БІОМЕТРИЧНИЙ ПІДПИС ЧИ ЕЛЕКТРОННИЙ
ЦИФРОВИЙ ПІДПИС: ПЕРЕВАГИ

Державно-управлінські студії № 6, 2019

УДК 351.004.9

В.П. Писаренко,
доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування Полтавської державної аграрної академії

БІОМЕТРИЧНИЙ ПІДПИС ЧИ ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС: ПЕРЕВАГИ

V. Pysarenko,
Doctor of Science in Public Administration, professor, professor of Public Administration and Administration of Poltava State Agricultural Academ

BIOMETRIC SIGNATURE OR ELECTRONIC DIGITAL SIGNATURE: ADVANTAGES

Анотація. *Стаття присвячена можливостям використання електронного цифрового підпису при підписанні електронних документах органів державного та публічного управління, органів місцевого самоврядування та рішенням проблеми авторства безпаперового документа, яке може бути досягнуто з використанням електронного цифрового підпису, як засобу, що дозволяє на основі криптографічних методів надійно встановити авторство і справжність документа. Уявленню про електронний цифровий підпис як аналог власноручного підпису, на думку багатьох фахівців у галузі права, заснованому лише на схожості виконуваної цими видами підпису функцій посвідчення.*

Проаналізовано переваги та недоліки використання електронного цифрового підпису та необхідність створення повноцінної інфраструктури цифрового підпису, яка сьогодні вимагає внесення змін до законодавства про цифровий підпис. Означено напрями впровадження альтернативних засобів ідентифікації особистості при підписані електронних документів, а саме біометричного цифрового підпису.

Ключові слова: *електронний цифровий підпис, електронний документ, органи публічного управління, центр сертифікації ключів, ідентифікація особистості, біометричний цифровий підпис.*

Annotation. *The article is devoted to the possibilities of using electronic digital signature when signing electronic documents of state and public*

administration bodies, local governments and solving the problem of authorship of a paperless document, which can be achieved using electronic digital signature as a means to reliably establish authorship based on cryptographic methods. the authenticity of the document. The idea of an electronic digital signature as an analogue of a handwritten signature, according to many experts in the field of law, based only on the similarity of the functions of the certificate performed by these types of signatures.

The advantages and disadvantages of using an electronic digital signature and the need to create a full-fledged digital signature infrastructure, which today requires changes in the legislation on digital signatures, are analyzed. The directions of introduction of alternative means of identification of the person at signing of electronic documents, namely biometric digital signature are defined.

Keywords: *electronic digital signature, electronic document, public administration bodies, key certification center, personal identification, biometric digital signature.*

Постановка проблеми. Збільшення обсягів інформації в усьому світі і бурхливий розвиток новітніх інформаційних технологій зумовило появу нових можливостей для їх використання в житті суспільства. Крім того, змінилася і сама роль інформації, яка стає найбільш цінним ресурсом.

Впровадження комп'ютерних технологій для обробки, передачі зберігання і використання інформації зумовило створення документів на принципово нових носіях, що, у свою чергу, викликало появу таких понять як електронний документ або документ в електронній формі.

Порядок застосування електронних документів і складу їх посвідчення вимагали законодавчого оформлення, і з середини 1990–х років багато країн світу приступили до розробки законів, мета яких надати юридичну силу електронним документам і зробити можливим їх використання нарівні з паперовими документами.

Постановка проблеми. Питання використання електронних документів продовжують цікавити науковців різних країн світу і сьогодні, незважаючи на прийняття цілого ряду законодавчих актів у цій галузі, багато проблем залишилися все ще невирішеними і потребують додаткового регулювання як на законодавчому, так і на нормативно-методичному рівні.

Аналіз останніх досліджень і публікацій. Науковці по різному тлумачать поняття - цифровий підпис. Електронний цифровий підпис А. В. Ткачов розглядає, як юридичну категорію і вважає, що вживання в нормативних документах таких виразів як - аналог власноручного підпису і рівнозначний власноручному підпису особи, є небажаними, так як заплутують учасників правовідносин і може породжувати процесуальні труднощі при ідентифікації осіб, які використовували електронний цифровий підпис для засвідчення комп'ютерних документів [1, с.8].

Рішення проблеми авторства безпаперового документа може бути досягнуто лише з використанням електронного цифрового підпису, що визначається Л. А. Сисоєвою як «…засіб, що дозволяє на основі

криптографічних методів надійно встановити авторство і справжність документа» [2, с.47].

У Законі України "Про електронний цифровий підпис" який визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису терміни "електронний підпис" вживається як дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних, а «електронний цифровий підпис» як вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа [3].

Причиною такої позиції є те, що електронний цифровий підпис дозволяє встановити лише факт її створення за допомогою певного закритого ключа, на відміну від власноручного підпису, що несе інформацію про індивідуальні ознаки автора. Висновок про тотожність автора документа з володарем закритого ключа заснований на припущенні, що він відомий тільки його власникові, але це положення може бути спростовано. Тому уявлення про електронний цифровий підпис як аналог власноручного підпису, на думку багатьох фахівців у галузі права, засноване лише на схожості виконуваної цими видами підпису функції посвідчення.

Формулювання цілей статті. Аналіз можливостей використання електронного цифрового підпису при електронному документуванні в діяльності органів публічного управління та використання альтернативних методів ідентифікації особистості при підписані електронних документів.

Виклад основного матеріалу. Підготовка України до вступу в ЄС потребує змін діючого законодавства та розробки нових правових актів щодо впровадження електронного документообігу. Позиція ЄС щодо правового регулювання документів електронного документообігу включає в себе досягнення деяких результатів - це головним чином розробку подібних законів у незалежних державах, які суттєво розрізняються правовими системами та традиціями. Для того, щоб усвідомити всю складність питання, необхідно пам'ятати, що мета Європейського Співтовариства полягає не в створенні однакового законодавчого порядку, а в сприянні торгівлі, розвитку інвестиційної діяльності і свободи пересування громадян. Тому, незважаючи на присутність гармонізації законодавства, до певної міри, вона представляється лише одним із засобів досягнення головної мети, і вже ніяк не є самою метою.

Однією з основних переваг, яку несе впровадження систем електронного документообігу для конкретного співробітника, що працює з документами це можливість за допомогою електронного цифрового підпису захистити документи від несанкціонованого доступу.

Ще однією проблемою є необхідність забезпечення юридичної сили електронних документів. Але чим далі, тим частіше ця проблема може вирішуватися як звичайна організаційно-технічна задача. Завдяки тому, що нарешті прийнятий закон, який регулює використання електронного цифрового підпису (ЕЦП), стало можливим надання електронним документам юридичного статусу.

Електронний цифровий підпис це - реквізит електронного документа, призначений для його захисту від підробки.

Інфраструктура цифрового підпису забезпечує:

можливість ідентифікації особи, що висловила свою волю шляхом складання електронного документа (авторство документа) або підтверджує факт ознайомлення з документом (віза на документі, штамп нотаріуса, відмітка про ознайомлення і т.п.);

можливість забезпечення конфіденційності документообігу.

Електронний цифровий підпис в електронному документі є рівнозначним власноручному підпису в документі на паперовому носії і це підтверджено чинним законодавством.

ЕЦП можливо отримати в результаті криптографічного перетворення інформації з використанням закритого ключа. Безумовно, складність математичного апарату двохключевої криптографії, за допомогою якої реалізується механізм ЕЦП, велика.

Система електронного документообігу органу виконавчої влади повинна відповідати вимогам п.3.7 Технічних умов (ТУ У 30.0-33240054-001:2005) [4], щодо комплексу засобів захисту інформації від несанкціонованого доступу [5, с. 26-31]. Слід визначити ключові властивість цифрового підпису. Це можливість надання юридичної значимості електронним повідомленням. Саме цифровий підпис надає статус електронного документа різним файлам, що містять інформаційний контент. Крім того, цифровий підпис дозволяє передавати електронні документи в незмінному вигляді і доводити в суді їх авторство.

Для повноцінного функціонування цифрового підпису потрібне створення серйозної інфраструктури, яка отримала визнання у світі під назвою "інфраструктура відкритих ключів" чи PKI (*public key infrastructure*) - в міжнародній термінології. Всі розвинені країни світу, в тому числі Україна, формують подібні національні інфраструктури.

Створення повноцінної інфраструктури цифрового підпису сьогодні вимагає внесення змін до законодавства про цифровий підпис що встановлюють:

обов'язок органів державної влади, державних організацій, їх посадових осіб супроводжувати цифровим підписом документи та допускати їх в обіг, приймати документи від громадян та їх об'єднань в електронній формі в супроводі цифрового підпису;

вимоги до засвідчувальних центрам, які здійснюють посвідчення відкритих ключів цифрового підпису, що застосовуються з метою забезпечення юридичної значимості та / або конфіденційності

документообігу між сторонами, якщо принаймні одна з цих сторін є органом державної влади;

обов'язок органів державної влади засвідчити відкритий ключ цифрового підпису для застосування в документообігу між цим органом та громадянином або організацією на вимогу цього громадянина або організації;

обов'язок органів державної влади розкривати і офіційно публікувати свої відкриті ключі цифрового підпису;

відповідальність засвідчувальних центрів відкритих ключів цифрового підпису за помилки в посвідченні ключів, а також органів державної влади та їх посадових осіб за компрометацію власних закритих ключів цифрового підпису;

стандарти, що забезпечують сумісність ключів цифрового підпису і цифрового підпису, і стандартів, що забезпечують заданий рівень стійкості ключів цифрового підпису і цифрового підпису;

вимоги щодо розробки та введення в дію альтернативних стандартів, заснованих на прийнятих в зарубіжних країнах алгоритмах і форматах даних і забезпечують сумісність з існуючою міжнародною інфраструктурою цифрового підпису;

вимоги до розробки відкритих програм, що еталонно реалізують стандарти цифрового підпису.

У відповідності до Закону України «Про електронний цифровий підпис» [3], за відсутності можливості накладання та перевірки електронного цифрового підпису (ЕЦП) за допомогою посиленого сертифіката (що зумовлене відсутністю акредитованих центрів сертифікації ключів, які мають право видавати такі сертифікати), для надання юридичного статусу електронному документу, підписаному ЕЦП, учасники документообігу можуть діяти в межах договору про визнання ЕЦП, чинність якого засвідчується без використання посиленого сертифіката. Оскільки кількість учасників досить велика і укладення угод між кожним з них є досить складним і незручним процесом, можливо доцільно забезпечити договірні засади електронного документообігу на основі договору приєднання. Такий договір складається однією стороною - ініціатором документообігу (координатором), решта бажаючих долучитися до системи приєднуються до нього шляхом надання координатору заповненої форми-картки (механізм підписання договору може бути визначеним окремо). Після укладення договору сторони діють у відповідності до нього і підписані електронним цифровим підписом електронні документи мають юридичний статус. Таким чином, організовується певна корпоративна мережа електронного документообігу.

Для забезпечення абонентів корпоративної мережі електронного документообігу послугами електронного цифрового підпису кожен з абонентів користується послугами Центра сертифікації ключів (ЦСК). Для цього абонент укладає із ЦСК угоду про надання послуг ЕЦП у формі договору приєднання. При цьому кожен абонент (або уповноважена ним особа) має прибути до ЦСК особисто із документами, які підтверджують

відомості, які вносяться у сертифікат ключа, або передати їх за допомогою кур'єрської доставки (порядок сертифікації та перелік документів визначено відповідними документами ЦСК).

Таким чином, для здійснення захищеного документообігу кожен абонент має здійснити наступні кроки:

встановити на своєму комп'ютері спеціальне програмне забезпечення для генерації ключів ЕЦП, яке надається центром сертифікації ключів, та згенерувати пару ключів ЕЦП та пару ключів шифрування. Особистий ключ ЕЦП залишається у абонента, а відкритий ключ у формі заявки на сертифікацію надається до ЦСК;

провести сертифікацію свого відкритого ключа у ЦСК, при цьому надати всі необхідні документи, які підтверджують відомості, що вносяться до сертифікату ключа;

встановити на своєму комп'ютері спеціальне програмне забезпечення для накладання та перевіряння ЕЦП, яке надається центром сертифікації ключів.

Для підписання та шифрування електронних документів необхідно використовувати свій особистий ключ, а для перевірки та розшифрування документів, отриманих від інших учасників системи - використовувати сертифікати ключів цих абонентів.

Кожен раз, при отриманні підписаного та зашифрованого документу, пересвідчуватися у чинності сертифіката абонента, який його підписав. Для цього необхідно звертатися до спеціального ресурсу ЦСК - таблиці чинних сертифікатів. Якщо сертифікат підписанта не є чинним на час створення документу - такий документ не є дійсним.

У цій методології і для шифрування, і для розшифровки відправником та одержувачем застосовується один і той же ключ, про використання якого вони домовилися до початку взаємодії. Якщо ключ не був скомпрометований, то при розшифровці автоматично виконується ідентифікація відправника, так як тільки відправник має ключ, за допомогою якого можна зашифрувати інформацію, і тільки одержувач має ключ, за допомогою якого можна розшифрувати інформацію. Так як відправник і одержувач - єдині люди, які знають цей симетричний ключ, при компрометації ключа буде скомпрометовано тільки взаємодію цих двох користувачів. Проблемою, яка буде актуальна і для інших криптосистем, є питання про те, як безпечно поширювати симетричні (секретні) ключі.

Висновки. Як бачимо, використання електронного цифрового підпису має безліч проблем та деякі взагалі не вирішені питання, що суттєво впливають на можливість її використання. З огляду на вищеперераховане пропонується розглянути, як альтернативний, принципово новий метод засвідчення особистості при підписанні електронних документів на основі біометричних засобів ідентифікації, заснований на фізіологічних характеристиках людини, тобто на унікальних характеристиках, даних йому від народження - малюнку папілярних ліній пальців. Необхідно нормативно узаконити термін - біометричний цифровий підпис, надати йому статус -

рівнозначного власноручному підпису в документі на паперовому носії. Біометрія дозволяє незаперечно ідентифікувати особистість, і цю інформацію неможливо підробити або виправити. Це значно спрощує та здешевлює електронний документообіг так як відпадає необхідність створення інфраструктури цифрового підпису.

Список використаної літератури:

1. Ткачев Л.В. Правовой статус компьютерных документов: основные характеристики. М., 2000, С. 8.
2. Сысоева Л.Л. Проблемы организации электронного визирования документов в системах электронного документооборота // Делопроизводство. 1998. № 2. С.47.
3. Закон України "Про електронний цифровий підпис" від 22 травня 2003 року № 852-IV// Відомості Верховної Ради України. 2003. № 36. Ст. 276.
4. Система електронного документообігу органу виконавчої влади. Технічні умови. ТУ У 30.0-33240054-001:2005.
5. Чирський Ю. Електронний цифровий підпис: правові аспекти застосування // Довідник секретаря та офіс-менеджера. №1(2007) С. 26-31.

References:

1. Tkachev L. (2000) Pravovoy status kompyuternykh dokumentov: Osnovnyye kharakteristiki. [Pravovoy status of computer documents: Basic characteristics]. Moscow, 2000, p 8.[Russia]
2. Sisoeva L. L. (1998) [Problemy elektronnoy organizatsii vyzyvaniya dokumentov v sistemakh elektronnogo dokumentooborota] Problems electron organization vyzyrovanyya documents in electronic document systems // Deloproyzvodstvo. 1998. № 2. p.47.[Ukraine]
3. Law of Ukraine (2003) Ob elektronnoy tsifrovoy podpisi [«On electronic digital signature»] on May 22, 2003 № 852-IV // Supreme Council of Ukraine. - 2003. - № 36. - Art. 276. [Ukraine]
4. (2005) Sistema elektronnogo dokumentooborota ispolnitel'nogo organa. Kharakteristiki [The system of electronic document executive body. Specifications] TU 30.0-33240054-001: 2005. [Ukraine]
5. J. Chyrskyy (2007) Elektronnaya podpis: pravovyye aspekty [Digital Signature: legal aspects of] // Handbook secretary and office manager. - №1 (2007) - P. 26-31. [Ukraine]