа електронним цифровим підписом використовується закритий ключ, який шифрує електронний документ. Закритий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписанту. На другому етапі використання електронного цифрового підпису електронний документ надсилається його одержувачу, який повинен мати відкритий ключ, що дає змогу лише розшифрувати документ. Відкритий ключ – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний сторонам у сфері електронного цифрового підпису [2].

Перелік документів, необхідних для отримання електронного цифрового підпису юридичною особою, ФОП і фізичними особами, є різними. Для отримання електронного цифрового підпису необхідно звернутися до Акредитованого центру сертифікації ключів.

Акредитований центр сертифікації ключів забезпечує дотримання вимог щодо надання послуг електронного цифрового підпису; надає допомогу під час генерування приватних і відкритих ключів на запит і вживає заходів для забезпечення безпеки інформації під час її генерації; використовує надійні засоби електронного цифрового підпису, програмно-технічних засобів, засобів криптографічного захисту інформації відповідно до вимог Департаменту Держспецзв'язку та захисту інформації й Управління юстиції [7].

Під час формування сертифіката акредитований центр присвоює унікальний реєстраційний номер сертифікату; перевіряє унікальність відкритого ключа підписанта в реєстрі чинних, блокованих і скасованих сертифікатів; включає дані про обмеження використання електронного цифрового підпису; включає електронну адресу електронного інформаційного ресурсу, де публікується список відкликаних сертифікатів акредитованого центру; на вимогу підписанта включає додаткові дані.

Сертифікат підписанта, сформований акредитованим центром, чинний не більше ніж два роки. Тобто термін дії кваліфікованого електронного цифрового підпису не перевищує 2 років. Потім необхідно проходити процедуру отримання спочатку [8].

Також існує спосіб отримати електронний підпис у режимі онлайн за допомогою Bank ID. Така послуга, наприклад, доступна в особистому кабінеті додатку Приват24, що є сервісом надання онлайн послуг Акціонерного товариства комерційного банку «Приватбанк»: по-перше необхідно авторизуватися в додатку «Приват24»; у меню «Сервіси» вибрати «Бізнес», «Електронний цифровий підпис фізичних осіб»; потім необхідно підтвердити правильність даних; наступним кроком буде створення й підтвердження паролю за допомогою SMS-повідомлення з кодом підтвердження; після цього електронний підпис автоматично завантажиться на комп'ютер [9].

Інші державні органи за необхідності й за погодженням із Кабінетом Міністрів України визначають свої центри сертифікації. Національний банк України має право створити центр сертифікації для забезпечення реєстрації, сертифікації відкритих ключів та акредитації центрів сертифікації ключів. Центральним засвідчувальним органом, відповідно до Постанови Кабінету Міністрів України «Про затвердження Положення про центральний засвідчувальний орган» від 28 жовтня 2004 року, є Міністерство юстиції України [10].

Перевірка електронного цифрового підпису – це операція, що виконується одержувачем захищеного електронного документа за допомогою відкритого ключа підписанта. Для виконання цієї операції необхідно отримати відкритий ключ відправника та захищений документ. Відповідний програмний модуль перевіряє, чи дійсно цифровий підпис відповідає документу й відкритому ключу. Якщо в документ або відкритий ключ унесено якісь зміни, перевірка закінчується з негативним результатом [11].

Через таку структуру цифровий підпис цифрового підпису має проблеми із захистом від фальсифікації. Зловмисник може отримати доступ до приватного ключа тим чи іншим способом: будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання приватного ключа. Це, у свою чергу, ставить під загрозу елек-

тронний підпис, створений за допомогою приватного ключа. Секретний ключ можна підробити різними способами. Традиційні способи компрометації зазвичай пов'язані з крадіжками та різними іншими протиправними діями. Але це дає змогу певною мірою очікувати, що охорона ключа нехай і опосередковано, але передбачена законом [12].

На жаль, це не стосується нетрадиційних методів компрометації, заснованих на реконструкції приватного ключа на основі даних, отриманих у реальних умовах, зокрема за допомогою відкритого ключа й перехоплення секретного повідомлення, доступу до конфіденційної інформації [12].

Іншою проблемою впровадження електронного документообігу з використанням цифрового підпису для вітчизняних підприємств є відсутність чіткої законодавчої бази, яка б регулювала систему електронного документообігу та стандартизувала процес накладення й перевірки цифрового підпису. Україна нескінченно далека від запровадження систем, які не дають змоги нам перейти від «паперової епохи», дорогою, неефективною та неконкурентоспроможною є невідповідність. Це пов'язано з тим, що відсутність єдиної державної політики та координації призвела до повного хаосу в системах електронного урядування. В одній податковій адміністрації електронний документообіг забезпечується трьома ключовими центрами сертифікації, які не сумісні між собою; незахищена програмна платформа. Українські підприємства є абсолютно незахищеними базами даних, оскільки створюються на основі імпортного програмного забезпечення в різних форматах кодування; нелегітимність чинної системи видачі цифрових підписів. Із січня 2009 року Центральний засвідчувальний орган офіційно не уповноважений видавати підписи, оскільки він не відповідає вимогам безпеки, а дію указу, інертного до міністрів, що регулює його роботу, частково призупинено [12].

Проблему захисту закритих ключів від пошкодження, модифікації, зміни можна вирішити за допомогою сертифікатів. Сертифікат – це електронний сертифікат, який установлює зв'язок між сертифікатом підпису та власником підпису й ідентифікує особу [11].

За використання сертифікованих засобів криптографічного захисту інформації гарантом якості виконання основної функції та відсутності публічних дій є Департамент спеціальних телекомунікаційних систем захисту інформації Служби безпеки України. При використанні несертифікованих засобів криптографічного захисту інформації таких гарантій ніхто дати не може, тобто використання сертифікатів значно знижує ризик фальсифікації ключів.

Щодо другої проблеми, яка пов'язана з відсутністю чіткої нормативно-правової бази щодо регулювання системи електронного документообігу та стандартизації процесу накладення й перевірки цифрового підпису, науковцями розроблено пропозиції та рекомендації щодо її подолання.

На державному рівні варто уніфікувати програмне забезпечення й розробити єдині стандарти якості, які б гарантували інформаційну безпеку зберігання та передачі даних, що використовуються для електронного підпису.

Деякі вчені також підкреслюють, що центр сертифікації ключів є критичним елементом у системі застосування цифрового підпису. Неналежна організація послуг цифрового підпису та/або незабезпечення належного рівня оперативної безпеки, захисту інформації чи збій зазначеного суб'єкта можуть створити умови, які сприятимуть масовому зловживанню під час використання цифрового підпису [7].

Суб'єктами є користувачі послуг цифрового підпису, зокрема фізичні та юридичні особи незалежно від форм власності. Зазначимо, що ключові сертифікаційні центри виконують функції технологічного посередника в системі електронного документообігу, учасниками якого можуть бути суб'єкти господарювання й органи державної влади. Діяльність центрів сертифікації ключів без суворого дотримання законодавства в цій сфері (припускає, зокрема, ненавмисне порушення встановленого порядку виконання своїх функцій) може призвести до сприятливих умов для господарських та адміністративних спорів щодо електронних документів унаслідок неналежного використання механізмів ЕЦП [7].

Для реалізації завдання органів державної влади у сфері електронного документообігу необхідно мати всі об'єктивні передумови: належну правову основу; юридично значущий електронний цифровий підпис і можливість його надання персоналу; розвинену телекомунікаційну інфраструктуру; політичну волю керівника органу; відповідні відомчі стандарти та програму впровадження електронного документообігу; відповідну систему забезпечення проходження електронних документів; потужне технічне оснащення реєстраторів; постійне навчання персоналу [13].

Висновки. Отже, основна мета застосування електронного підпису – це спрощення та прискорення документообігу між суб'єктами господарювання, органами державної влади й місцевого самоврядування та громадянами в широкому розумінні. Масове використання електронного підпису дасть змогу створити сприятливі умови для функціонування бізнесу, налагодити безконтактний спосіб спілкування між фізичними та юридичними особами й державними органами та звести нанівець роль людського фактору, а отже, уникнути корупції. Але для цього передусім необхідно законодавчо врегулювати систему електронного документообігу, а також розробити стандарти, які дадуть змогу спростити процес накладання й перевірки цифрового підпису.

ЛІТЕРАТУРА

1. Цивільний кодекс України від 16 січня 2003 року № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 03.11.2021).
2. Про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС : Регламент Європейського Парламенту і Ради (ЄС) від 23 липня 2014 року № 910/2014. URL: https://zakon.rada.gov.ua/laws/show/984_016-14#Text (дата звернення: 06.11.2021).
3. Про електронні довірчі послуги : Закон України від 5 жовтня 2017 р. № 2155. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 06.11.2021).
4. Про внесення змін до деяких законодавчих актів України щодо функціонування платіжних систем та розвитку безготівкових розрахунків : Закон України від 18 вересня 2012 р. № 5284-VI. URL: (дата звернення: 07.11.2021).
5. Про електронні документи та документообіг : Закон України від 22 травня 2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 07.11.2021).
6. Про електронні підписи : Типовий закон ЮНСІТРАЛ від 5 липня 2001 р. URL: https://zakon.rada.gov.ua/laws/show/995_937#Text (дата звернення: 09.11.2021).
7. Азарова А.О., Роїк О.М., Года К.О. Електронний цифровий підпис як засіб захисту інформації на вітчизняних підприємствах. *Економічний простір.* 2012. № 60. С. 258–263.
8. Дутов М. Правові проблеми електронного документообігу. *Право України.* 2002. № 6. С. 122–124.
9. Іванов А.І. Нормативно-правове регулювання використання електронного цифрового підпису. *Вісник Пенітенціарної асоціації України*. 2018. № 1 (3). С. 39–46.
10. Лужецький В.А., Войтович О.П., Дудатьєв А.В. Інформаційна безпека : посібник. Вінниця, 2009. 240 с.
11. Свидрук І. Правове забезпечення електронної торгівлі. *Підприємництво, господарство і право.* 2001. № 10. С. 35–40.
12. Отримати електронний підпис КЕП (ЕЦП) легко. URL: https://onlinebank.dp.ua/publications/861-kep-online-privat24/ (дата звернення: 06.11.2021).
13. Електронний документообіг: досвід головдержслужби України. URL: http://www.softline.kiev.ua/ua/elektronnij-dokumentoobig/634-elektronnij-do kumentoobig-dosvid-golovderzhsluzhbi-ukrajini (дата звернення: 10.11.2021).