**Зміст**

Вступ

Розділ 1. Електронний цифровий підпис в цивільному праві України

1.1 Поняття та ознаки електронного цифрового підпису

1.2 Переваги електронного цифрового підпису та документообігу

Розділ 2. Правове регулювання використання електронного цифрового підпису

2.1 Регулювання електронного цифрового підпису нормами права: міжнародний досвід

2.2 Становлення українського законодавства про цифровий підпис

Розділ 3. Електронний цифровий підпис в цивільному обігу

3.1 Використання електронного цифрового підпису при здійсненні електронних правочинів

3.2 Проблеми вдосконалення використання електронного цифрового підпису

Розділ 4. Електронний цифровий підпис та документообіг в державній податковій службі

4.1 Використання електронного цифрового підпису в роботі органів державної податкової служби

4.2 Вдосконалення подання платниками податків податкової звітності в електронній формі

Висновок

Список використаних джерел

**Вступ**

Чи завжди ми відрізняємо електронний документ від документа в електронному вигляді? В електронному документі інформація, зафіксована за допомогою електронних даних, має включати обов’язкові реквізити документа, найголовнішим з яких є електронний підпис. Тобто без електронного підпису за певних вимог документ не має юридичної сили і не може вважатися електронним документом.

Електронний документообіг є одним із тих інструментів, які в змозі забезпечити потреби сьогодення в швидкому інформаційному обміні. А використання електронного цифрового підпису, що підтверджує оригінальність документа і надійно захищає його від підробок, – ефективне рішення для всіх, хто не хоче чекати приходу кур’єрської пошти за багато сотень кілометрів, щоб перевірити дійсність отриманої інформації або підтвердити факт укладення договору. Документи можуть бути засвідчені електронним цифровим підписом і передані до місця призначення протягом декількох секунд, адже електронний документ передається за допомогою швидкісних телекомунікаційних систем, однією з яких є, наприклад, Інтернет. За таких умов усі учасники обміну електронними документами незалежно від відстані мають однакові можливості в електронному інформаційному обміні.

Отже, можна сказати, що документообіг з використанням електронного цифрового підпису невдовзі посяде домінуюче місце у системі опрацювання, підготовки, підписання та надсилання документа, оскільки традиційні схеми: розроблення проекту документа в електронному вигляді, створення паперової копії для підпису, пересилання паперової копії з підписом, розгляд паперової копії, перенесення її на комп’ютер – є малоефективними, трудомісткими та такими, що потребують забагато часу.

Запропоновані інформаційні технології дають можливість фізичним особам, підприємствам та організаціям, суб’єктам господарювання більш ефективно і творчо вирішувати економічні та соціальні проблеми. Отже, актуальність курсової роботи не викликає сумніву.

Мета курсової роботи – дослідити правові основи використання електронного цифрового підпису в цивільному обігу України.

Для досягнення поставленої мети слід вирішити наступні завдання:

- визначити сутність та ознаки електронного цифрового підпису;

- описати переваги використання електронного цифрового підпису;

- навести міжнародний досвід правового регулювання електронного цифрового підпису;

- охарактеризувати становлення українського законодавства про цифровий підпис;

- описати можливості використання електронного цифрового підпису при здійсненні електронних правочинів;

- визначити проблеми вдосконалення використання електронного цифрового підпису.

Предмет курсової роботи – регулювання використання електронного цифрового підпису нормами права.

Об’єкт курсової роботи - електронно-цифровий підпис у цивільному обігу.

**Розділ 1. Електронний цифровий підпис в цивільному праві України**

**1.1 Поняття та ознаки електронного цифрового підпису**

Електронний цифровий підпис – це блок інформації, який прикріпляється до файлу даних автором і захищає файл від несанкціонованої модифікації та вказує на власника підпису, використовується фізичними та юридичними особами як аналог власноручного підпису для додання електронному документу юридичної сили, відповідає юридичній силі документа на паперовому носії, підписаного власноручним підписом правомочної особи, та скріпленого печаткою.

Варто звернути увагу на трактування електронного підпису в країнах Євросоюзу. Так, Директива 1999 /93/ ЄС Європейського парламенту та Ради від 13 грудня 1999 року «Про систему електронних підписів» надає два

терміни [15]:

- електронний підпис – це «дані, подані в електронній формі, які додаються чи логічно поєднуються з іншими електронними даними та які служать в якості методу засвідчення достовірності»;

- «удосконалений електронний підпис», що означає електронний підпис, який відповідає певним вимогам, а саме, знаходиться під повним контролем особи, яка його ставить, і пов’язаний винятково із цією особою, дозволяє за підписом ідентифікувати особу і пов’язаний з даними таким чином, що будь-яку зміну даних після додавання підпису можна виявити.

Електронний цифровий підпис є якісно новим етапом в розвитку сучасного документообігу. Сертифікати електронного цифрового підпису, згідно Закону «Про електронний цифровий підпис», який вступив у дію з 1 січня 2004 року, мають однакову силу з власноручним підписом особи. Використання електронного цифрового підпису в системі електронного документообігу істотно прискорює проведення численних комерційних операцій, скорочує об’єми паперової бухгалтерської документації, економить час співробітників і витрати підприємства, пов’язані з укладенням договорів, оформленням платіжних документів, наданням звітності в контролюючі органи, отриманням довідок від різних держустанов.

Підробити ЕЦП, створений акредитованим сертифікаційним центром, неможливо.

Метою застосування систем цифрового підпису є автентифікація інформації – захист учасників інформаційного обміну від нав’язування хибної інформації, встановлення факту модифікації інформації, яка передається або зберігається, й отримання гарантії її справжності, а також вирішення питання про авторство повідомлень. Система цифрового підпису припускає, що кожен користувач мережі має свій таємний ключ, який використовується для формування підпису, а також відповідний цьому таємному ключу відкритий ключ, відомий решті користувачів мережі й призначений для перевірки підпису. Цифровий підпис обчислюється на основі таємного ключа відправника інформації й власне інформаційних бітів документу (файлу). Один з користувачів може бути обраним в якості «нотаріуса» й завіряти за допомогою свого таємного ключа будь-які документи. Решта користувачів можуть провести верифікацію його підпису, тобто пересвідчитися у справжності отриманого документу. Спосіб обчислення цифрового підпису такий, що знання відкритого ключа не може призвести до підробки підпису. Перевірити підпис може будь-який користувач, що має відкритий ключ, в тому числі незалежний арбітр, якого уповноважено вирішувати можливі суперечки про авторство повідомлення (документу) [17].

З січня 2004 року вступив в дію прийнятий парламентом закон «Про електронні документи і електронний документообіг», в якому чітко визначені поняття, сфери застосування і юридична сила електронних документів і електронного документообігу.

Електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа. Електронний документ може бути створений, переданий, збережений і переведений електронними засобами у візуальну форму.

Законом України «Про електронні документи та електронний документообіг» встановлено основні організаційно-правові засади електронного документообігу та використання електронних документів. Так, за визначенням, електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа, зокрема електронний цифровий підпис (ст. 5). Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Проте Закон встановлює певні обмеження на застосування електронного документа як оригіналу. В електронній формі не може бути створено оригінал свідоцтва про право на спадщину; інший документ, який згідно із законодавством може бути створений лише в одному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів (ст. 8 Закону).

Як уже зазначалося, обов’язковим реквізитом електронного документа є електронний цифровий підпис – 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 (ст. 1 Закону «Про електронний цифровий підпис»).

Особистий ключ відомий лише його володільцеві. Відкритий ключ доступний всім учасникам електронного документообігу. Такий ключ включається до сертифіката відкритого ключа та може розповсюджуватись в електронній формі або у формі документа на папері.

Засвідчення чинності відкритого ключа здійснюється шляхом формування сертифіката відкритого ключа – документа, що видається центром сертифікації ключів. Посилений сертифікат відкритого ключа видається акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом.

Зазначена особливість дає можливість поряд із звичайним електронним цифровим підписом виділити цифровий підпис, підтверджений посиленим сертифікатом відкритого ключа.

Сертифікат відкритого ключа містить [4]:

- найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);

- позначку, що сертифікат виданий в Україні;

- унікальний реєстраційний номер сертифіката ключа;

- основні дані (реквізити) підписувала-власника особистого ключа;

- дату і час початку та закінчення строку чинності сертифіката;

- відкритий ключ;

- найменування криптографічного алгоритму, що використовується власником особистого ключа;

- інформацію про обмеження використання підпису.

Посилений сертифікат відкритого ключа, крім обов’язкових даних, які містяться в сертифікаті відкритого ключа, повинен мати ознаку посиленого сертифіката відкритого ключа. Інші дані можуть вноситися у посилений сертифікат ключа на вимогу його власника

Юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом відкритого ключа, а також використовувати електронний цифровий підпис без сертифіката відкритого ключа.

Розподіл ризиків збитків, що можуть бути заподіяні підписувачам, користувачам та третім особам, які застосовують електронні цифрові підписи без сертифіката відкритого ключа, визначається суб’єктами правових відносин у сфері послуг електронного цифрового підпису на договірних засадах.

Щодо органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій державної форми власності, то для них законодавець встановив імперативну (обов’язкову) норму, згідно з якою зазначені організації можуть застосовувати електронний цифровий підпис лише за умови використання надійних засобів електронного цифрового підпису, що повинно бути підтверджено сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, отриманим на ці засоби від спеціально уповноваженого центрального органу виконавчої влади у сфері криптографічного захисту інформації, та наявності посилених сертифікатів відкритих ключів у своїх працівників-підписувачів.

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) лише в тому разі, якщо:

- електронний цифровий підпис підтверджено з використанням посиленого сертифіката відкритого ключа за допомогою надійних засобів цифрового підпису;

- під час перевірки використовувався посилений сертифікат відкритого ключа, чинний на момент накладення електронного цифрового підпису;

- особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

Для порівняння: у Німеччині, за законодавством, електронний цифровий підпис не прирівнюють до власноручного підпису; у Франції, навпаки, згідно зі статтею 1316 Цивільного кодексу, сторонам надається право вибору, оскільки в суді як докази визнаються (допускаються) літери та цифри чи будь-який інший знак або символ, значення (зміст) якого може бути з’ясовано незалежно від способу створення та передачі [12, с.25-28].

Підробити електронний цифровий підпис, а разом з ним і засвідчений документ неможливо, адже це потребуватиме величезної кількості обчислень, які, як вважається, не можуть бути реалізовані за сучасного рівня математики й обчислювальної техніки за прийнятний час, тобто поки інформація, що міститься в підписаному документі, є актуальною. Додатковий захист від підробки забезпечує центр сертифікації, який серед іншого цілодобово приймає заяви про скасування, блокування та поновлення сертифікатів ключів.

**1.2 Переваги електронного цифрового підпису та документообігу**

Електронний цифровий підпис може використовуватися юридичними і фізичними особами як аналог власноручного підпису для надання електронному документу юридичної сили. Юридична сила електронного документа, підписаного ЕЦП, еквівалентна юридичній силі документа на паперовому носієві, підписаного власноручним підписом правомочної особи та скріпленого печаткою.

Електронний цифровий підпис володіє всіма основними функціями власноручного підпису [18]:

- засвідчує те, що отриманий документ надійшов від особи, що підписала його;

- гарантує цілісність і захист від виправлень підписаного документа;

- не дає можливості особі, яка підписала документ, відмовитися від зобов’язань, що виникли в результаті підписання цього електронного документа.

Безпека використання ЕЦП забезпечується тим, що засоби, які використовуються для роботи з ЕЦП, проходять експертизу і сертифікацію в Департаменті спеціальних телекомунікаційних систем СБУ, яка гарантує неможливість зламу і підробки ЕЦП.

Переваги ЕЦП:

- юридична сила електронних документів, підписаних ЕЦП, законами України прирівнюється до юридичної сили документів з власноручним підписом або друком, а також створює правову основу для застосування ЕЦП і здійснення юридично значущих дій шляхом електронного документообігу.

- конфіденційність і безпека інформації. Використовуючи ЕЦП, користувач дістає додаткову можливість шифрування документів. Завдяки надійним криптографічним алгоритмам забезпечується конфіденційність інформації, яка має на увазі неможливість доступу до неї будь-якої особи.

- безпека використання ЕЦП забезпечується тим, що програмне забезпечення, яке використовується для роботи з ЕЦП, пройшло експертизу і сертифікацію в Департаменті спеціальних телекомунікаційних систем СБУ, яка гарантує неможливість зламу і підробки ЕЦП.

- можливість ведення електронного документообігу з державними структурами та можливість використовувати одні і ті ж засоби ЕЦП при обміні даними зі всіма міністерствами, відомствами, при подачі звітності до будь-яких контролюючих органів на території України.

- удосконалення бізнес-процесів на підприємстві істотно скорочує об’єми паперової бухгалтерської документації, економить час співробітників і витрати підприємства, пов’язані з укладенням договорів, оформленням платіжних документів.

- ведення ділових відносин на сучасному рівні використання ЕЦП істотно прискорює проведення численних комерційних операцій, виключає необхідність додаткових зустрічей і багатогодинних переговорів.

- електронний цифровий підпис – ефективне рішення для всіх, хто хоче йти в ногу з новими вимогами часу. Документи, підписані електронним цифровим підписом, можуть бути передані до місця призначення протягом декількох секунд. Всі учасники електронного обміну документами дістають рівні можливості незалежно від їх віддаленості один від одного.

Електронний документообіг (оборот електронних документів) – сукупність процесів створення, обробки, відправки, передачі, отримання, збереження, використання і знищення електронних документів, які відбуваються із застосуванням перевірки цілісності і, у разі потреби, з підтвердженням факту отримання таких документів.

В Законі «Про електронні документи та електронний документообіг» указується, що обов’язковим реквізитом електронного документа є електронний цифровий підпис, який використовується для ідентифікації автора і/або підписувача електронного документа іншими суб’єктами електронного документообігу. Накладенням електронного підпису закінчується створення електронного документа.

При підписанні електронного документа його початковий зміст не змінюється, а додається блок даних – електронний цифровий підпис.

Отримання цього блоку можна розділити на два етапи:

На першому етапі за допомогою програмного забезпечення і спеціальної математичної функції обчислюється так званий «відбиток повідомлення» (message digest).

Цей відбиток має наступні особливості: фіксовану довжину, незалежно від довжини повідомлення; унікальність відбитку для кожного повідомлення; неможливість відновлення повідомлення по його відбитку.

Таким чином, якщо документ був модифікований, то зміниться і його відбиток, який відобразиться при перевірці електронного цифрового підпису.

На другому етапі відбиток документа шифрується за допомогою програмного забезпечення і особистого ключа автора.

Таким чином, обчислення відбитку документа захищає його від модифікації сторонніми особами після підписання, а шифровка особистим ключем автора підтверджує авторство документа.

Переваги використання електронного документообігу [18]:

- перехід до зручнішого, швидшого і економнішого безпаперового документообігу;

- удосконалення процедури підготовки, подачі/доставки, обліку і збереження документів, їх аутентифікація, цілісність, конфіденційність і неспростовність;

- криптографічний захист інформації (електронних документів) при їх передачі відкритими каналами;

- мінімізація фінансових ризиків за рахунок підвищення конфіденційності інформаційного обміну документами;

- економія ресурсів за рахунок використання оперативного електронного архіву;

- можливість швидкого пошуку і перегляду електронних документів, а також визначення їх юридичної сили по ЕЦП;

- значне скорочення процедури підписання договорів, оформлення і подачі податкової і фінансової звітності;

- швидкий і надійний обмін електронними документами з партнерами, контрагентами незалежно від віддаленості адресата.

**Розділ 2. Правове регулювання використання електронного цифрового підпису**

**2.1 Регулювання електронного цифрового підпису нормами права: міжнародний досвід**

Останнім часом ми спостерігаємо підвищену законодавчу активність в області правового регулювання електронного цифрового підпису (ЕЦП). Тільки протягом року в США, Австрії, Англії, Ірландії, Індії і Сінгапурі були прийняті закони, які стосуються електронного цифрового підпису. Деякі з них направлені безпосередньо на нормативно-правове регулювання застосування ЕЦП, інші – на нормативно-правове регулювання електронної комерції і застосування інформаційних технологій, зокрема ЕЦП. У 1997 році в Німеччині був прийнятий Закон «Про електронний цифровий підпис» (Singaturgesetz). Діють також міжнародні правові акти. Наприклад, Директива Європейського Парламенту і Ради № 1999/93/EC «Про загальні рамкові умови для електронних підписів» 1999 року (далі по тексту – Директива). Об’єктивною необхідністю для такого бурхливого розвитку нового напряму законодавства стала зміна характеру суспільних відносин в економіці, управлінні і банківській сфері, пов’язаного з широким впровадженням інформаційних технологій в сферу комунікацій. У зв’язку з цим виникло нове поняття – електронний документ. Він відрізняється від традиційного документа перш за все тим, що має не фізичну, а логічну природу. А це, у свою чергу, призводить до відриву властивостей документа від властивостей носія і, відповідно, до неможливості застосування таких традиційних реквізитів, як рукописний підпис, друк, бланк і захисні елементи бланка, при здійсненні різного роду операцій, зокрема договорів. Сьогодні, коли говорять про необхідність швидкого становлення законодавства про електронний цифровий підпис (ЕЦП), перш за все згадують Інтернет і електронну комерцію. Це дійсно важливі, але далеко не єдині його передумови. Питання правового регулювання застосування ЕЦП повинні відігравати не меншу роль і в забезпеченні внутрішнього документообігу підприємств, установ, адміністративних органів.

Вперше про електронний цифровий підпис заговорили ще в 60-70-х роках, хоча ні об’єктивних передумов і технічних умов, ні організаційних структур для повноцінного посвідчення особи автора електронного документа у той час ще не існувало. Під «електронним підписом» розуміли якусь послідовність символів, отриманих в результаті одностороннього перетворення документа (повідомлення) по відомому алгоритму.

Зарубіжні країни по-різному визначають ЕЦП, хоча основні, базові риси і властивості ЕЦП указуються в кожному законі. Держави – члени Європейського Союзу в своїх законодавчих актах наслідують прийняту в Європейському Союзі Директиву Європейського Парламенту і Ради

№ 1999/93/EС «Про загальні рамкові умови для електронних підписів». Відповідно до неї ЕЦП – це «дані в електронній формі, які прикладені до інших електронних даних або логічно з ними пов’язані і призначені для аутентифікації». Федеральний закон Німеччини «Про цифровий підпис» 1997 р., наслідуючи положення Директиви, практично повторює це визначення. Закон Ірландії «Про електронну комерцію» також практично повторює це визначення, додаючи лише, що дані в електронній формі (ЕЦП), включають розширені ЕЦП [16, с.23].

Федеральний закон Австрії «Про цифровий підпис» (Singaturgesetz) 2000 року визначає ЕЦП як «електронні дані, які додаються до інших електронних даних або пов’язані з ними іншим логічним способом і служать для аутентифікації змісту документа та ідентифікації особи, що підписала документ». У даному визначенні також зазначається, що ЕЦП служить не тільки для аутентифікації змісту електронного документа, але і для ідентифікації особи, що підписала документ.

Закон Великобританії «Про електронні комунікації» 2001 року дає наступне визначення ЕЦП: «Суть, що має електронну форму, включена в склад або іншим чином пов’язана з електронними даними і призначена для їх аутентифікації».

Федеральний закон США «Про електронні підписи в глобальній і національній торгівлі» 2000 р. визначає ЕЦП як «електронний звук, символ або процес, прикріплений або логічно пов’язаний з контрактом або іншим документом і здійснений або вибраний особою з наміром підписати документ». «Аутентифікація електронного документа за допомогою електронних методів або процесів відповідно до норми закону» - таке визначення міститься в Законі Індії «Про інформаційні технології».

Крім цього вказані нормативно-правові акти вводять додаткові визначення, наприклад, кваліфікований електронний підпис. Такі поняття вводяться в законодавчі акти для досягнення оптимального нормативно-правового регулювання. Під кваліфікованим ЕЦП розуміється звичайний ЕЦП, що задовольняє вимогам відповідного закону та інших нормативно-правових актів. Зокрема, в Директиві встановлено, що «держави - члени Європейського Союзу повинні піклуватися про те, щоб розширений підпис був створений захищеною системою засобів ЕЦП».

Якісні характеристики засобів ЕЦП і даних, які використовуються при його створенні, встановлюються національним законодавством держав - членів Європейського Союзу. Зокрема, такі вимоги встановлені законодавствами Ірландії, Німеччині і Австрії. У загальних рисах ці вимоги зводяться до необхідності захисту ключів, вживаних при створенні ЕЦП, від неправомірного їх використання третіми особами, які не володіють законними правами на них, а також від підробки. Що ж до засобів ЕЦП, то вони не повинні в процесі створення підпису змінювати зміст електронного документа або перешкоджати доступу власника підпису до даних, що містяться в електронному документі. Крім того, засоби ЕЦП повинні бути захищені від несанкціонованого доступу до них з боку третіх осіб.

Особливої уваги заслуговує питання доступності засобів шифрування і, зокрема, засобів ЕЦП. Зокрема, певним лібералізмом відрізняється регламентація порядку використання засобів ЕЦП в Німеччині. Відповідно до Принципів німецької політики в області шифрування, розроблених Федеральним Урядом, від 2 червня 1999 року, «Федеральний Уряд не має наміру забороняти вільну доступність засобів шифрування в Германії».

У Великобританії Законом «Про електронні комунікації» передбачено ліцензування діяльності, пов’язаної з шифруванням. Таке ліцензування здійснюється Державним секретарем (the Secretary of State), що створює і веде спеціальний реєстр, в якому міститься інформація про органи, що надають послуги в області шифрування інформації. Для отримання ліцензії необхідна відповідність ряду вимог технічного характеру, що встановлюються Державним секретарем. Вони стосуються якісних характеристик засобів ЕЦП. В цілому у Великобританії встановлені жорсткіші вимоги до засобів ЕЦП, ніж у Німеччині.

Законодавства зарубіжних держав регламентують діяльність системи засвідчувальних центрів. Зокрема, в Європейському Союзі Директивою засвідчувальний центр визначається як «орган або юридична або фізична особа, яка видає сертифікат або надає інші послуги, пов’язані з електронним цифровим підписом». Під сертифікатом розуміється «електронне посвідчення, за допомогою якого відбувається ідентифікація засобів перевірки підпису особи і підтвердження її особи». Крім того, Директива використовує поняття кваліфікованого сертифікату, тобто виданого відповідно до вимог закону та інших нормативно-правових актів.

Директива також встановлює вимоги до змісту сертифікату. Відповідно до Додатку № 1 до Директиви кваліфікований сертифікат повинен містити:

а) повідомлення, що даний сертифікат є кваліфікованим;

б) повідомлення засвідчувального центру і держави, що даний сертифікат діє;

в) ім’я особи, що звернулася за отриманням сертифікату відкритого ключа ЕЦП, або його псевдонім, який служить з метою ідентифікації особи;

г) місце для вказівки специфічних рис особи, яка звернулася для видачі сертифікату відкритого ключа ЕЦП, що використовується у разі потреби з метою визначення особи;

д) інформацію про засоби перевірки підписів, які відповідають засобам ЕЦП, що знаходяться під контролем особи, охочої отримати сертифікат відкритого ключа ЕЦП;

е) повідомлення про початок і кінець терміну дії сертифікату відкритого ключа ЕЦП;

ж) унікальний номер сертифікату;

з) розширену ЕЦП засвідчувального центру;

и) у разі потреби – обмеження території дії сертифікату;

к) у разі потреби – обмеження ціни операції, для якої може застосовуватися сертифікат.

Директива встановлює також ряд вимог до діяльності засвідчувальних центрів. Зокрема, даний центр винен:

а) довести наявність необхідної надійності для надання послуг з сертифікації;

б) забезпечити швидке і безпечне надання послуг з реєстрації, а також безпечне і негайне відкликання сертифікату відкритого ключа ЕЦП;

в) забезпечити точне визначення дати і часу видачі або відкликання сертифікату відкритого ключа ЕЦП;

г) перевірити відповідними засобами відповідно до права окремих держав особу і, у разі потреби, специфічні риси особи, яка звернулася за отриманням сертифікату відкритого ключа ЕЦП;

д) надати роботу персоналу, що володіє спеціальними знаннями, досвідом і кваліфікацією, особливо знаннями в області управління, технології і застосування ЕЦП, а також ґрунтовними знаннями в області процедур забезпечення достатньої безпеки;

е) дотримуватися в подальшому необхідних процедур управління та інших норм;

ж) застосовувати системи, що користуються довірою, і продукти, захищені від внесення змін, що забезпечують технічний і криптографічний захист відповідних процедур;

з) прийняти заходи проти фальсифікації сертифікатів, а у випадках, коли виробляються засоби і елементи ЕЦП, забезпечити конфіденційність даних при їх виробництві;

и) володіти достатньою кількістю фінансових коштів для роботи відповідно до вимог Директиви; мати змогу нести ризик відповідальності за збитки, наприклад в результаті укладення відповідних договорів страхування;

к) вказати всю відповідну інформацію про кваліфікований сертифікат і про термін його дії, для того, щоб, особливо в судовому процесі, можна було довести сертифікацію;

л) не дозволяти зберігання і копіювання засобів та елементів ЕЦП особам, які надають послуги з управління ключами ЕЦП;

м) інформувати власників сертифікатів про умови застосування сертифікату відкритого ключа ЕЦП, про існування вільної системи ліцензування засвідчувальних центрів, про процедури оскарження та погодження.

В цілому законодавства держав-членів ЄС, таких як Ірландія, Німеччина, Австрія, повторюють (деколи навіть структурно), за винятком деяких незначних змін в деталях, вимоги Директиви. У Німеччині і Австрії федеральними урядами прийняті відповідні ухвали про ЕЦП на виконання національних законодавчих актів. Національні законодавчі акти держав – членів ЄС по-різному регулюють процедуру ліцензування засвідчувальних центрів. Наприклад, Закон Ірландії «Про електронну комерцію» встановлює обов’язковість ліцензування діяльності засвідчувальних центрів. Таке ліцензування здійснюється міністром громадських підприємств (Minister for Public Enterprise). Закони Німеччини і Австрії «Про цифровий підпис» встановлюють добровільний порядок ліцензування засвідчвальних центрів. Істотною специфікою володіє також законодавство Великобританії. Закон «Про електронні комунікації» не передбачає діяльність центрів по посвідченню відкритих ключів ЕЦП, він лише говорить про посвідчення самого ЕЦП. Коротке нормативно-правове регулювання діяльності засвідчувальних центрів згідно цього закону зводиться до наступного:

а) передбачена сертифікація не відкритого ключа ЕЦП, а самого підпису;

б) особа може засвідчити підпис після того, як зробить заяву, що підпис, засоби його створення і перевірки, а також засоби і процеси зв’язку, що відносяться до ЕЦП, дійсно підтверджують незмінність даних і (або) умов зв’язку.

Таким чином, законодавство Великобританії дає можливість сторонам самим здійснювати посвідчення ЕЦП. Закон Індії «Про інформаційні технології» встановлює обов’язковість ліцензування діяльності засвідчувальних центрів одним уповноваженим державним органом – Керівником засвідчувальних центрів (Controller of Certifying Authorities). Ліцензія може бути видана засвідчувальному центру у разі задоволення вимог з кваліфікації і чисельності кадрів, фінансових ресурсів, інфраструктури. При здійсненні діяльності засвідчувальний центр зобов’язаний [16, с.25]:

а) використовувати програмне і апаратне забезпечення та процеси, захищені від неправомірного привласнення і зловживання;

б) забезпечити оптимальний ступінь надійності своїх послуг, достатній для їх надання;

в) дотримуватися захищених процесів для забезпечення конфіденційності ЕЦП, що завіряються;

г) дотримувати інші стандарти, встановлені іншими нормативно-правовими актами.

Закон Індії не встановлює вимог до змісту сертифікату. У США федеральне законодавство не регулює діяльність засвідчувальних центрів, але їх нормативно-правове регулювання здійснюється законодавством окремих штатів, хоча й не всіх. Зокрема, питання, пов’язані з інфраструктурою ЕЦП, регламентовані в таких штатах, як Айова, Міннесота, Міссурі, Род-айленд, Юта, Вермонт, Вашингтон. Законодавства зарубіжних держав не завжди встановлюють відповідальність за порушення режиму застосування ЕЦП. Норми про відповідальність можуть міститися в інших нормативно-правових актах, зокрема, кодифікованих (кримінальні, адміністративні кодекси і т.п.). Для держав - членів ЄС загальне регулювання відповідальності за порушення законодавства про ЕЦП здійснюється на основі Директиви.

Правове регулювання відповідальності за законом Індії «Про інформаційні технології» володіє значною специфікою. Зокрема, цей закон перераховує різні види злочинів в області застосування електронного цифрового підпису і встановлює різні види покарань. Тим самим він структурно нагадує кодифікований кримінальний акт. Суб’єктами перерахованих злочинів можуть бути як сторони по операції, що здійснюють застосування ЕЦП, так і засвідчувальний центр. Як приклад таких злочинів можна назвати: спотворення відомостей засвідчувальним центром для отримання ліцензії; порушення конфіденційності даних; обман при публікації сертифікату; публікація сертифікату з метою шахрайства. Як покарання передбачаються різні терміни позбавлення волі. Міжнародним регіональним законодавством ЄС і національними законодавствами держав-членів ЄС передбачається ряд випадків обмеження відповідальності засвідчувальних центрів. Зокрема, відповідно до Директиви, а також законодавств Ірландії, Німеччині, Австрії визначена можливість обмеження відповідальності. Таке обмеження може бути здійснене шляхом встановлення певного переліку операцій, при здійсненні яких можливе використання сертифікату, або на підставі вказівки суми операції, для якої застосовується сертифікат. При спричиненні стороні збитків у разі використання сертифікату в операції з сумою, яка перевищує вказану в сертифікаті, засвідчувальний центр відповідальності не несе. Федеральний закон Австрії також встановлює, що засвідчувальний центр не несе відповідальності перед іншими особами, якщо він доведе, що порушення обов’язків відбулося не з вини самого засвідчувального центру або його співробітників. Потерпілий, відповідно до закону, може посилатися на ту обставину, що обов’язки, встановлені законом, були порушені або мало місце недотримання вимог закону і прийнятих на його виконання інших нормативно-правових актів в області безпеки, а також якщо не були здійснені належні заходи. При цьому вказані обставини повинні привести до виникнення збитків у потерпілої сторони. Федеральний закон США «Про електронні підписи в глобальній і національній торгівлі», так само, як і Федеральний закон Німеччини, не містить яких-небудь положень про відповідальність, що випливає з правовідносин між партнерами по операції у зв’язку з неналежним застосуванням ЕЦП. Відповідальність, пов’язана із застосуванням ЕЦП, регулюється законодавством штатів. Зокрема, в Законі штату Юта (1996 р.) встановлюється відповідальність засвідчувального центру за невиконання або неналежне виконання зобов’язань. Відповідно до нього засвідчувальний центр несе відповідальність в межах, встановлених у сертифікаті відкритого ключа ЕЦП.

Згідно ст.46-3-308 Закону штату Юта засвідчувальний центр, за деякими виключеннями, не відповідає за [16, с.24]:

а) будь-який збиток, заподіяний фальшивим або сфальсифікованим підписом власника сертифікату відкритого ключа ЕЦП, якщо засвідчувальний центр діяв відповідно до вимог Закону;

б) спотворення в сертифікаті, помилку при його видачі при перевищенні меж відповідальності засвідчувального центру, вказаних в сертифікаті.

Із засвідчувального центру не можуть бути стягнуті штрафні санкції.

**2.2 Становлення українського законодавства про цифровий підпис**

У XXI ст. інформаційно-комунікаційні технології стануть провідним чинником, що істотно впливатиме на розвиток суспільства. Багато країн уже усвідомили ті переваги, які надає їхній розвиток та поширення. Нині в Україні є відчутною потреба унормувати нові відносини, що виникають у зв’язку з бурхливим розвитком комп’ютерних технологій.

Розвиток електронної комерції і електронного документообігу в Україні стикається з недостатністю правового регулювання застосування ЕЦП і електронного документообігу.

Правові основи для застосування електронних документів у цивільних відносинах уперше закладено новим Цивільним кодексом України, що набрав чинності з 1 січня 2004 р. згідно зі ст. 207 «Вимоги до письмової форми правочину»: «правочин вважається таким, що вчинений у письмовій формі, якщо воля сторін виражена за допомогою телетайпного, електронного або іншого технічного засобу зв’язку». Під час здійснення правочинів допускається застосування електронно-цифрового підпису. По суті, Цивільний кодекс України прирівнює електронні документи до паперових і допускає засвідчення їх електронним підписом [14, с.13].

На виконання рекомендацій Парламентських слухань з питань побудови інформаційного суспільства в Україні у державі створено нормативно-правове підґрунтя і технологічну основу функціонування юридично значимого електронного цифрового підпису. Законами України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV, а також «Про електронний цифровий підпис» від 22 травня 2003 року № 852-ІV встановлено основні організаційно-правові засади електронного документообігу та використання електронних документів, а також правовий статус електронного цифрового підпису (ЕЦП) та порядок його застосування юридичними і фізичними особами, визначено організаційну інфраструктуру ЕЦП та її суб’єктів. Передбачається послідовна розробка нормативно-правових актів, сфера регулювання яких визначається вперше, визначено необхідність підтримки функціонування центрального засвідчувального органу, як основного елемента інфраструктури електронного цифрового підпису.

На виконання вищеназваних законів протягом 2004 року прийнято шість постанов Кабінету Міністрів України (від 26 травня 2004 р. № 680, від 13 липня 2004 р. № 903, від 28 жовтня 2004 р. №№ 1451 - 1454), які стосуються сфер електронного документообігу та електронного цифрового підпису.

Дорученням Кабінету Міністрів України від 23.02.2005 № 6056/2/1-05 передбачалось створення центрального засвідчувального органу та забезпечення умов для акредитації центрів сертифікації ключів інфраструктури електронного цифрового підпису.

Постановою Кабінету Міністрів України від 6 травня 2005 р. № 324 «Про заходи щодо виконання у 2005 році Програми діяльності Кабінету Міністрів України «Назустріч людям» підтверджено необхідність прийняття цільової програми впровадження й розвитку електронного документообігу з використанням електронного цифрового підпису.

В Указі Президента України «Про першочергові заходи щодо впровадження новітніх інформаційних технологій» від 20 жовтня 2005 р. № 1497 одним із пріоритетних напрямків сфери інформаційних технологій визначено впровадження в Україні електронного документообігу із застосуванням електронного цифрового підпису.

Проте, жодним із вищезазначених законів та нормативно-правових актів не було передбачено конкретних заходів щодо створення, впровадження й утримання інфраструктури електронного цифрового підпису та не визначені механізми фінансування цих заходів.

З метою вирішення питань, які стосуються проблематики запровадження в Україні системи електронного урядування, 24 лютого 2003 року було прийнято Постанову Кабінету Міністрів України № 208 «Про заходи щодо створення електронної інформаційної системи «Електронний уряд».

Відповідно до цієї Постанови передбачено створити належні нормативно-правові засади функціонування системи «Електронний уряд», забезпечити умови для більш швидкого та доступного надання інформаційних послуг громадянам та юридичним особам шляхом використання електронної інформаційної системи «Електронний уряд», яка забезпечує: взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій, інтегрувати державні електронні інформаційні ресурси і системи в Єдиний веб-портал органів виконавчої влади.

Вдосконалення та оновлення нормативно-правової бази України, створення спеціальних юридичних норм сприятиме ефективному впровадженню та функціонуванню електронного документообігу та електронного цифрового підпису. Для регулювання правовідносин у сфері інформаційних технологій Верховна Рада України вже ухвалила кілька Законів України, які набули чинності:

- «Про електронні документи та електронний документообіг» від 22 травня 2003 р. № 851-IV;

- «Про електронний цифровий підпис» від 22 травня 2003 p. № 852-IV;

- «Про обов’язковий примірник документів» від 9 квітня 1999 p. № 595-XTV;

- «Про Національну програму інформатизації» від 4 лютого 1998 р. № 74/98-ВР;

- «Про телекомунікації» від 18 листопада 2003 p. № 1280-IV;

- «Про Національну систему конфіденційного зв’язку» від 10 січня 2002 р. № 2919-111;

- «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР.

Прийняття згаданих нормативно-правових актів, предметом регулювання яких є процеси електронного документообігу, дасть можливість створити сприятливі умови в сфері застосування сучасних інформаційних технологій, стимулювати в Україні розвиток ринку та інфраструктури послуг, що надають за допомогою засобів інформатизації.

В Україні порядок застосування засобів ЕЦП в порівнянні із зарубіжними країнами регламентований набагато жорсткіше. На даний час діє Указ Президента «Про заходи з дотримання законності в області розробки, виробництва, реалізації і експлуатації шифрувальних засобів, а також надання послуг в області шифрування інформації». Відповідно до нього заборонена діяльність юридичних і фізичних осіб, пов’язана з розробкою, виробництвом, реалізацією і експлуатацією шифрувальних засобів, а також захищених засобів зберігання, обробки і передачі інформації, наданням послуг в області шифрування інформації без ліцензій. Забороняється також використання державними організаціями і підприємствами в інформаційно-телекомунікаційних системах шифрувальних засобів, включаючи криптографічні засоби забезпечення достовірності інформації (електронний підпис), що не мають сертифікату. Така політика держави в області регулювання застосування і реалізації криптографічних засобів, у тому числі і засобів ЕЦП, мабуть, пояснюється прагненням використовувати тільки засоби, сертифіковані уповноваженими державними органами. Зміст нормативно-правових актів України, які регулюють застосування шифрувальних засобів, у тому числі і засобів ЕЦП, демонструє існуючу тенденцію встановлення «тоталітарного підходу» в цій справі. Безумовно, для вирішення безлічі проблем, пов’язаних з національною безпекою, необхідна наявність певних обмежень в області розробки, застосування і обороту засобів ЕЦП. Проте нав’язування продукції тільки одного або декількох виробників у цій області (а для самих виробників – обов’язкова платна сертифікація їх діяльності), особливо якщо воно супроводжується закритістю алгоритму, може у результаті призводити до посилення корупції і зниження справжньої, а не декларативної захищеності засобів ЕЦП. Правове регулювання застосування засобів ЕЦП повинно прагнути до більшої гнучкості у віддзеркаленні вимог об’єктивної дійсності. Можливо, враховуючи особливості України, було б доцільно розглянути багаторівневий підхід до визнання дійсності ЕЦП і ліцензування її засобів: одні вимоги – для адміністративної сфери, інші – для корпоративної і треті – для особистого документообігу. У зарубіжному законодавстві ми спостерігаємо окремі ознаки багаторівневого підходу, наприклад введення поняття кваліфікованого ЕЦП в Директиві [15, с.32].

Таким чином, проаналізувавши хід подій у сфері інформаційних правовідносин та інформатизації, зокрема, впровадження системи електронного документування в Україні, різноманітні документи та матеріали, можна зробити висновок, що у цьому напрямку здійснюються певні заходи. Можливо, не настільки інтенсивно, як в інших державах, але можна стверджувати, що через деякий час Україна, за умови системної правової та практичної розбудови системи електронного документування, також буде характеризуватися неабиякими здобутками у цій сфері.

**Розділ 3. Електронний цифровий підпис в цивільному обігу**

**3.1 Використання електронного цифрового підпису при здійсненні електронних правочинів**

Не зважаючи на те, що чинне українське законодавство не містить такого окремого поняття як «електронний правочин», українське законодавство дозволяє їх практичне вчинення. Зокрема, можливість вчинення електронних правочинів передбачена Цивільним кодексом України від 16 січня 2003 року. Під електронним правочином слід розуміти правочин, вчинений за допомогою електронних засобів комунікації, суть якого полягає в обміні сторонами за допомогою цього засобу електронними волевиявленнями. Ключовою відмінністю електронного правочину від традиційного, як випливає з вищенаведеного, є спосіб його вчинення. Таким чином, якщо для вчинення відповідного волевиявлення сторони використовують електронні засоби комунікації, ми розуміємо під таким правочином саме електронний правочин. При цьому не має значення чи обмін волевиявленнями, вчиненими в електронній формі відбувається on-line, чи за одночасної присутності сторін правочину, які надсилають волевиявлення через телеінформаційні мережі, наприклад Інтернет, чи наприклад вчинення такого правочину відбувається off-line, шляхом обміну інформаційними носіями із записаними текстовими файлами, що містять волевиявлення сторін.

Ми вважаємо, що при вирішенні питання, чи має даний правочин електронний характер, вагоме значення має також і спосіб його вчинення. Йдеться передусім про правочини, які вчиняються on-line (наприклад, купівля-продаж комп’ютерних програм, відео та аудіо матеріалів тощо). В наведених прикладах вчинення правочину, як і його виконання відбуваються в мережі. Отже, можна зробити висновок, що в такому випадку йдеться про електронний правочин sensu stricto, тобто електронний в момент укладення та виконання. Проте не слід забувати про випадки, коли вчинення правочину відбувається в електронній формі on-line чи off-line, а виконання відбувається традиційним способом. І такий правочин теж вважатиметься електронним. Таким чином, достатньо наявності хоча б одного критерію електронного вчинення правочину. Як слушно зауважує О. Гудзь, традиційний, матеріалізований спосіб виконання правочину не є базовим критерієм оцінки при вирішенні питання, чи є даний правочин електронним. Правочин вважається електронним і у випадку, коли фаза вчинення здійснюється традиційним способом, а виконання – в електронній (дематеріалізованій) формі. Необхідно зауважити, що існує ряд електронних правочинів, виконання яких можливе лише в електронній формі (наприклад, доступ до телеінформаційних мереж, доступ до баз даних, які існують лише в електронній формі тощо) та правочини, які можуть бути виконані лише традиційним способом (наприклад, купівля-продаж комп’ютерів, автомобіля тощо) [10, с.21].

З огляду на вищезазначені твердження, вважаємо за доцільне використання поняття «електронний правочин», адже поняття «правочин, вчинений в електронній формі», виключає зі сфери аналізу правочини, вчинення яких відбувається в традиційний спосіб, натомість виконання – в електронній формі.

Безумовно, різниця між традиційними та електронними правочинами виникає власне в способі обміну сторонами волевиявленнями, та іноді з огляду на спосіб виконання зобов’язання. Різниця полягає також і у методі комунікації сторін на етапі вчинення правочину, і часто, його виконання, зважаючи на те, які використовуються засоби комунікації на відстані, спосіб отримання інформації про сторону правочину, його зміст та спосіб виконання, ризики сторін, що випливають з вчинення електронного правочину, відсутності таких чинників як час та відстань, форма вчинення та виконання правочину.

Характерною рисою електронних правочинів є інтерактивність, безпосередність, мультимедійність пропозицій та реклами.

Інтерактивність полягає у індивідуалізації способу пересилання інформації між сторінками, які сприяють вчиненню правочину. Зокрема, йдеться про поступовий обмін інформацією від пасивного (через Інтернет - сторінки), до активного через надсилання детальної інформації електронною поштою.

Безпосередність електронних правочинів має найбільший вимір у випадку Інтернету, адже кожен має безпосередній доступ до глобальної мережі електронного переказу незалежно від часу та місцезнаходження. Очевидним є те, що надання послуг та товарів за допомогою мережі знижує затрати на здійснення трансакції, позбавляє необхідності особистого контакту, що за умов зростаючої глобалізації торгівлі має істотне значення.

Відсутність особистого контакту з контрагентом та товаром, який є предметом договору купівлі-продажу зумовлює створення різних методів мультимедійного представлення товару, шляхом використання фотографій, фільмів, обширного опису. Усе це покликано замінити безпосередній контакт продавця зі споживачем.

Вищенаведене свідчить, що проблемним є питання форми, в якій укладається електронний правочин.

В українській доктрині цивільного права погляди щодо електронної форми правочину різняться. Так, одні науковці, поділяючи підхід прийнятий в багатьох зарубіжних країнах, вважать, що електронна форма правочину є окремою формою правочину. Відповідно до цього підходу «письмова» та «електронна» форми є видовими щодо родового поняття, яким слід вважати «запис», тобто фіксацію змісту правочину на матеріальному або електронному носієві, який надає можливість зберігати інформацію про зміст правочину протягом тривалого часу і відтворити її на першу вимогу у формі, зрозумілій людині. На думку представників іншої позиції, зокрема

І. Спасибо-Фатєєвої, А. Чучковської та О. Ґудзь, правочин, вчинений з використанням електронних засобів зв’язку, є різновидом письмової форми. Так, І. Спасибо-Фатєєва вважає, що віднесення правочинів, вчинених за допомогою електронних засобів зв’язку, до письмових, слід розуміти як подання інформації (змісту правочину) на інших носіях, аніж папір, однак із фіксацією волі (думки, намірів) сторін через логічно упорядковані знаки. Матеріальним носієм буде комп’ютерний диск, із якого зчитується відповідна інформація через її сприйняття на моніторі або після роздрукування на папері. Тому електронно-цифрова форма є різновидом письмової форми з урахуванням специфіки мережі Інтернет. На думку

О. Гудзь, єдиною відмінністю електронного правочину є те, що він фіксується на віртуальному папері, а не на виробленому із переробленої деревини. Як слушно зазначає А. Чучковська, еволюція носія письмової форми не призводить до виникнення нової форми поряд із письмовою [11, с.24].

Відтак, поняття електронної форми правочину є спірним в доктрині цивільного права. Нерідко в літературі для визначення волевиявлення, вчиненого в електронній формі за допомогою електронних засобів комунікації вживається поняття «електронна форма». Виникає питання, чи на підставі українського законодавства доцільним є використання такого терміну, тобто чи законодавець приймаючи новий ЦК та Закон України «Про електронний цифровий підпис» ввів в українську правову систему нову електронну форму правочину, прирівнюючи її до звичайної письмової форми, чи лише обмежився встановленням двох видів, за допомогою яких суб’єкти можуть складати волевиявлення в письмовій формі, тобто шляхом складення власноручного або електронного підпису на документі.

Зазначимо, що текст електронних правочинів також може викладатися за допомогою писемності, загальновідомих умовних знаків, які розташовуються у певному порядку, змістом яких буде волевиявлення особи, спрямоване на набуття, зміну або припинення цивільних прав та обов’язків. Даний текст може мати всі реквізити документу. Передається указаний текст правочину за допомогою електронного зв’язку. Підписуватися може шляхом накладення електронного підпису, який ідентифікує підписувача і захищає документ від підробки. Єдиною відмінністю електронного правочину є те, що він фіксується на віртуальному папері, а не на виробленому із переробленої деревини.

Під електронним підписом, у принципі, може матися на увазі будь-який спосіб підписання електронного документа, зокрема графічне зображення рукописного підпису та звичайних паролів. Проте в Законі про ЕЦП наголошується на регулюванні відносин, пов’язаних з використанням одного різновиду електронного підпису – електронного цифрового підпису.

Його особливість полягає в тому, що він ґрунтується на алгоритмах криптографічного захисту інформації. ЕЦП накладається за допомогою особистого ключа – спеціального коду, відомого тільки особі, яка підписала документ. Дійсність ЕЦП перевіряється за допомогою відкритого ключа – коду перевірки, доступного решті суб’єктів електронного документообігу. Відкритий ключ має бути сертифікований центром сертифікації ключів.

Застосування будь-яких інших видів електронного підпису допускається на договірних засадах. Однак можна з упевненістю припустити, що поза такими договірними відносинами (для інших суб’єктів) інші види електронного підпису будуть практично позбавлені юридичної чинності й доказовості. Інакше кажучи, такі електронні підписи матимуть якусь значущість тільки для сторін конкретного договору, в межах якого вони застосовуються.

Щоб кожний «підписувач» мав свій, унікальний, підпис, використовується так званий особистий ключ – код, який має бути відомий лише його власнику. Якщо цей код повідомити програмі, то відповідно до криптографічного алгоритму вона сформує унікальне контрольне значення і додасть його до документу. Тобто підпише електронний документ унікальним ЕЦП господаря даного особистого ключа.

Для перевірки вірогідності ЕЦП та цілісності електронного документа використовується інший код – так званий відкритий ключ. На відміну від особистого, відкритий ключ доступний усім іншим зацікавленим учасникам електронного документообігу. Цей код не дозволяє підробити ЕЦП автора електронного документа, але дозволяє перевірити його справжність. Отримавши цей код, програма, використовуючи вже згаданий алгоритм, звірить його з отриманим разом з документом ЕЦП автора. Якщо ці контрольні значення зійдуться, підпис вважатиметься справжнім, а отриманий документ – цілісним [11, с.26].

Отже, ми дійшли висновку, що без існування електронного цифрового підпису неможливе існування електронного правочину.

**3.2 Проблеми вдосконалення використання електронного цифрового підпису**

Для запровадження електронного бізнесу типу «Бізнес-Бізнес» ключовою правовою проблемою є надання правового статусу документам, які передаються електронним шляхом. Наприклад, електронним шляхом можуть укладатися угоди, надаватись доручення банкам для перерахування коштів, можуть пересилатися сертифікати на продукцію тощо. У звичайному режимі документи засвідчуються підписами відповідальних осіб та печатками. В електронному режимі роль підпису може виконувати електронний (або ж цифровий) підпис.

В Законі України «Про електронний цифровий підпис», електронний підпис визначається як «дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов’язані та призначені для ідентифікації підписувача цих даних». Поруч там же знаходимо інше поняття: електронний цифровий підпис, або ж цифровий підпис. Це – «... 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 підпис складається із двох кодів: особистого, яким володіє особа, що ставить підпис, і відкритий, з допомогою якого можна перевірити достовірність підпису. Відкритий код мають в своєму розпорядженні всі особи, з якими власник закритого коду має стосунки. Особистий код містить унікальну інформацію про дані, які він засвідчує, і деякі дані, відомі виключно особі, з якою підпис пов’язаний. За допомогою відкритої частини коду отримувач повідомлення отримує можливість перевірити достовірність підпису.

Таким чином, електронний підпис виступає аналогом звичайного підпису в застосуванні до електронних документів.

Технологія електронного підпису може бути не менш ефективною, ніж звичайного. Але для практичного використання виникають проблеми правового визнання електронного підпису нарівні із звичайним, що в свою чергу потребує певного регулювання процедур надання засобів цифрового підпису.

Засоби для цифрового підпису (програмне забезпечення для шифрування та коди) надають уповноважені на це установи – центри сертифікації, які засвідчують надання засобів електронного підпису особі сертифікатом. Українське законодавство передбачає два види сертифікатів: звичайний та посилений. Звичайний може видаватися будь-якою особою (центром сертифікації), яка вирішила займатися цим видом діяльності. Для видачі посиленого сертифіката центр сертифікації повинен користуватися засобами електронного цифрового підпису, які в Законі названо «надійними засобами електронного цифрового підпису» та пройти акредитацію уповноваженим на це органом – центральним засвідчувальним центром.

Не менш серйозною прогалиною закону є недостатня увага до питання захисту інформації про особу. Закон досить широко як для такого документу говорить про те, що в сертифікаті вказуються необхідні дані про особу. Тоді як Директива ЄС передбачає лише ім’я особи, яка буде користуватись підписом, а за бажанням може бути вказано псевдонім у формі, що дозволяє встановити особу.

Крім того, при систематичному співробітництві підприємства з партнерами за допомогою електронних технологій, можуть виникати й інші проблеми при розв’язанні господарських конфліктів. Все це потребує доповнення законодавства, перш за все Господарського та Цивільного кодексів і відповідних процесуальних кодексів, що поки що залишається лише перспективою.

Проблеми запровадження в Україні електронного документу та електронного цифрового підпису стають все більш актуальними. Вони набувають значної політичної та економічної ваги у зв’язку з розширенням використання інформаційно-комунікаційних технологій у суспільних відносинах, розбудові систем електронних платежів, електронної торгівлі тощо. При цьому, якщо у Цивільному кодексі (1963 року із наступними змінами, внесеними до нього) було багато обмежень щодо використання електронного документа, то новий Цивільний кодекс 2003 року дозволив широке застосування електронних документів у цивільних правовідносинах.

Одне з проблемних питань, що повинні вирішити законодавство у цій сфері, – це робота центрів сертифікації ключів, які мають надавати послуги цифрового підпису. Спеціалісти вважають, що кількість бажаючих займатися такою діяльністю, можливо, буде досить незначною. Зокрема, тому, що фінансовий бар’єр виходу на ринок таких структур за нинішніх умов буде досить високим з огляду на специфіку їх функцій (надання засобів цифрового підпису, формування, розповсюдження, скасування, блокування та поновлення сертифікації ключів, генерація відкритих та особистих ключів тощо). А враховуючи те, що все повинно починатися практично з нуля, оскільки майже таким на даному етапі є ринок користувачів, «повернення» зроблених вкладень буде досить довгим.

Отже, на наш погляд центр сертифікації ключів є критичним елементом в системі застосування ЕЦП. Неналежна організація надання послуг ЕЦП, незабезпечення відповідного рівня безпеки функціонування, захисту інформації або збої у роботі зазначеного суб’єкта може створити умови, що сприятимуть масовим зловживанням при застосуванні ЕЦП, в тому числі їх підробленню, компрометації та неможливість використовувати даний механізм підписувачами, що отримують послуги ЕЦП у цих суб’єктів та особами, які перевіряють ЕЦП.

Суб’єктами, на яких проблема справляє негативний вплив є учасники електронного документообігу – користувачі послуг ЕЦП, зокрема фізичні особи, юридичні особи (ЕЦП використовується у якості печатки) незалежно від форми власності. Слід зазначити, що центри сертифікації ключів виконують функції технологічного посередника у системі електронного документообігу, учасниками якої можуть бути суб’єкти господарювання та органи державної влади. Діяльність центрів сертифікації ключів без суворого дотримання законодавства у зазначеній сфері, у тому числі ненавмисні порушення встановленого порядку виконання своїх функцій, може привести до створення сприятливих умов щодо виникнення господарських та адміністративних спорів за документами в електронному вигляді, в результаті невірного застосування механізмів ЕЦП.

Аналіз європейського законодавства та досвіду країн, в яких розгорнута та функціонує розвинута система ЕЦП свідчить, що проблема не може бути вирішена за допомогою ринкових механізмів та потребує державного втручання. Так, наприклад в Директиві Європейського Союзу 1999/93/ЄС «Про основи законодавства Співтовариства щодо електронних підписів» (стаття 3, параграф 3) зазначається, що кожна країна-член ЄС повинна забезпечити створення відповідної системи, що дозволяє здійснення нагляду за створеними на її території надавачами послуг з сертифікації, які видають посилені сертифікати невизначеному колу осіб (аналог акредитованих центрів сертифікації ключів, відповідно до законодавства України).

Відсутність запропонованого регулювання на законодавчому рівні та враховуючи вимоги Закону «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» щодо прав та повноважень суб’єктів господарювання та органів державного нагляду, з розповсюдженням в країні технологій електронного документообігу може привести до поширення зловживань з боку суб’єктів ринку послуг ЕЦП, та, як наслідок, до низького рівня довіри громадян щодо механізмів ЕЦП зокрема і електронного документообігу в цілому.

Хоча можна розглядати окремо шляхи вирішення кожної з переліку проблем, головним залишається те, що Україна є державою з невизначеною на макрорівні моделлю створення інформаційного суспільства і його економіки, що цілком нівелює часткові зусилля, наприклад, із розвитку системи Internet-крамниць і он-лайнових аукціонів та ін. Нині не викликає сумніву тільки те, що приєднання України до загальносвітових процесів глобалізації й інформатизації не буде легким, простим і дешевим.

**Розділ 4. Електронний цифровий підпис та документообіг в державній податковій службі**

**4.1 Використання електронного цифрового підпису в роботі органів державної податкової служби**

Як уже згадувалось вище, відповідно до вимог статті 5 Закону України від 22 травня 2003 року №852-IV,,Про електронний цифровий підпис” органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа. Стаття 3 цього Закону визначає, що електронний цифровий підпис 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, тобто засобів електронного цифрового підпису, що мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Питання співпраці, зобов’язань та відповідальності між акредитованими центрами сертифікації ключів та платниками податків у сфері надання послуг ЕЦП регулюються договірними відносинами згідно діючого законодавства. Починаючи з червня 2006 року, для опрацювання технологічного процесу приймання податкової звітності в електронному вигляді, органами ДПС використовувалось безкоштовне програмне забезпечення накладання електронного підпису «Нотар». Для участі в проекті залучалися платники податків, з якими укладався договір "Про забезпечення електронного документообігу платника податків з Державною податковою інспекцією засобами телекомунікаційного зв'язку".

З метою дотримання вимог чинного законодавства, впровадження, налагодження та застосування безпаперових технологій подання податкової звітності в електронній формі, Державною податковою адміністрацією України затверджено Інструкцію з підготовки і подання податкових документів в електронному вигляді засобами телекомунікаційного зв’язку та Примірний договір про визнання електронних документів (наказ ДПА України від 10.04.08 №233,,Про подання електронної податкової звітності”, зареєстрований у Міністерстві юстиції України 16.04.08 за № 320/15011) та укладено договори про співпрацю з акредитованими центрами сертифікації ключів (далі – АЦСК), а саме: ТОВ,,Український сертифікаційний центр”, ЗАТ,,Інфраструктура відкритих ключів”, ТОВ,,Арт-мастер”, ДП,,Українські спеціальні системи”. Дані АЦСК відповідно до статті 9 Закону України „Про електронний цифровий підпис” пройшли акредитацію у центральному засвідчувальному органі, який визначений Кабінетом Міністрів України та мають право надавати послуги ЕЦП. Оскільки послуги цих АЦСК є платними, ДПА України були досягнуті домовленості із АЦСК щодо безкоштовного або за пільговими тарифами надання засобів ЕЦП платникам податків, які уклали договори з органами ДПС "Про забезпечення електронного документообігу платника податків з Державною податковою інспекцією засобами телекомунікаційного зв'язку". Надання засобів ЕЦП здійснюється АЦСК з 20.02.08 на підставі оригіналу договору, укладеного між заявником та відповідною ДПІ. Також вказаними АЦСК проводяться акції по розповсюдженню ключів електронного цифрового підпису по зниженим тарифам.

Виходячи з вищенаведеного та на виконання розпорядження Кабінету Міністрів України від 06.02.08 №262-р «Про заходи щодо удосконалення системи адміністрування податку на додану вартість» стосовно забезпечення відповідно до законодавства криптографічного і технічного захисту поданої платниками податків інформації та посилення контролю за дотриманням вимог до її конфіденційності, приймання податкової звітності в електронному вигляді підписаної за допомогою безкоштовного програмного забезпечення накладання електронного підпису «Нотар» буде припинено з 01 січня 2009 року, про що необхідно повідомити платників податків через інформаційні сайти регіональних ДПА, об’яви на інформаційних дошках та засобами Е-Маіl. Безкоштовне розповсюдження засобів ЕЦП серед платників податків буде впроваджено ДПА України після введення в експлуатацію власного акредитованого центру сертифікації ключів.

**4.2 Вдосконалення подання платниками податків податкової звітності в електронній формі**

Правовідносини щодо подання податкової звітності платниками податків регулюються базовим законом у цій сфері – Законом України “Про порядок погашення зобов’язань платників податків перед бюджетами та державними цільовими фондами” та відповідними законами України з питань оподаткування за окремими податками, а також законами України “Про електронний цифровий підпис”, “Про електронні документи та електронний документообіг”. Але існує нагальна потреба законодавчого унормування питань забезпечення платників податків необхідним програмним продуктом при наданні ними податкової звітності в електронній формі. Тому, враховуючи це, буде доцільно прийняти закон, який дозволить створити організаційні умови щодо поступового переходу до подання платниками податків податкової звітності та інших податкових документів в електронному вигляді. Таким законом на сьогодні міг би стати Закон України «Про внесення змін до Закону України «Про порядок погашення зобов’язань платників податків перед бюджетами та цільовими фондами», проект якого зареєстрованний 30 травня 2008 року у Верховній Раді.

Підготовка зазначеного проекту зумовлена необхідністю удосконалення норм Закону України “Про порядок погашення зобов’язань платників податків перед бюджетами та державними цільовими фондами”, які регулюють питання податкової звітності.

Нова форма податкової декларації з податку на додану вартість, яка введена відповідно до Наказу Державної податкової адміністрації України від 10.04.2008 року № 233,,Про подання електронної податкової звітності” призвела до необхідності переходу платників цього податку на електронну звітності.

За даними Державної податкової служби загальна кількість зареєстрованих платників податку на додану вартість станом на 1.04.2008 року складала 349072 особи, з них юридичні особи – 287636, фізичних осіб – 61436. Подано 129161 розшифровок за звітний період березень 2008 року в електронному вигляді платниками податків.

Для подання податкових документів до органів державної податкової служби в електронному вигляді платник податків відповідно до нормативних актів Державної податкової адміністрації України повинен мати:

* спеціалізоване програмне забезпечення для формування податкових документів в електронному вигляді у затвердженому форматі (стандарті);
* доступ до мереж Інтернет та можливість відправлення/приймання електронних повідомлень по електронній пошті;
* засіб криптографічного захисту інформації (сумісний за форматами даних із засобами КЗІ, що використовуються в органах державної податкової служби);
* чинні посилені сертифікати відкритих ключів, сформованих акредитованим центром сертифікації ключів для платника податків та уповноважених посадових осіб платника податків, підписи яких є обов'язковими для податкової звітності у паперовій формі.

Спеціалізоване програмн забезпеченн для формування податкових документів в електронному вигляді у затвердженому форматі (стандарті) відповідно до наказу Державної податкової служби від 10.04.2008 року № 233 “Про подання електронної звітності” надається платникам податків безкоштовно.

Згідно із цим нормативно-правовим актом платник податків отримує в будь-якому включеному до системи подання податкових документів в електронному вигляді акредитованому центрі сертифікації ключів посилені сертифікати відкритих ключів посадових осіб юридичної особи, що мають право підпису (керівника,бухгалтера), та печатку юридичної особи. Платник податків фізична особа – суб'єкт підприємницької діяльності може обмежитись одним ключем електронного цифрового підпису.

Отримання цього продукту провадиться платниками податків за власні кошти. Вартість послуги електронного цифрового підпису залежить від тарифів акредитованих центрів сертифікації ключів та за даними цінового моніторингу на теперішній час складає від 120 до 1140 гривень. На сьогодні існує досить обмежена кількість приватних компаній (провайдерів), які мають відповідні дозвільні та регламентні документі на здійснення такої діяльності, та з якими Державною податковою адміністрацією України укладено договір про подання податкової звітності платниками податків із застосуванням електронного підпису. За наявним та постійним попитом на цей продукт вартісна складова його буде мати тенденцію до збільшення.

Чинне податкове законодавство України не містить обов’язку платника податку (пункт 2 частини першої статті 9 Закону України “Про систему оподаткування”, стаття 4 Закону України “Про порядок погашення зобов’язань платників податків перед бюджетами та державними цільовими фондами”, пункт 7.2 статті 7 Закону України “Про податок на додану вартість”, пункт 16.4 статті 16 Закону України “Про оподаткування прибутку підприємств”, стаття 18 Закону України “Про податок з доходів фізичних осіб”, статті 8-10. частина шоста статті 11-1 Закону України “Про державну податкову службу в Україні”) надавати податкову звітність в електронній формі. Відповідно до підпункту “з” підпункту 4.4.2 пункту 4.4 статті 4 Закону України “Про порядок погашення зобов’язань платників податків перед бюджетами та державними цільовими фондами” податкова звітність в електронній формі може надаватися платником податків податковому органу лише за добровільним рішенням такого платника, за умови реєстрації електронного підпису підзвітної особи у порядку, визначеному законодавством. Із зазначеного не випливає обов’язок платників податків нести додаткові витрати на отримання необхідного програмного забезпечення, тим більш у випадках, коли перехід на електронну звітність провадиться за ініціативою держави, що загалом базується на припису статті 67 Конституції України.

Світова практика оподаткування не передбачає платності при наданні податкової звітності. Навпаки, багато країн пропонують безоплатну видачу ключів, електронних програм, встановлення Інтернету та підтримку і обслуговування мереж.

Отже, прийняття зазначеного Закону дозволить створити організаційні умови щодо поступового переходу до подання платниками податків податкової звітності та інших податкових документів в електронному вигляді.

**Висновки**

Стрімкий розвиток та глобальне впровадження новітніх інформаційних технологій, інтенсифікація інформаційних відносин, створили умови, коли життя людини є майже не мислимим без мобільного телефону, телевізора, комп’ютера та Інтернету.

Розвиток суспільних відносин став вимогою в цілому щодо розроблення, вдосконалення та оновлення нормативно-правової бази України, створення спеціальних юридичних норм та правил регулювання сфери інформаційних правовідносин.

Верховною Радою України були прийняті закони України, які набули чинності, «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», «Про обов’язковий примірник документів», «Про Національну програму інформатизації», «Про телекомунікації», «Про Національну систему конфіденційного зв’язку», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо.

Закон України «Про електронні документи та електронний документообіг» визначив основні організаційно-правові засади електронного документообігу та використання електронних документів.

Законом встановлено, що електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа, зокрема, електронний цифровий підпис. Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Проте, закон також встановив певні обмеження на застосування електронного документа як оригіналу. Зокрема, в електронній формі не може бути створено оригінал свідоцтва про право на спадщину; інший документ, який, згідно із законодавством, може бути створений лише в одному примірнику (поки не буде створено централізованого сховища оригіналів електронних документів).

Електронний цифровий підпис дає змогу підтвердити цілісність електронного документу, тобто його захищеність від несанкціонованого спотворення, руйнування або знищення в процесі руху від відправника до одержувача, та ідентифікувати підписувача.

Правочини здійснені за допомогою накладання на них електронного цифрового підпису та передані адресату в мережі передачі даних мають великий ступінь захисту від несанкціонованого доступу, спотворення чи знищення змісту правочину, адже такий підпис отримується за результатом криптографічного перетворення набору електронних даних.

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки), 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.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Особистий ключ має бути відомий лише його володільцеві. Відкритий ключ доступний всім учасникам електронного документообігу.

Засвідчення чинності відкритого ключа здійснюється шляхом формування сертифіката відкритого ключа – документа, що видається центром сертифікації ключів. Посилений сертифікат відкритого ключа видається акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом.

Сертифікат ключа містить найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру); зазначення, що сертифікат виданий в Україні; унікальний реєстраційний номер сертифіката ключа; основні дані (реквізити) підписувача – власника особистого ключа; дату і час початку та закінчення строку чинності сертифіката; відкритий ключ; найменування криптографічного алгоритму, що використовується власником особистого ключа; інформацію про обмеження використання підпису.

Посилений сертифікат ключа, крім обов’язкових даних, які містяться в сертифікаті ключа, повинен мати ознаку посиленого сертифіката ключа.

Юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом ключа, а також використовувати електронний цифровий підпис без сертифіката ключа.

Розподіл ризиків збитків, що можуть бути заподіяні підписувачам, користувачам та третім особам, які користуються електронними цифровими підписами без сертифіката ключа, визначається суб’єктами правових відносин у сфері послуг електронного цифрового підпису на договірних засадах.

Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа.

Отже, електронний цифровий підпис спрямований на спрощення та прискорення документообігу між суб’єктами господарювання, що, в свою чергу, має зміцнити конкурентоспроможність вітчизняних підприємств, адже пришвидшиться процедура укладення цивільно-правових та господарських договорів, оформлення експортно-імпортних операцій, надання електронних банківських послуг.

Станом на сьогодні, згідно з інформацією, розміщеною на офіційному веб-сайті центрального засвідчувального органу, акредитацію пройшли три центри сертифікації ключів, тобто система електронного цифрового підпису є повністю структурно укомплектованою для належного функціонування.

**Список використаних джерел**

1. Конституція України від 28.061996 р. № 254 к/96-ВР // Відомості Верховної Ради України від 23.07.1996 р. – 1996, № 30, ст. 141.
2. Цивільний кодекс України від 16.01.2003 р. № 435-ІV (із наступн. змінами) // Відомості Верховної Ради України вiд 03.10.2003 р. – 2003, № 40, ст. 356.
3. Закон України «Про електронні документи й електронний документообіг» від 22.05.2003 р. № 851-IV.
4. Закон України «Про електронний цифровий підпис» від 22.05.2003 р. № 852-IV.
5. Закон України «Про платіжні системи і переклад грошей в Україні» від 05.04.2001 р. № 2346-III.
6. Закон України «Про бухгалтерський облік і фінансову звітність в Україні» від 16.07.99 р. № 996-XIV.
7. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні» від 09.01.2007 р. № 537-V.
8. Закон України «Про порядок погашення зобов’язань платників податків перед бюджетами та цільовими фондами» від 21.12.2000 р. № 2181-ІІІ.
9. Директива 1999/93/EC Европейского парламента и совета от 13 Декабря, 1999 г. Относительно структуры сообщества для электронных подписей.
10. Положення про документальне забезпечення записів у бухгалтерському обліку, затверджено наказом Міністерства фінансів України від 24.05.95 р. № 88.
11. Перелік типових документів, що створюються в діяльності органів державної влади і місцевого самоврядування, інших установ, організацій і підприємств, із указівкою термінів зберігання документів, затверджено наказом Головного архівного управління при КМУ від 20.07.98 р. № 41.
12. Наказ ДПА України,,Про подання електронної податкової звітності” від 10.04.08 №233, зареєстрований у Міністерстві юстиції України 16.04.08 за № 320/15011.
13. Проект Закону України «Про внесення змін допідпункту “з” підпункту 4.4.2 пункту 4.4 статті 4 Закону України «Про порядок погашення зобов’язань платників податків перед бюджетами та цільовими фондами» від 30.05.08 р. № 2582.
14. Блажівська Наталя. Електронний правочин // Юридичний журнал. №1/2007.
15. Гудзь О. Еволюція форм правочинів: від усної – до «електронної»//Юридичний журнал. – 2006. – № 1(43). – С. 32-37.
16. Дутов М. Сравнительный анализ европейского законодательства в области электронного документооборота // Підприємництво, господарство і право. 2002. № 8. - С. 25-28
17. Кирилюк Дмитро. Правові засади використання електронних розрахункових документів та електронних підписів в банківській діяльності // Юридичний журнал. №12/2005.
18. Лінецький Сергій. Як використовувати електронні документи? Юридичний журнал. №9/2003.
19. Сергієнко Дмитро. Україні – електронний документообіг // Юридичний журнал. №2/2002.
20. Симонович П.С. Регулирование электронной цифровой подписи нормами права: международный опит // «Журнал российского права», № 3, март 2002 г.
21. Чирський Ю. Електронний цифровий підпис: правові аспекти застосування // Довідник секретаря та офіс-менеджера. - №1(2007) - С. 26-31.
22. Чирський Юрій. Запровадження системи електронного документообігу в Україні // Юридичний журнал. № 6/2006.