МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

А.В. ЧУЧКОВСЬКА

ПРАВОВЕ РЕГУЛЮВАННЯ ЕЛЕКТРОННОЇ КОМЕРЦІЇ В УКРАЇНІ

Рекомендовано
Міністерством освіти і науки України
як навчальний посібник для студентів
вищих навчальних закладів

Київ – 2007

УДК 347.4(075.8)
ББК 67.404.2я73
Ч 11

Гриф надано
Міністерством освіти і науки України
(лист №1-4/18–Г–500 від 17.01.2006 року)

Рецензенти:
Пронська Г.В. – доктор юридичних наук, професор;
Луць В.В. – доктор юридичних наук, професор.

Чучковська А.В.
Ч 11 Правове регулювання електронної комерції в Україні. Навчальний посібник. – К.: Центр учбової літератури, 2007. – 224 с.

ISBN 966-364-384-6

Матеріал навчального посібника – перше комплексне дослідження правового регулювання вчинення господарських договорів через мережі електрозв'язку, зокрема через мережу Інтернет, де на підставі чинного законодавства України, нормативних актів міжнародних організацій та окремих держав світу подано аналіз такого нового правового поняття, як електронна комерція, визначені правовідносини, які складають це поняття, та принципи її правового регулювання, досліджено вчинення правочинів через мережі електрозв'язку, в зв'язку з чим досліджується поняття та використання електронних документів та електронних підписів, поняття форми господарського договору з врахуванням сучасних електронних носіїв інформації, особливі додаткові істотні умови таких господарських договорів.

ISBN 966-364-384-6
© Чучковська А.В., 2007
© Центр учбової літератури, 2007

ВСТУП

У останнє десятиліття XX ст. інформаційно-комунікаційні технології, перш за все глобальна інформаційна мережа Інтернет, стали одним з факторів, які істотно впливають як на розвиток суспільства в цілому, так і на розвиток господарської сфери зокрема.

Українське суспільство не тільки усвідомлює необхідність використання можливостей глобальної інформаційної мережі Інтернет у сфері господарювання, а й докладає конкретних зусиль до цього [2–4, 6].

Мережа Інтернет являє собою найбільш розгалужену міжнародну мережу електрозв'язку загального користування[1], призначену для обміну електронними документами[2], що не виключає у майбутньому створення іншої мережі електрозв'язку загального користування.

Використання можливостей мережі Інтернет у сфері господарювання призводить не тільки до швидкого росту кількості господарських та цивільних договорів, що укладаються через мережі електрозв'язку, а й до руху підприємництва в напрямку світової глобалізації [7].

Поступово у діловій та правовій практиці з'являється та закріплюється нове поняття "електронна комерція" (e-commerce). Фактично електронна комерція в Україні, як певні суспільні відносини, вже існує. Але в Україні, як і в багатьох інших дер-

---

[1] Закон України "Про зв'язок" у ст. 1 визначає електричний зв'язок як передачу, випромінювання або прийом знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах; мережу зв'язку – як сукупність засобів та споруд зв'язку, поєднаних в єдиному технологічному процесі для забезпечення інформаційного обміну; мережу зв'язку загального користування – як мережу зв'язку, що експлуатується підприємствами та об'єднаннями зв'язку для забезпечення потреб в послугах зв'язку усіх споживачів.

[2] Визначення поняття "електронний документ" наводиться та обґрунтовується у розділі 2 роботи.

жавах світу, правова база для регулювання відповідних відносин лише починає створюватися.

Тільки у 1998 р. в Україні з'являються перші нормативні акти, що регламентують порядок створення та використання електронних цифрових підписів (далі – ЕЦП) та електронних документів. У 2000–2002 рр. до Верховної Ради України вперше вноситься група законопроектів, покликаних комплексно врегулювати відносини, що виникають при вчиненні правочинів через мережі електрозв'язку. 22 травня 2003 р. прийнятий перший з таких законів, а саме закон "Про електронний цифровий підпис", який визначає правовий режим ЕЦП та регулює відносини, що виникають при його використанні.

Перший закон у світі, який врегулював вчинення правочинів через мережі електрозв'язку, зокрема використання з цією метою електронних підписів, прийняли у США у 1995 р.

Враховуючи комплексність та новизну відносин, що виникають при вчиненні правочинів через мережі електрозв'язку, у 1996 р. Комісією ООН по праву міжнародної торгівлі (ЮНСІТРАЛ) був прийнятий Типовий закон "Про електронну комерцію" [8], після чого аналогічні нормативні акти були прийняті у ряді держав світу: Сінгапурі (1998), Великобританії (1999), Австралії (1999), Гонконзі (2000), Ірландії (2000), Філіппінах (2000), США (2000), Тунісі (2000), Люксембурзі (2000) тощо.

Таким чином, з 1995 р. в багатьох державах світу почало формуватися новітнє законодавство, спрямоване на регулювання укладання правочинів через мережі електрозв'язку, тобто на комплексне регулювання електронної комерції.

Електронна комерція є комплексним, системним правовим поняттям, яке включає три групи правовідносин: правовідносини, пов'язані із вчиненням правочинів через мережі електрозв'язку у сфері господарювання; правовідносини, пов'язані із використанням електронних документів; правовідносини, пов'язані із використанням електронного підпису[3].

[3] Визначення поняття "електронний підпис" наводиться та обґрунтовується у розділі 3 роботи.

Ці правовідносини перебувають у тісній взаємодії: в основі електронної комерції лежить електронний документ, який набирає юридичної сили документа завдяки застосуванню електронного підпису. Вчинення господарських договорів через мережі електрозв'язку складається з процесів формування, обробки, зберігання, відправлення, одержання, перевірки та використання електронних документів.

Для електронної комерції мережа Інтернет є середовищем здійснення господарської діяльності, зокрема середовищем, в якому вчиняються господарські договори через мережі електрозв'язку [9]. Середовищем здійснення електронної комерції, крім мережі Інтернет, можуть виступати й інші мережі електрозв'язку не тільки загального, а й відомчого[4] або подвійного призначення, за допомогою яких може відбуватися обмін електронними документами. Тобто, електронна комерція не пов'язується з використанням якоїсь однієї чітко встановленої мережі електрозв'язку.

Широке використання Інтернет для здійснення електронної комерції пов'язане з тим, що ця телекомунікаційна мережа дозволяє істотно знизити витрати на організацію та підтримку всієї інфраструктури господарської діяльності; зменшуються витрати на рекламу та обслуговування, а значить, і собівартість товару; скорочується час укладання та виконання договорів з контрагентами; істотно розширюється ринок збуту товарів та послуг для продавця та можливість вибору для покупця [10–14].

Аналіз досліджень окремих фахівців дозволяє стверджувати, що, не дивлячись на ознаки економічного спаду, керівники багатьох європейських компаній заявляють про збільшення інвестицій до електронної комерції протягом ближчих 12 місяців [15], розглядаючи її як один з засобів підтримання своєї конкурентоспроможності та забезпечення майбутнього успіху [16]. Так, у 1999 р. європейський ринок електронної ко-

[4] Закон України "Про зв'язок" у ст. 1 визначає відомчу мережу зв'язку як мережу зв'язку, що експлуатується юридичною або фізичною особою для задоволення власних потреб.

мерції збільшився на 200 відсотків; загальний оборот ринку електронної комерції у 1999 р. склав 3,5 млрд доларів [17].

На рівні міжнародних організацій та законодавства окремих країн світу лише з 90-х рр. XX ст. почалася робота зі створення правового регулювання відносин у сфері електронної комерції, основним напрямком якої є прийняття комплексних нормативних актів про електронну комерцію, присвячених регулюванню системи відносин, що виникають при вчиненні правочинів через мережі електрозв'язку, та окремих законів про електронні підписи, що пов'язано зі складністю та новизною відносин, що виникають при використанні електронних підписів у електронній комерції.

Так, одними з найавторитетніших джерел являються Типовий закон ЮНСІТРАЛ від 16 грудня 1996 р. "Про електронну комерцію" та Типовий закон ЮНСІТРАЛ від 5 червня 2001 р. "Про електронні підписи" [18]. Причиною розробки цих законів була поява нових засобів, за допомогою яких сторони обмінюються між собою інформацією, використовуючи при укладанні правочинів сучасні методи зв'язку. Типові закони покликані стати взірцем для оцінки та оновлення певних аспектів законів держав світу та практики їх застосування в галузі торгових відносин з використанням сучасних методів зв'язку, а також для прийняття відповідного законодавства.

У рамках Європейського Союзу прийнятий цілий ряд актів, спрямованих на врегулювання відносин у сфері електронної комерції. Серед них: Директива ЄС від 8 червня 2000 р. "Про деякі правові аспекти послуг інформаційного суспільства, в тому числі електронної комерції, на внутрішньому ринку"[19]; Директива ЄС від 13 грудня 1999 р. "Про правові підстави для використання електронних підписів"[20].

У Великобританії прийняті та діють закони від 18 листопада 1999 р. "Про регулювання електронної комерції" [21] та від 13 лютого 2002 р. "Про регулювання використання електронних підписів" [22]. Штат Юта (США) прийняв Закон від 1 травня 1995 р. "Про електронний підпис" [23] та Закон від 3 липня 2000 року "Про електронні правочини" [24].

Більшість інших держав світу перебуває у стадії формування законодавства про електронну комерцію. Так, у Сінгапурі діє Закон від 10 липня 1998 р. "Про електронні правочини" [25], у Австралії діє Закон від 10 грудня 1999 р. "Про електронні правочини" [26], у Гонконзі діє Ордонанс від 7 січня 2000 р. "Про електронні правочини"[27], в Ірландії діє Закон від 10 липня 2000 р. "Про електронну комерцію" [28], у Філіппінах діє Закон від 14 червня 2000 р. "Про електронну комерцію" [29], у Тунісі 9 серпня 2000 р. був прийнятий Закон "Про електронний обмін та електронну комерцію" [30], у Люксембурзі 14 серпня 2000 р. прийнятий Закон "Про електронну комерцію" [31] тощо. У вказаних державах ведеться законопроектна робота з підготовки правового регулювання використання електронних підписів. Всі наведені закони ґрунтуються на положеннях зазначених вище Типових законів ЮНСІТРАЛ та європейських Директив.

В інших державах навпаки, спочатку була розроблена правова база використання електронних підписів, після чого постало питання про прийняття комплексних законів про електронну комерцію. Серед нормативних актів, присвячених регулюванню цих відносин, можна назвати:

1) Модельний Закон Міжпарламентської асамблеї країн–учасниць СНД від 9 грудня 2000 р. "Про електронний цифровий підпис" [32, с. 310];
2) Закон Італійської Республіки від 1 березня 1997 р. "Закон Басаніні" [33];
3) федеральний Закон Австрії від 30 липня 1999 р. "Про електронний підпис" [35];
4) федеральний Закон США від 1 жовтня 2000 р. "Про електронні підписи у міжнародних та внутрішньодержавних торгових відносинах" [36];
5) Закон Російської Федерації від 10 січня 2002 р. "Про електронний цифровий підпис" [37];
6) Закон України від 22 травня 2003 р. "Про електронний цифровий підпис";
7) тощо.

Такі держави, як Туркменістан [38], Республіка Бєларусь [39] регулювання електронної комерції почали з прийняття законів, що встановлюють правові підстави використання електронних документів. В Україні 22 травня 2003 р. прийнятий Закон "Про електронний документ та електронний документообіг", що набрав чинності з 28 грудня 2003 р. У РФ існує законопроект про електронний документ та електронний документообіг.

Правове регулювання електронної комерції в Україні перебуває у процесі становлення. Кожна з трьох груп відносин, що складають електронну комерцію, лише починає одержувати відповідне правове регулювання.

Прийнятий 16 січня 2003 р. Господарський кодекс України [40] (далі – ГКУ), як основний комплексний нормативний акт у сфері господарювання, не врахував сучасних тенденцій використання інформаційно-телекомунікаційних технологій у господарській сфері. Електронна комерція, а саме питання вчинення договорів через мережі електрозв'язку, використання з цією метою електронних документів, ЕЦП, взаємовідносини та відповідальність суб'єктів електронної комерції залишилися неврегульованими.

Новий Цивільний кодекс України [41] (далі – ЦКУ), прийнятий 16 січня 2003 р., спробував вирішити проблему можливості укладання договорів з використанням мереж електрозв'язку. ЦКУ містить єдину статтю 207, яка у найбільш загальному вигляді закріплює потенційну можливість укладання договорів через мережі електрозв'язку (передбачається можливість здійснення волевиявлення сторін з використанням електронних засобів зв'язку для укладання правочинів у письмовій формі та застосування з цією метою ЕЦП).

Комплексне та системне регулювання електронної комерції в Україні у зв'язку зі складністю та виходячи з характеру цих відносин, з нашої точки зору, повинне бути оформлене окремим законом, про що має бути зазначено у ГКУ в розділі 4 "Господарські зобов'язання".

Правове регулювання відносин, пов'язаних із використанням електронних документів, та відносин, пов'язаних із вико-

ристанням електронного підпису, також перебуває у стадії становлення. Правовою підставою використання електронних документів та електронних підписів в Україні є такі нормативні акти: Закон України від 22 травня 2003 р. "Про електронний цифровий підпис"; Закон України від 22 травня 2003 р. "Про електронний документ та електронний документообіг"; Закон України від 5 квітня 2001 р. "Про платіжні системи та переказ грошей в Україні [42]"; Закон України від 9 квітня 1999 р. "Про обов'язковий примірник документів" [43]; Закон України від 2 жовтня 1992 р. "Про інформацію" [44]; Інструкція "Про безготівкові розрахунки в Україні в національній валюті", затверджена Постановою Правління НБУ від 29 березня 2001 р. (в редакції 4 грудня 2001 р.) № 135 [45]; Інструкція "Про міжбанківські розрахунки в Україні", затверджена Постановою Правління НБУ України від 27 грудня 1999 р. (в редакції 23 квітня 2002 р.) № 621 [46]; "Правила організації захисту електронних банківських документів", затверджені Постановою Правління НБУ від 10 червня 1999 р. № 280 [47].

Більшість зазначених нормативних актів вузькоспеціалізовані, призначені для регулювання відносин виключно в банківській сфері, а тому неприйнятні для застосування в інших сферах господарської діяльності.

22 травня 2003 р. Верховною Радою України прийняті Закон "Про електронний цифровий підпис" [48], що визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні ЕЦП, та Закон "Про електронні документи та електронний документообіг" [49], що повинен встановити основні організаційно-правові засади електронного документообігу та використання електронних документів в Україні. Але ці закони, незважаючи на їх новизну, вже можна назвати недосконалими, та такими, що потребують доопрацювання.

В Україні, також, прийнятий Закон від 14 травня 2003 р. "Про телекомунікації"[50] № 2059-2, який повинен замінити Закон України від 16 травня 1995 р. "Про зв'язок" [51], визначити правові засади діяльності у галузі телекомунікацій в Україні

та врегулювати відносини суб'єктів ринку телекомунікаційних послуг, зокрема провайдерів телекомунікацій, між собою та з органами державної влади і органами місцевого самоврядування (на даний закон Президентом України було накладено вето).

Поняття, що розглядаються в кожному із зазначених законів та законопроектів, і є предметом їх правового регулювання, можуть бути предметом самостійного комплексного дослідження, що пов'язано з їх складністю, багатогранністю та абсолютною новизною.

У Верховній Раді України зареєстрований законопроект від 17 лютого 2003 р. № 3114 "Про електронну торгівлю" [52], який має забезпечити правові умови для електронної торгівлі: закріплення прав і обов'язків осіб, що здійснюють електронну торгівлю, визначення правил вчинення правочинів з використанням електронних документів, а також визнання електронних документів як судових доказів.

Незважаючи на те, що Закон України "Про електронний цифровий підпис" набрав чинності з 1 січня 2004 р., залишається доцільним прийняття комплексного закону, який повинен встановити певні принципи електронної комерції, системно врегулювати відносини, пов'язані зі вчиненням правочинів через глобальну інформаційну мережу Інтернет, порядок використання з цією метою електронних документів та ЕЦП, участь інформаційних посередників у сфері електронної комерції, а також встановити відповідальність суб'єктів електронної комерції за правопорушення у сфері електронної комерції.

Формування абсолютно нового як для України, так і для інших країн світу законодавства, майже повна відсутність судової практики будуть вимагати ретельного вивчення законодавства та практики його застосування, і ці питання ще багато років будуть залишатися надзвичайно актуальними для дослідження.

РОЗДІЛ 1
Загальна характеристика правового регулювання електронної комерції в Україні

1.1. Правовідносини, що виникають у сфері електронної комерції

Перехід до третього тисячоліття фахівцями в галузі філософії, економіки, юриспруденції, інформатики пов'язується з переходом до інформаційного суспільства, під яким розуміється суспільство, в якому ключову роль відіграють послуги з отримання, обробки та поширення інформації, на відміну від індустріального суспільства, основу якого складають процеси створення, розподілення та перерозподілення матеріальних благ [53, с. 394, 54, с. 12–14, 55, с. 1]. Тобто в інформаційному суспільстві вирішальну роль відіграють галузі, пов'язані з одержанням, розповсюдженням та обробкою інформації. [56, с. 4, 57, с. 5, 58, с. 5, 59, с. 3].

Наприкінці XX ст. вперше в історії людства основним предметом суспільного виробництва у промислово розвинутих державах світу стає інформація, а не матеріальні об'єкти. [60, с. 14]. В умовах інформаційного суспільства ключову роль відіграють телекомунікаційні мережі[1] як середовище, в якому відбуваються процеси збирання та обміну інформацією у локальних, загальнодержавних та міжнародних масштабах. Однією з найбільш поширених телекомунікаційних мереж є міжнародна мережа Інтернет (далі – Інтернет).

Сучасне суспільство використовує Інтернет для задоволення найрізноманітніших потреб своїх громадян. Інтернет висту-

[1] Мережа телекомунікацій – комплекс поєднаних у єдиному технологічному процесі засобів та об'єктів телекомунікацій, призначений для передавання, приймання інформації між кінцевими пунктами мережі.

пає, перш за все, дуже ємним джерелом будь-якої інформації, зручним та швидким засобом поширення, обробки та зберігання інформації, середовищем здійснення електронної комерції. [61].

Як свідчать кількісні показники, в 2005 р. кількість користувачів Інтернет вже досягла мільярда осіб порівняно з 300 млн у 1999 р.; прибуток від електронної комерції у всьому світі у 2000 р. склав $185 млрд, у 2001 р. – $686,3 млрд, у 2003 р. – $1,2 трлн [62–63].

Перш ніж приступати до розгляду правовідносин, що виникають у сфері електронної комерції, слід з'ясувати, що саме являє собою мережа Інтернет з точки зору права.

Наближення рівня технологій, що нівелює розбіжності в технічних пристроях, дозволяє вільно обмінюватися інформацією як між персональними комп'ютерами, так й між переносними персональними комп'ютерами, сотовими телефонами, бортовими комп'ютерами автомобілів, що призводить до виникнення комунікації нового рівня.

Виникнення засобів зв'язку (технічного обладнання, що використовується для організації зв'язку) нового рівня розглядається дослідниками в зв'язку з поняттям "інформаційного суспільства" [64, с. 14]. Матеріальною (технологічною) базою інформаційного суспільства є глобальні телекомунікаційні мережі, найбільшою з яких є Інтернет. З часу свого виникнення Інтернет дуже швидко перетворився на соціальне явище, що стало підґрунтям дослідження поняття "Інтернет" не тільки через призму технічних наук, як сукупності технічних засобів для обміну інформацією, а й через призму соціальних – як сукупності суспільних відносин з приводу використання міжнародної телекомунікаційної мережі. [65, с. 23]

Інтернет з технічної точки зору являє собою найбільшу телекомунікаційну (від англ. терміна, який означає мережу передачі даних – telecommunications network) [66, с. 239, 67, 23] мережу, створену шляхом об'єднання понад десяти тисяч п'ятисот телекомунікаційних мереж різного типу [68, с. 466].

Зазначена мережа виступає середовищем передачі відомостей про оточуючий світ, його об'єкти, процеси та явища, що

дозволяє провести їх безпосередню комп'ютерну обробку. На сьогоднішній день для передачі даних в мережі Інтернет використовується більшість каналів зв'язку – від звичайної телефонної лінії до трансатлантичного кабелю та груп супутників.

Збільшення маси користувачів мережі Інтернет призвело до того, що вона стала відігравати роль соціального явища, що робить можливим включення її до предмета гуманітарних наук.

В юридичній літературі автори пропонують різні підходи до розуміння поняття "Інтернет". Так, С.В. Малахов зазначає, що мережу Інтернет можна розглядати в трьох аспектах: як певну сукупність майна, як певне суспільне утворення (Інтернет – як сукупність користувачів Інтернет) та як сукупність інформаційних суспільних відносин [69, с. 13]. Розглядаючи Інтернет через призму об'єкта цивільних правовідносин, а саме як технічний комплекс, окремі речі, які перебувають у власності великої кількості осіб, автор висловлює думку про те, що Інтернет у своїй цілісності не може бути переданий одним суб'єктом суспільних відносин іншому; визначення буття Інтернет яким-небудь одним власником не є можливим [69, с. 13]. Виходячи з цього, автор робить висновок про неможливість перебування Інтернету на титулі права власності у якої-небудь особи, а звідси неможливість бути об'єктом цивільного обігу [70, с. 62]. Визнаючи той факт, що "Інтернет... не належить нікому окремо" [70, с. 61], не можна погодитися з принциповою неможливістю для Інтернет виступати об'єктом цивільного обігу та належати одному власнику. Причому мова йде не про виникнення нового об'єкта цивільного права, а про можливість наявності у Інтернет, як певного технічного комплексу, ознак об'єкта права.

Досліджуючи Інтернет через призму суб'єкта правовідносин (тобто як сукупності користувачів мережі Інтернет), С.В. Малахов обґрунтовано довів відсутність ознак юридичної особи у сукупності користувачів Інтернету (організаційної єдності, відокремленого майна, органів, здатних представляти Інтернет в суді, тощо) [70, с. 59]. Розглядаючи мережу Інтернет в третьому аспекті, С.В. Малахов пропонує визначати Інтернет як "сукупність інформаційних суспільних відносин у віртуальному

середовищі" [69, с. 6]. Автор не дає визначення поняття віртуального середовища, але його можна розуміти як "сукупність програмно-технічних засобів імітації простору та поведінки в ньому людини" [71, с. 57]. З нашої точки зору, поняття "віртуальне середовище" не є правовим, а саме визначення Інтернет як сукупності інформаційних відносин у віртуальному середовищі є дуже абстрактним.

В.П. Талимончик визначає Інтернет як комплексний предмет правового регулювання, що об'єднує різноманітні суспільні відносини у єдиній соціально-технічній системі, створеній в процесі розвитку глобальної комп'ютерної мережі та призначеній для здійснення масової інформації та телекомунікації [72, с. 84]. Автор, з одного боку, цілком правильно вказує на комплексність такого поняття, як Інтернет, що ґрунтується на поєднанні соціальних та технічних елементів у єдину систему. З іншого боку, у своєму визначенні В.П. Талімончик, визначаючи Інтернет лише як сукупність певних суспільних відносин, фактично одним аспектом (соціальним) підмінює все явище, яке носить комплексний характер.

С.В. Петровський визначає Інтернет як технічну систему, враховуючи, але не включаючи до цього поняття суспільні відносини щодо обміну даними. [65, с. 27].

Автор правильно зазначив на необхідність виділення ознак телекомунікаційної мережі Інтернет, серед яких він назвав: а) мережа Інтернет є технологічною системою, яка забезпечує обмін інформацією між комп'ютерними пристроями, Інтернет являє собою різновид мережі електрозв'язку; б) мережа Інтернет має глобальний, міжнародний характер; в) мережа Інтернет є відкритою для користування всіма фізичними та юридичними особами, тобто на сьогоднішній день представляє собою мережу зв'язку загального користування; г) мережа Інтернет призначена для передачі даних, що читаються машиною.

Сукупність зазначених ознак дозволила автору визначити Інтернет як міжнародну мережу електрозв'язку загального користування, призначену для обміну даними, що читаються машиною, тобто відомостями про навколишній світ, його об'єкти,

процеси та явища, об'єктивованими в форму, що дозволяє провести їх безпосередню машинну обробку. [65, с. 37] Необхідно звернути увагу на те, що саме остання ознака дозволяє не тільки відокремити Інтернет від більшості інших мереж зв'язку, а й розрізняє його з такими мережами електрозв'язку як, наприклад, телеграфна або телефонна.

У законодавстві України протягом останніх років активно використовується поняття "Інтернет", але не міститься його визначення. Вітчизняна юридична література також вживає це поняття, але не пропонує його розуміння. Усунення вказаної прогалини може бути досягнуто прийняттям Закону України "Про телекомунікації"[2]. Цей закон визначає Інтернет як глобальну загальнодоступну телекомунікаційну мережу, яка логічно зв'язана глобальним унікальним адресним простором[3], використовує єдині технічні стандарти та Інтернет-протоколи передавання даних і призначена для обміну інформацією. Вказане визначення, на нашу думку, відповідає наведеним вище чотирьом ознакам, а саме: Інтернет є певним технічним майновим комплексом; має глобальний характер; Інтернет є відкритим для всіх користувачів; призначений для передавання інформації, придатної до комп'ютерної обробки. В той же час таке визначення базується на неюридичній термінології і таким чином не може включатися до існуючих юридичних конструкцій, застосовуватися у юридичній теорії та практиці. Як зазначає І. Жилінкова, наочне домінування технічної сторони Інтернету не повинно заважати юридичному осмисленню цього феномена [226].

Фактична можливість укладати правочини через мережу Інтернет призвела до виникнення такого явища, як електрон-

[2] Закон України "Про телекомунікації" 25 липня 2003 р. підписаний головою Верховної Ради України, а 9 серпня 2003 р. Президентом України на даний закон було накладено вето.

[3] Законопроект визначає адресний простір мережі Інтернет як сукупність набору адрес Інтернет-протоколу, назв доменів, правил, встановлених відповідно до міжнародних стандартів Інтернет.

на комерція[4], формування законодавства та відповідної судової практики [73, с. 171–174, 74].

До формування законодавства, яке б врегулювало відносини у сфері електронної комерції, існує два підходи. Перший – прийняття комплексного нормативного акта про електронну комерцію та окремого закону про електронні підписи [75, 228, с. 12], другий – прийняття двох і більше нормативних актів, кожен з яких регулює окрему групу відносин у сфері електронної комерції [76]: відносини, пов'язані із вчиненням правочинів через мережі електрозв'язку у сфері господарювання; відносини, пов'язані із використанням електронних документів; відносини, пов'язані із використанням електронного цифрового підпису.

Як встановлено Указом Президента України від 22 січня 2000 р. "Про запровадження єдиної державної регуляторної політики у сфері підприємництва" № 89/2000 [77], єдина державна регуляторна політика у сфері підприємництва здійснюється шляхом впорядкування нормативного регулювання підприємницької діяльності, і одним з основних принципів впорядкування нормативного регулювання підприємницької діяльності є доцільність, достатність та відповідність нормативного регулювання вимогам ринкових відносин (п. 3 Указу).

Виходячи з цього, вважаємо, що для доцільного, достатнього та відповідного нормативного регулювання електронної комерції в Україні необхідно було б прийняти Закон "Про електронну комерцію", який би регулював відносини, що виникають під час здійснення електронної комерції, а саме від поняття електронної комерції, електронного документа до вчинення правочинів через мережі електрозв'язку. Визначення правового статусу ЕЦП та регулювання відносини у сфері використання ЕЦП регулюється Законом України від 22 травня 2003 року "Про електронний цифровий підпис".

[4] Необхідно зазначити, що у США, в європейських країнах використовується поняття electronic commerce (e-commerce), яке часто неправильно перекладається на російську та українську мови як електронна торгівля. Ми вважаємо, що лінгвістично та юридично правильним є переклад цього поняття як електронна комерція.

Саме такий шлях запропоновано Типовим законом ЮНСІТРАЛ "Про електронну комерцію", Директивою ЄС "Про деякі правові аспекти послуг інформаційного суспільства, в тому числі електронної комерції, на внутрішньому ринку".

У ряді держав світу ведеться законопроектна робота з врегулювання відносин у сфері електронної комерції. Наприклад, у Російській Федерації до Державної Думи подано цілий ряд законопроектів у цій сфері: "Про електронну торгівлю" [78], "Про правочини, що вчиняються за допомогою електронних засобів (Про електронні правочини)" [79]. В Україні на розгляді у Верховній Раді знаходиться законопроект "Про електронну торгівлю". Закони "Про електронний цифровий підпис" прийняті у таких державах, як Італія, Ізраїль, Німеччина, Російська Федерація, США, Україна та ін.

В юридичній літературі [90, с. 19, 81, 82, с. 140, 83, 84, 85, с. 20–30, 86, 87] справедливо приділяється значна увага дослідженню поняття "електронна комерція", хоч єдина точка зору щодо визначення цього поняття відсутня. З метою забезпечення чіткості правового регулювання необхідно на доктринальному та законодавчому рівні виробити єдине розуміння даного поняття, а звідси чітко визначити, яке коло відносин включає електронна комерція.

Існуючі в літературі підходи до визначення електронної комерції можна умовно розділити на дві групи. Перша група авторів розуміє електронну комерцію як вчинення правочинів, передбачених законодавством, через мережі електрозв'язку, зокрема через Інтернет (Н. Солов'яненко, А. Шамраєв, М.М. Кулешів, І.Т. Балабанов, Л. Новомлинський та інші). Саме такий підхід до розуміння електронної комерції є найбільш поширений і, по суті, прийнятий. Загальною ознакою, що поєднує ці визначення, є те, що правочини вчиняються через мережі електрозв'язку, наприклад через Інтернет.

У той же час серед цієї групи вчених немає єдності щодо того, які правочини можуть вчинятися через мережі електрозв'язку. Так, А. Шамраєв називає предметом електронної комерції відносини, що виникають при вчиненні правочинів електронним способом. Н. Солов'яненко визначає електронну

комерцію як укладання на міжнародних та внутрішніх ринках у комп'ютерній формі правочинів [88]. І.Т. Балабанов розуміє під електронною комерцією торгівлю через мережу Інтернет за допомогою комп'ютерів покупця та продавця [89, с. 73]. О. Шевченко розуміє під електронною торгівлею звичну для нас торгівлю, але таку, що здійснюється завдяки мережі Інтернет [227]. А. Оперкент дає таке визначення електронної комерції – це економічний процес обміну товарами та послугами на базі існуючих партнерських зв'язків за допомогою електронних засобів комунікації [90]. Л. Новомлинський розуміє електронну комерцію як будь-яку трансакцію, яка вчиняється за допомогою мережі пов'язаних між собою комп'ютерів, по завершенні якої відбувається передача прав власності або прав користування речовим товаром чи послугою [91].

Найбільш вдало сфера застосування електронної комерції передбачена Типовим законом ЮНСІТРАЛ "Про електронну комерцію", в якому зазначено, що сферою застосування електронної комерції є всі відносини комерційного характеру, а саме вчинення таких правочинів, але не обмежуючись ними: будь-які торгові правочини на поставку або обмін товарами чи послугами, дистриб'юторські правочини, комерційне представництво та агентські відносини, факторинг, лізинг, правочини на будівництво промислових об'єктів, консалтинг, інжиніринг, ліцензійні правочини, інвестування, фінансування, банківські послуги, страхування, правочини про експлуатацію або концесії, договірне оформлення спільних підприємств та інших форм промислового та ділового співробітництва, правочини на перевезення товарів та пасажирів повітряним, морським, залізничним або автомобільним транспортом. Тобто, Типовий закон встановлює загальнодозвільне правило, за яким залучає до сфери електронної комерції вчинення всіх можливих договорів. В той же час передбачається можливість кожній державі, що приймає законодавство у сфері електронної комерції, встановити певні винятки з цього правила, тобто передбачити правочини, які не можуть вчинятися через мережі електрозв'язку.

Таке загальнодозвільне правило повинно бути запозичене українським законодавцем, і передбачене як у спеціальному законі про електронну комерцію (таке положення передбачене у законопроекті України "Про електронну торгівлю"), так і в ЦКУ, який містить прямо протилежне правило. Так, ст. 207 ч. 3 ЦКУ передбачає, що "використання при вчиненні правочинів ... електронно-числового підпису ... допускається у випадках, встановлених законом, іншими актами цивільного законодавства, або за письмовою згодою сторін, у якій мають міститися зразки відповідного аналога їхніх власноручних підписів". Норма аналогічного змісту закріплена і в ст. 160 ч. 2 ЦК РФ [92, с. 346].

Такий підхід був запозичений багатьма державами світу (Канада, США, Туніс та інші), які, відштовхуючись від Типового закону, приймали національні закони про електронну комерцію. Аналогічні положення про перелік правочинів, які можуть вчинятися через мережі електрозв'язку, закріплені і в законопроекті РФ "Про електронну торгівлю", законопроекті України "Про електронну торгівлю", де, зокрема передбачено, що електронна торгівля – це укладання шляхом обміну електронними документами будь-яких цивільно-правових правочинів, а також придбання і здійснення з використанням електронних засобів інших прав і обов'язків у сфері підприємницької діяльності. Тобто відбувається запозичення законодавцями різних країн світу підходу, запропонованого Типовим законом ЮНСІТРАЛ, що призведе до уніфікації законодавства у сфері електронної комерції.

Друга група авторів розуміє під електронною комерцією одну з форм організації та здійснення господарської діяльності (М.М. Дутов, В. Наумов, А.А. Тедєєв, Б. Скородумов). Наприклад, М.М. Дутов пропонує розуміти електронну комерцію як одну з сучасних форм організації і здійснення господарської, переважно банківської і торговельної, діяльності [93, с. 1]. А.А. Тедєєв під електронною комерцією (електронною економічною діяльністю, що здійснюється з використанням комп'ютерної мережі Інтернет) розуміє підприємницьку діяльність, а також тісно пов'язану з нею непідприємницьку діяльність, що

здійснюється у принципово новій, електронній формі з використанням сучасних комунікаційних засобів у інформаційному середовищі глобальної комп'ютерної мережі Інтернет [94]. В. Наумов під електронною торгівлею розуміє комерційну діяльність у сфері реклами та поширення товарів і послуг за допомогою використання мережі Інтернет [95]. Б. Скородумов пропонує визначати електронну комерцію як будь-яку форму бізнес-процесів, в якій взаємодія між суб'єктами відбувається електронним чином та супроводжується фізичним переміщенням інформаційних або інших матеріальних ресурсів [96].

Такий підхід є досить спірним і недостатньо обґрунтованим. Ні в законодавстві, ні в доктрині господарського права України не міститься понять форми організації господарської діяльності та форми здійснення господарської діяльності. Представники цієї точки зору також не дають цих визначень і не наводять належної аргументації на підтримку саме такого широкого розуміння електронної комерції. Кваліфікація електронної комерції як підприємницької та пов'язаної з нею непідприємницької діяльності не відповідає положенням Типового закону ЮНСІТРАЛ "Про електронну комерцію".

Необхідно зазначити, що чинними законами України та підзаконними нормативними актами поняття електронної комерції не передбачено, його визначення відсутнє. В той же час, протягом невеликого проміжку часу в законодавстві України існувало поняття "системи електронної комерції". Так, 24 вересня 1999 р. Правління Національного банку України прийняло постанову № 479[5], якою було затверджено Положення "Про порядок емісії платіжних карток і здійснення операцій з їх застосуванням" [97]. Вказане положення встановлювало загальні вимоги Національного банку України до порядку здійснення банками емісії платіжних карток, визначало операції, що здійснюються з їх застосуванням, та порядок розрахунків за цими операціями, а також установлювало загальні вимоги до внутрішніх

[5] Постанова втратила чинність на підставі Постанови Нацбанку № 367 від 27 серпня 2001 р.

платіжних систем, що створюються в Україні. У контексті даного положення використовувалося поняття системи електронної комерції, яка визначалася як сукупність програмно-технічних засобів, процедур та правил, використання яких дає змогу споживачу здійснити віддалений доступ до прейскурантів підприємств торгівлі (послуг), виконати замовлення на поставку та оплату замовлених товарів (послуг).

Таке визначення цілком справедливо вказувало на таку ознаку електронної комерції як її системність. Сукупність програмно-технічних засобів, процедур та правил регламентує порядок використання електронних документів, електронного цифрового підпису, електронний документообіг, що у своїй сукупності дозволяє вчиняти правочини через мережі електрозв'язку. Системність електронної комерції також полягає в тому, що вона включає в себе не тільки укладання правочинів через мережі електрозв'язку, а й дає змогу контрагентам виконати замовлення та оплатити замовлені товари.

Загальною ознакою наведених вище двох підходів до розуміння електронної комерції є використання сучасних засобів зв'язку – мереж електрозв'язку, наприклад, Інтернет. Причому більш коректно буде говорити про використання мереж електрозв'язку без уточнення якої саме, оскільки такими мережами можуть бути не тільки Інтернет, а й інші мережі загального або локального характеру (навіть з урахуванням майбутніх мереж) [98], що ніяким чином не впливає на зміст самого поняття електронної комерції.

Вказана ознака – використання мереж електрозв'язку для здійснення електронної комерції – авторами обох підходів називається як кваліфікуюча ознака електронної комерції [99, с. 23, 100], і тягне за собою необхідність правового регулювання відносин у сфері електронного документа і документообігу, а також у сфері використання електронних підписів в контексті електронної комерції.

Отже можна зробити висновок про те, що електронна комерція характеризується такими ознаками:

1) електронна комерція є комплексним, системним поняттям, яке включає відносини у сфері вчинення правочинів, у сфері електронного документа та електронного документообігу, у сфері використання електронних підписів;
2) для електронної комерції мережі електрозв'язку є, перш за все, середовищем вчинення правочинів та надання банківських послуг;
3) електронна комерція не пов'язується з використанням якоїсь однієї чітко встановленої мережі електрозв'язку. Вчинення правочинів з використанням електронних засобів зв'язку може відбуватися як через мережу Інтернет, так і через будь-яку іншу мережу електрозв'язку, яка дозволяє здійснювати обмін електронними документами;
4) перелік правочинів, які можуть вчинятися з використанням мереж електрозв'язку, невичерпний; загальним правилом повинно бути положення про загальнодозвільний порядок вчинення правочинів з використанням електронних засобів зв'язку. Винятки з цього правила можуть бути встановлені законом.

Виходячи з наведених ознак, пропонуємо визначення електронної комерції в Україні як системи взаємопов'язаних правовідносин у сфері вчинення правочинів шляхом обміну електронними документами, який здійснюється за допомогою використання мереж електрозв'язку, зокрема Інтернет.

Таким чином, електронна комерція охоплює три групи відносин:

1) відносини, пов'язані із вчиненням правочинів через мережі електрозв'язку у сфері господарювання;
2) відносини, пов'язані із використанням та обміном електронними документами;
3) відносини, пов'язані із використанням електронних підписів.

Першу, основну і найбільш велику групу складають відносини, пов'язані із вчиненням правочинів у сфері господарювання. Поняття "вчинення правочину" охоплює проміжок часу від його укладання до проведеного належним чином виконання,

яким, за загальним правилом (ст. 599 ЦК України), припиняється зобов'язання.

Одним з інститутів господарського права є господарський договір, який є однією з найпоширених підстав виникнення зобов'язань[6]. Не вдаючись до наукової дискусії про правову природу господарського договору, приєднаємося до визначення, запропонованого О.А. Беляневич: господарський договір – це засноване на правочині сторін і зафіксоване у встановленій законом формі зобов'язальне правовідношення між суб'єктами господарювання, змістом якого є взаємні права і обов'язки сторін у галузі господарської діяльності [101, с. 145].

Вчинення правочинів у сфері господарювання за загальним правилом відбувається у письмовій формі. Це правило встановлене ст. 208 ЦКУ, яка передбачає, що у письмовій формі належить вчиняти правочини, зокрема, між юридичними особами. Частина 7 ст. 179 Господарського кодексу України містить відсильну норму, яка передбачає, що господарські договори укладаються за правилами, встановленими ЦКУ з урахуванням особливостей, передбачених ГКУ, іншими нормативними актами щодо окремих видів договорів. На необхідність додержання письмової форми господарських договорів зазначається і в матеріалах судової практики [102, п. 6]. Таким чином, закон вимагає, щоб господарські договори укладалися письмово і були підписані уповноваженими особами.

Традиційним матеріальним носієм письмової форми виступав папір. Сучасний розвиток інформаційних технологій надав суспільству новий вид матеріального носія – електронний. Отже, використання нового матеріального носія (електронного) при вчиненні господарських договорів для забезпечення виконання законодавчої вимоги дотримання письмової форми призвело до відокремлення групи господарських договорів, які

[6] В силу господарського зобов'язання один суб'єкт господарювання зобов'язаний вчинити певні дії господарського характеру, як-то: перерахувати гроші, поставити товар, виконати роботу, надати ділову інформацію, тощо. А інший суб'єкт вправі вимагати від зобов'язаної сторони виконання цих дій.

вчиняються з використанням електронних засобів зв'язку. Зазначена відокремлена група господарських договорів і становить ядро електронної комерції.

Як цілком справедливо зазначають А. Орлов та А. Ананьев [99, с. 23], правочини у сфері електронної комерції не мають ніяких інших особливостей крім тієї, що укладаються з використанням електронних засобів телекомунікацій.

Окремо необхідно згадати, що ч.1 ст. 181 ГКУ дає змогу контрагентам обирати певну письмову форму господарського договору. Зокрема, такі господарські договори, як договір поставки, міни, купівлі-продажу, можуть укладатися у формі одного письмового документа, що підписується сторонами. Це так звана повна письмова форма. Крім цього, договірні відносини між контрагентами можуть бути встановлені у так званій скороченій письмовій формі – шляхом обміну листами, радіограмами, телеграмами, телетайпограмами, телефонограмами та ін. Вказані положення ГКУ повторюються у ряді роз'яснень ВАСУ [103, с. 95, 104, с. 113].

Отже, законодавець допускає укладання договорів у письмовій формі, наприклад, шляхом обміну телефонограмами, які при передачі засобами телефонного зв'язку не фіксуються на матеріальному носії. Порівняно з телефонограмами електронна комерція, що дозволяє укладати договори через мережі електрозв'язку з фіксуванням змісту договору на електронних носіях, що об'єктивується у вигляді електронного документа, уявляється нам юридично більш визначеною.

М.І. Брагінський, визнаючи господарські договори різновидом цивільно-правових, відмічає, що господарські договори мають певну специфіку і, відповідно, вони мають окрім родових і видові ознаки [105, с. 10]. Видовими ознаками господарських договорів, що вирізняють їх з решти договорів, М.І. Брагінський називає те, що:

1) суб'єктами такого договору є фізичні або юридичні особи, зареєстровані у встановленому законом порядку як суб'єкти підприємницької діяльності;

2) зміст господарського договору складають умови, на яких передаються товари, виконуються роботи чи надаються послуги з метою здійснення господарської діяльності чи з іншою метою, не пов'язаною із особистим споживанням;
3) господарський договір втілюється у повній чи скороченій письмовій формі;
4) для окремих видів господарських договорів, зокрема зовнішньоекономічних контрактів чи біржових правочинів, може встановлюватися окремий порядок їх укладання (підписання), обліку та реєстрації;
5) певні особливості можуть також характеризувати порядок виконання або умови відповідальності за господарським договором (наприклад, відповідальність підприємця незалежно від його вини).

Відштовхуючись від запропонованого визначення електронної комерції та її ознак, необхідно зазначити, що господарські договори, вчинення яких складає перший блок правовідносин у сфері електронної комерції, окрім зазначених вище видових ознак, характеризуються й іншими ознаками, які породжені використанням мереж електрозв'язку для їх укладання. До таких ознак можна віднести наступне:

- у сфері електронної комерції використовуються такі мережі електрозв'язку, які є придатними для створення, зберігання, обміну електронними документами (наприклад Інтернет);
- такі мережі електрозв'язку виступають середовищем вчинення правочинів;
- перелік правочинів, які можуть вчинятися з використанням мереж електрозв'язку, невичерпний.

Таким чином, вчинення господарських договорів з використанням мережі електрозв'язку ґрунтується на загальних цивілістичних положеннях про вчинення правочинів; на загальних положеннях господарського права щодо вчинення господарських договорів; та на спеціальних положеннях, які регламентують особливості вчинення господарських договорів через мережі електрозв'язку.

В юридичній літературі та законодавстві в зв'язку з поняттям електронної комерції використовується поняття електронного документа. Отже, другий блок відносин у сфері електронної комерції складають відносини, пов'язані із використанням електронних документів.

Як уже зазначалося, кваліфікуючою ознакою правочинів у сфері електронної комерції є їх укладання з використанням мереж електрозв'язку. Саме ця ознака призвела до необхідності дослідження такого поняття, як електронний документ, в якому формалізується правочин, укладений у сфері електронної комерції.

У законодавстві України вже тривалий час вживається поняття електронного документа, даються різні його визначення. Серед таких нормативних актів можна назвати: Закон України від 5 квітня 2001 р. "Про платіжні системи та переказ грошей в Україні", Постанову Правління НБУ України від 27 грудня 1999 р. (в редакції 23 квітня 2002 р.), якою затверджена Інструкція "Про міжбанківські розрахунки в Україні" № 621, Постанову Правління НБУ від 29 березня 2001 р. (в редакції 4 грудня 2001 р.), якою затверджена Інструкція "Про безготівкові розрахунки в Україні в національній валюті" № 135, Постанову Правління НБУ від 10 червня 1999 р. (в редакції 4 грудня 2002 р.), якою затверджені "Правила організації захисту електронних банківських документів" № 280, тощо.

Основним недоліком визначень поняття електронного документа у згаданих вище нормативних актах є те, що всі вони є вузькоспеціалізованими, спрямованими на застосування у розрахункових відносинах.

В юридичній літературі [80, с. 19, 82, с. 140, 106, 92, 107, 108, 109] також приділяється достатньо уваги дослідженню цього поняття, що однак не привело до формування чіткого підходу чи підходів до визначення цього поняття.

Законодавство, що регулює відносини, пов'язані з використанням електронних документів у сфері електронної комерції, повинно дати відповідь на такі питання: що таке електронний документ; що є оригіналом та копією електронних документів; які вимоги повинні висуватися до зберігання

електронних документів; що повинно вважатися відправленням та одержанням електронних документів; крім того, повинен бути визначений правовий статус інформаційних посередників; забезпечена можливість використання електронних документів як судових доказів (відразу зазначимо, що останнє зазначене коло відносин потребує окремого ретельного правового дослідження, а тому у зв'язку з обмеженістю обсягу роботи не буде в ній розглядатися).

Третій блок правовідносин у сфері електронної комерції складають відносини, пов'язані із використанням електронних підписів. Правочин, укладений у сфері електронної комерції, втілюється в електронному документі. Підтвердження волевиявлення контрагента на укладання такого правочину відбувається за допомогою вчинення електронного підпису уповноваженої особи.

Необхідно зазначити, що у вітчизняній юридичній літературі [93, 80, 81, 110, 112] одночасно використовуються такі поняття, як електронний підпис, електронний цифровий підпис, цифровий підпис. Автори не приділяють уваги співвідношенню цих понять, часто вживають їх як синоніми, що є хибним підходом. Поняття електронного підпису є загальним, а ЕЦП – його різновид. Тобто поняття електронного підпису поширюється на всі пов'язані з електронним документом символи, коди, паролі, тощо, в тому числі такі, які не є власне електронним цифровим підписом. Вони можуть розглядатися як підпис, якщо виконані та прийняті сторонами за взаємною згодою та з явним наміром підтвердити дійсність написаного, при цьому законодавство про електронні цифрові підписи на такі електронні підписи не повинно поширюватися. Детальніше це питання буде розглянуто у розділі 2 посібника.

Один з найбільш важливих етапів оформлення будь-якого договору, зокрема й договору, який укладається через мережі електрозв'язку, – його підписання, оскільки підпис узаконює його. Як правило, акт підписання включає в себе власноручний

підпис першої особи підприємства або його повноважного представника, а також відбиток печатки організації, що є підтвердженням повноважень особи, яка підписала договір [113, с. 4] (ч. 1 ст. 181 ГКУ).

Таким чином, одним з головних реквізитів документів є підпис. Він підтверджує факт взаємозв'язку між відомостями, які містяться в документі, та особою, яка підписала документ, тобто є одним із засобів ідентифікації особи [114]. В основу використання рукописного підпису, як засобу ідентифікації, покладена гіпотеза про унікальність особистих біометричних параметрів людини.

Недоліком рукописного підпису є функціональний недолік, пов'язаний з тим, що рукописний підпис забезпечує лише підтвердження його відношення до особи, яка поставила підпис (ідентифікація), але не забезпечує його цілісності та незмінності (аутентифікація). Без спеціальних додаткових заходів захисту рукописний підпис не гарантує того факту, що документ не піддавався змістовним змінам у процесі зберігання або транспортування.

Характерною особливістю рукописного підпису є його нерозривний фізичний зв'язок з носієм інформації. Тобто рукописний підпис можливий лише на документах, які мають матеріальну природу. Електронні документи, які мають логічну природу, до цієї категорії не відносяться. Отже, при укладанні правочинів, факт яких посвідчується рукописним підписом, сторони-учасники повинні знаходитися або у безпосередньому контакті, або у опосередкованому, через матеріальний носій та послуги сторонніх організацій (служба доставки, тощо). Основний зміст електронної комерції полягає у можливості вчинення правочинів без фізичної взаємодії між контрагентами, тобто вони позбавляються необхідності фізично приїздити та зустрічатися один з одним, що досягається через використання електронних документів, які за своєю природою не можуть бути ідентифіковані рукописним підписом.

На відміну від рукописного підпису електронний цифровий підпис (ЕЦП) має не фізичну, а логічну природу, тобто є по-

слідовністю символів, що дозволяє однозначно пов'язати автора документа, зміст документа та володільця ЕЦП. Логічний характер електронного цифрового підпису робить його незалежним від матеріальної природи документа. За його допомогою можна ідентифікувати та аутентифікувати документи, що мають електронну природу.

Серед позитивних властивостей електронного цифрового підпису можна назвати [115, с. 310–311]:

1) незалежність електронного цифрового підпису від носія дозволяє використовувати його для надання юридичної сили електронним документам, в яких матеріалізуються правочини, вчинені через мережі електрозв'язку;
2) можливість розширити функціональні властивості підпису за рахунок криптографічних засобів (засобів шифрування), що лежать в основі механізму роботи засобів електронного цифрового підпису;
3) ефективність створення, використання та зберігання електронних документів може бути значно підвищена за рахунок автоматизації процесів створення, застосування, посвідчення та перевірки ЕЦП;
4) надійність (захисні властивості) електронного цифрового підпису при використанні сертифікованих засобів ЕЦП вища ніж ручних.

Правовідносини, пов'язані із використанням ЕЦП, досить складні, що пов'язано не тільки з новизною цього явища в Україні та світі, а з тим, що тісний зв'язок між електронним цифровим підписом та електронною комерцією змушує суспільство висувати до держави високі вимоги щодо захисту прав та законних інтересів учасників правовідносин у сфері використання ЕЦП. І в першу чергу, на законодавчому та доктринальному рівні необхідно прийти до однакового розуміння поняття електронного цифрового підпису, його правового режиму.

Правове регулювання використання ЕЦП в електронній комерції включає два аспекти – легалізацію електронного цифрового підпису та державне регулювання відносин у сфері використання ЕЦП в електронній комерції. Кожен з

цих аспектів вимагає окремого розгляду і буде розглянутий у розділі 3 посібника.

Як уже відзначалося, електронна комерція – це нове комплексне поняття, яке включає широке коло відносин, зокрема вчинення правочинів через мережі електрозв'язку. Основною відмінною ознакою, що дозволяє виділити такі правочини зі всієї маси господарських договорів, є використання при їх вчиненні мереж електрозв'язку, зокрема Інтернет. Використання таких технічних засобів стало причиною появи в юридичній літературі та законодавстві ряду нових термінів (електронний підпис, інформаційні посередники, тощо), які раніше не використовувалися і зміст яких різними нормативними актами та авторами визначається по-різному.

Зазначені обставини вимагають наукового і законодавчого осмислення та запровадження ряду понять, які використовуються у зв'язку зі вчиненням правочинів через мережі електрозв'язку.

Визначення запропонованих нижче понять знайшли своє відображення у законах України "Про електронний цифровий підпис", "Про телекомунікації", ряді підзаконних нормативних актів, у законопроектах України "Про електронну торгівлю", "Про електронний документ та електронний документообіг", у чинному законодавстві і законопроектах інших країн, наприклад, РФ "Про електронну торгівлю", "Про правочини, що вчиняються за допомогою електронних засобів (Про електронні правочини)".

Обрання та запровадження нових понять повинно ґрунтуватися на таких критеріях, як: доцільність запровадження нового поняття; чіткість викладення його змісту; мінімальна завантаженість технічними термінами та термінами іноземного походження як самого поняття, так і його визначення тощо.

Серед понять, що повинні офіційно використовуватися в електронній комерції, можна назвати такі:

1. Електронні носії – магнітний диск, магнітна стрічка, лазерний диск та інші матеріальні носії, які використовуються для запису та зберігання інформації за допомогою електронно-обчислювальної техніки.

2. Електронні документи – це документи, складені певними та компетентними установами, підприємствами, організаціями, посадовими особами, а також громадянами, які містять юридично значущі відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі, зафіксовані на електронному носії.

3. Відправник електронного документа – фізична або юридична особа, якими або від імені яких відправляються електронні документи, за виключенням осіб, які діють в якості інформаційних посередників щодо даного електронного документа.

4. Одержувач електронного документа (адресат) – фізична або юридична особа, якій електронні документи надсилаються відправником або від імені відправника, за виключенням осіб, які діють в якості інформаційних посередників щодо даного електронного документа.

5. Інформаційна система – система, призначена для формування, відправлення, одержання, зберігання або іншої обробки електронних документів.

6. Інформаційний посередник – це юридична особа, яка надає послуги у сфері господарської діяльності на умовах оплатності, на відстані за допомогою електронного обладнання, яке використовується для переробки та зберігання інформації, та за індивідуальним запитом осіб, що здійснюють електронну комерцію. Такими послугами можуть бути, наприклад, послуги, надання яких забезпечують механізми, що дозволяють пошук, доступ та отримання інформації; послуги, що складаються з передачі інформації через мережу зв'язку, надання доступу до мережі зв'язку чи послуги по розміщенню інформації, що надається одержувачем послуг; послуги, що передаються від одного місця до іншого, такі як надання відеопослуг за запитом, або відправлення електронних документів за допомогою електронної пошти.

7. Особа, яка здійснює електронну комерцію, – юридична або фізична особа, яка є суб'єктом підприємницької діяльності, що здійснює з використанням електронних документів укладання та виконання будь-яких цивільно-правових правочинів.

8. Електронний підпис – електронні дані, які додаються до інших електронних даних або логічно з ним пов'язані та призначені для ідентифікації підписувача цих даних.

9. Електронний цифровий підпис (ЕЦП) – вид електронного підпису, представлений у формі електронних даних, одержаних шляхом криптографічного перетворення інформації, який дозволяє ідентифікувати володільця сертифіката ключа підпису та встановити істинність електронного документа, відкритий ключ якого має чинний на момент використання сертифікат.

10. Засоби ЕЦП – програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів та/або перевірки ЕЦП.

11. Сертифікат на засіб ЕЦП – документ на паперовому носії, виданий за правилами системи сертифікації для підтвердження відповідності засобів електронного цифрового підпису встановленим вимогам.

12. Закритий ключ ЕЦП – унікальна послідовність символів, відома володільцю сертифіката ключа підпису, та призначена для створення в електронних документах електронного цифрового підпису з використанням засобів ЕЦП.

13. Відкритий ключ ЕЦП – унікальна послідовність символів, яка відповідає закритому ключу електронного цифрового підпису, доступна будь-якому користувачу мережі електрозв'язку та призначена для підтвердження з використанням засобів ЕЦП оригінальності електронного цифрового підпису в електронному документі.

14. Користувач відкритого ключа ЕЦП – особа, яка використовує відкритий ключ електронного цифрового підпису.

15. Сертифікат відкритого ключа ЕЦП (сертифікат ключа підпису) – електронний документ з електронним цифровим підписом уповноваженої особи провайдера сертифікаційних послуг або документ на паперовому носії, які включають в себе відкритий ключ ЕЦП та які видаються провайдером сертифікаційних послуг учаснику мережі електрозв'язку для підтвердження дійсності електронного цифрового підпису та ідентифікації володільця сертифіката ключа підпису.

16. Володілець сертифіката ключа підпису (володілець сертифіката) – фізична особа, на ім'я якої провайдером сертифікаційних послуг виданий сертифікат ключа підпису, і яка володіє відповідним закритим ключем електронного цифрового підпису, який дозволяє за допомогою засобів ЕЦП створювати свій електронний цифровий підпис в електронних документах (підписувати електронні документи).

17. Послуги електронного цифрового підпису – надання у користування засобів цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих та блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги у зазначеній сфері.

18. Провайдер сертифікаційних послуг – юридична особа, яка має повноваження посвідчувати відповідність відкритого ключа електронного цифрового підпису закритому ключу особи, на чиє ім'я виданий сертифікат.

19. Підтвердження дійсності електронного цифрового підпису в електронному документі – позитивний результат перевірки відповідним сертифікованим засобом електронного цифрового підпису з використанням сертифіката ключа підпису приналежності електронного цифрового підпису в електронному документі володільцю сертифіката ключа підпису та відсутності викривлень у підписаному даним електронний цифровим підписом електронному документі.

1.2. Суб'єкти правовідносин у сфері електронної комерції

Суб'єктом правовідносин є правоздатний суб'єкт суспільного життя, який є носієм юридичних прав та обов'язків [116, с. 128], а звідси суб'єктами господарського права є учасники господарських відносин, які безпосередньо здійснюють господарську діяльність або управляють такою діяльністю, створені у встановленому законом порядку, мають необхідне для

здійснення такої діяльності майно і володіють господарською правосуб'єктністю [117, с. 104].

Отже, однією з ознак суб'єктів господарського права є наявність господарської правосуб'єктності, тобто визнаної державою за певним суб'єктом господарювання можливості бути суб'єктом права (мати і здійснювати господарські права та обов'язки, відповідати за їх належне виконання і мати юридичну можливість захищати свої права та законні інтереси від можливих порушень); обсяг господарської правосуб'єктності учасників господарських правовідносин фіксується в законі та в їхніх установчих документах.

Електронна комерція включає три групи відносин (вчинення правочинів через мережі електрозв'язку, відносини у сфері електронного документа та електронного документообігу, використання електронних підписів), сукупність яких дозволяє віднести до її суб'єктів:

- суб'єктів господарського права, які вчиняють правочини через мережі електрозв'язку з використанням електронних документів (особи, які здійснюють електронну комерцію);
- інформаційних посередників[7], які забезпечують процес обміну електронними документами, зберігають їх чи надають інші послуги щодо цих документів;
- провайдерів сертифікаційних послуг (центри сертифікації ключів, акредитовані центри сертифікації ключів, засвідчувальний центр).

Чинне законодавство України та доктрина господарського права України ще не містять визначення суб'єкта електронної комерції та переліку таких суб'єктів. Законопроект України "Про електронну торгівлю" використовує поняття електронного торгівця, під яким розуміють юридичну або фізичну особу, яка є суб'єктом підприємницької діяльності, що здійснює з ви-

[7] Необхідно зазначити, що термін "інформаційний посередник" повинен розглядатися не як родова категорія, а стосовно кожної окремої послуги, оскільки одна й та ж особа може виступати одержувачем однієї послуг та інформаційним посередником стосовно іншої послуги.

користанням електронних документів укладання та виконання будь-яких цивільно-правових правочинів. Слід зазначити що, дане визначення є прийнятним за змістом, але сам запропонований термін "електронний торгівець" є не зовсім вдалим. Термін "особа, що здійснює електронну комерцію"[8] уявляється більш адекватним та юридично ємним.

Центральне місце серед суб'єктів електронної комерції займають інформаційні посередники. Інформаційний посередник – це юридична особа, яка надає послуги у сфері господарської діяльності на умовах оплатності на відстані, за допомогою електронного обладнання, яке використовується для переробки та зберігання інформації та за індивідуальним запитом особи, яка здійснює електронну комерцію. Зазначені особи надають такі послуги у сфері електронної комерції: послуги, надання яких забезпечує механізми, що дозволяють пошук, доступ та отримання інформації; послуги, що складаються з передачі інформації через мережу зв'язку, надання доступу до мережі зв'язку чи послуги по розміщенню інформації, що надається особами, які здійснюють електронну комерцію; послуги, що передаються від одного місця до іншого, такі як надання відеопослуг за запитом, або відправлення електронних документів за допомогою електронної пошти.

У зв'язку з обмеженістю обсягів посібника ми не маємо змоги розглянути особливості надання інформаційними посередниками такої послуги, як доступ до мереж електрозв'язку, та проаналізувати відповідність світової практики і вітчизняних реалій в цій частині, а також особливості зобов'язань, які виникають у зв'язку з наданням послуг через мережі електрозв'язку, що є предметом дослідження інших авторів [65, 118]. Розглянемо лише ті аспекти діяльності інформаційних посередників, які безпосередньо пов'язані із вчиненням правочинів через мережі електрозв'язку.

[8] Так, наприклад, саме такий термін використовується у законопроекті РФ "Про правочини, що вчиняються за допомогою електронних засобів (Про електронні правочини)".

Іншим суб'єктом електронної комерції виступає особа, яка здійснює електронну комерцію. Це фізична або юридична особа, яка з метою здійснення господарської діяльності використовує послуги, які надаються інформаційним посередником, зокрема з метою пошуку інформації та доступу до неї, та вчиняє правочини через мережі електрозв'язку.

У посібнику зроблено акцент саме на тих послугах інформаційних посередників, які безпосередньо обслуговують вчинення господарських договорів через мережі електрозв'язку.

Оскільки будь-який суб'єкт господарського права в силу своєї господарської правосуб'єктності має право вчиняти правочини (в т.ч. укладати господарські договори), то кожен з суб'єктів при вчиненні ним через мережі електрозв'язку таких правочинів буде залучатися до сфери електронної комерції і буде розглядатися, відповідно, як суб'єкт правовідносин у сфері електронної комерції. Причому можливість вчинення таких правочинів ґрунтується на послугах інформаційних посередників, а також на послугах, які надають провайдери сертифікаційних послуг в частині створення та сертифікації ключів електронного цифрового підпису.

Таким чином, ще одним суб'єктом електронної комерції виступають провайдери сертифікаційних послуг. Прийнятий 22 травня 2003 р. Закон України "Про електронний цифровий підпис" не містить такого терміна. Він був запропонований нами для зручності викладення матеріалу в межах цього дослідження як родове поняття, що включає всіх суб'єктів, які надають послуги ЕЦП: центри сертифікації ключів, акредитовані центри сертифікації ключів, засвідчувальний центр (ст. ст. 8–10 названого Закону), які перебувають у певній ієрархії один відносно одного.

Центри сертифікації ключів, акредитовані центр сертифікації ключів та засвідчувальні центри є юридичними особами або фізичними особами, які є суб'єктами підприємницької діяльності, та надають послуги ЕЦП. Різниця між першими двома суб'єктами полягає у тому, що акредитований центр сер-

тифікації ключів повинен пройти акредитацію[9], порядок проведення якої повинен встановити Кабінет Міністрів України (ч. 4 ст. 9 зазначеного Закону), і має право видавати лише так звані посилені сертифікати ключів підписів (ч. 2 ст. 9 зазначеного Закону). Більш детально питання акредитації центрів сертифікації та видачі посилених сертифікатів буде розглянуто у розділі 3. Засвідчувальний центр за обсягом своїх повноважень не відрізняється від акредитованого центру сертифікації, але видавати посилені сертифікати він має право лише центральним органам виконавчої влади та підпорядкованим ним підприємствам, організаціям та установам (ч. 1 ст. 10 вказаного Закону). Таким чином, кожний центральний орган виконавчої влади може мати свій засвідчувальний центр.

Підставою для включення провайдерів сертифікаційних послуг до суб'єктів електронної комерції є наданням останніми послуг, пов'язаних із створенням та використанням ЕЦП: сертифікація ключів підписів, ведення реєстру сертифікатів, здійснення підтвердження дійсності ЕЦП в електронних документах щодо виданих ним сертифікатів ключів підписів, тощо.

Існування таких суб'єктів електронної комерції юридично дозволило вчиняти господарські правочини через мережі електрозв'язку. Детальніше правовий статус провайдерів сертифікаційних послуг буде розглянуто в окремому підрозділі.

Із діяльністю зазначеного вище суб'єкта тісно пов'язане існування органу державної виконавчої влади, покликаного здійснювати функцію державного регулювання в такій виключно важливій для суспільства й держави сфері як створення та використання електронного цифрового підпису. Підкреслимо,

[9] Закон України від 22 травня 2003 р. "Про електронний цифровий підпис" у ст. 1 визначає акредитацію як процедуру документального засвідчення компетентності центра сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів; посилений сертифікат ключа підпису – це сертифікат ключа, який відповідає вимогам цього закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом.

що цей орган здійснює державне регулювання саме у зазначеній сфері, а не у сфері всієї електронної комерції.

Таким чином, якщо виникають правовідносини у сфері електронної комерції в частині вчинення господарського договору через мережу електрозв'язку, то суб'єкти таких правовідносин будуть перебувати у горизонтальних правовідносинах без підпорядкування один одному.

1.3. Принципи правового регулювання електронної комерції

Під правовими принципами розуміють основні начала, найбільш загальні керівні положення права, які мають у зв'язку з їх законодавчим закріпленням загальнообов'язковий характер. Такі загальні начала притаманні як праву в цілому (правовій системі), так і окремим правовим галузям, а також підгалузям, інститутам та підінститутам. Відповідно принципи господарського права – це керівні начала, які визначають характер правового регулювання відповідних відносин [119, с. 24].

Значення правових, в тому числі галузевих, принципів подвійне. З одного боку, вони відображають сутність змісту, соціальну спрямованість та головні галузеві особливості правового регулювання. Це дозволяє краще розуміти його зміст, правильно тлумачити та застосовувати конкретні правові норми. З іншого боку, принципи права повинні враховуватися при виявленні прогалин у законодавстві та застосуванні правових норм за аналогією.

Підкреслимо, що правові принципи носять загальнообов'язковий характер, що пов'язано з тим, що вони, як правило, прямо закріплені у відповідних правових нормах. Тому їх дотримання та врахування при розгляді конкретних правовідносин є обов'язковою вимогою закону.

Новизна такого суспільного явища, як електронна комерція, комплексність цього поняття стали причиною того, що новітнє законодавство, призначене для врегулювання всього комплексу відносин у сфері електронної комерції, у більшості держав

світу лише формується. Спочатку правовому регулюванню піддаються окремі відносини (щодо використання електронних підписів, електронних документів, вносяться певні доповнення до цивільного законодавства). Такий стан характерний для більшості держав світу, зокрема й для України.

У вже згадуваному законопроекті України "Про електронну торгівлю" вперше була зроблена спроба сформулювати принципи правового регулювання електронної комерції і, зокрема, зазначено, що правове регулювання електронної торгівлі ґрунтується на принципах рівності її учасників, свободи договору, безперешкодного здійснення підприємницької діяльності, вільного переміщення товарів, послуг і фінансових коштів на всій території України, а також гарантіях судового захисту прав учасників електронної торгівлі. Крім того зазначається, що придбання і здійснення фізичними і юридичними особами прав і обов'язків у сфері електронної торгівлі можуть бути обмежені тільки законами України та постановами Кабінету Міністрів України. Але ж, зазначені у законопроекті принципи властиві господарській діяльності в цілому і не підкреслюють відокремлюючих рис електронної комерції, а це дає підстави звернутися до міжнародного досвіду.

В цьому аспекті заслуговує на увагу положення Типового закону ЮНСІТРАЛ "Про електронну комерцію", який прямо не містить переліку принципів, на яких ґрунтується електронна комерція, але аналіз змісту якого дозволяє виділити такі принципи:

1) вільне здійснення електронної комерції, який означає, що особам, які здійснюють електронну комерцію, не потрібно одержувати попереднього дозволу уповноваженого державного органу на вчинення правочинів через мережі електрозв'язку;
2) недискримінація правочинів, що вчиняються через мережі електрозв'язку, це означає, що паперові матеріальні носії і електронні матеріальні носії письмової форми еквівалентні з точки зору державних органів та судочинства.

Закріплення такого основоположного принципу виключить дискримінацію щодо електронних документів, зробить її неприпустимою, тобто буде забезпечений однаковий правовий режим щодо документів на паперових і електронних носіях;

3) відкритість, або технологічний нейтралітет, що покликано гарантувати, що закон не створює переваг тільки одному виду технології, а є загальним і тому придатним для нових технологій. Крім того, цей принцип дозволяє використовувати різні технологічні рішення з різною надійністю і тому з різними законними наслідками використання таких рішень;
4) гарантування судового захисту прав особам, які здійснюють електронну комерцію.

Отже доцільно запозичити зазначені принципи електронної комерції і зазначити їх у спеціальному комплексному законі про електронну комерцію, що буде сприяти встановленню необхідного та достатнього правового регулювання електронної комерції в Україні.

Вільне здійснення електронної комерції, тобто вчинення правочинів через мережі електрозв'язку, означає, що таке вчинення правочинів не вимагає одержання попереднього дозволу. Зазначений принцип тісно пов'язаний із таким поняттям, як свобода договору. Будь-яка людина вправі втілювати свої інтереси шляхом вільного укладання правочинів, які є для неї найбільш вигідними. [120, с. 78] Суттю договору є співвідношення волі і прагнень договірних сторін. Отже, вільне здійснення електронної комерції означає, що в ідеальному вигляді контрагенти мають свободу укласти договір на свій розсуд і відносно всього того, що може становити для них інтерес.

В частинах 1–2 ст. 67 ГКУ закріплено, що відносини підприємства з іншими підприємствами, організаціями, громадянами в усіх сферах господарської діяльності здійснюються на основі договорів. Підприємства вільні у виборі предмета договору, визначенні зобов'язань, інших умов господарських взаємовідносин, що не суперечить законодавству України.

В той же час у ГКУ, в основу якого покладена ідея оптимального співвідношення приватних та публічних інтересів у галузі господарювання, передбачається обмеження у встановлених випадках вільного розсуду сторін при укладенні договорів (ст. 179).

Таким чином свобода вчинення правочинів через мережі електрозв'язку може бути обмежена чинним законодавством лише двома обставинами: встановленням необхідності дотримання певного порядку укладання господарських договорів у зв'язку з використанням мереж електрозв'язку (порядок обміну електронними документами, тощо), а також визначенням окремих вимог щодо змісту договірного зобов'язання.

Поширеною в юридичній літературі [99, с. 23] є точка зору про те, що вчинення того чи іншого правочину не на паперовому носії, а через мережі електрозв'язку (на електронному носії) не призводить до зміни правової природи та суті договору. Дотримання законодавчої вимоги про необхідність укладання господарських договорів особами, які здійснюють електронну комерцію, у письмовій формі досягається шляхом законодавчого визнання таких господарських договорів, вчинених у письмовій формі. Тобто господарський договір не повинен позбавлятися юридичної сили лише з тієї підстави, що він вчинений на електронному носії та об'єктивований у електронному документі [121, 122]. Зазначений висновок особливо підкреслюється у Типовому законі ЮНСІТРАЛ "Про електронну комерцію" (ст. 11).

Мета запровадження принципу недискримінації правочинів полягає в тому, щоб усунути таку юридичну перепону розвитку електронної комерції, як законодавча вимога дотримання письмової форми. Результатом дії цього принципу стане законодавче визнання господарського договору, вчиненого через мережі електрозв'язку таким, який вчинений у письмовій формі. Відповідно вимога щодо укладання господарських договорів у письмовій формі вважається виконаною.

Із принципу недискримінації господарського договору, вчиненого на електронному носії та об'єктивованого у електронному документі, можна зробити ще один висновок про те, що використ-

тання такого матеріального носія письмової форми, як електронний носій, не може розглядатися як єдина причина для позбавлення господарського договору юридичної сили. З іншого боку, вказаний принцип не повинен тлумачитися як такий, що встановлює юридичну силу будь-якого електронного документа.

Окремо необхідно зазначити на встановлення сфери застосування принципу недискримінації правочинів, які вчиняються через мережі електрозв'язку. Це питання по-різному вирішується в законах або у законопроектах, які обговорюються у різних державах.

Так, Типовий закон ЮНСІТРАЛ "Про електронну комерцію" в ч. 2 ст. 11 "Укладання та дійсність договорів" допускає можливість кожної окремо держави передбачити випадки, коли виключається можливість вчинення правочинів через мережі електрозв'язку. Це було зроблено, оскільки в іншому випадку норми ст. 11 Типового закону можуть мати несприятливі наслідки в результаті створення переважного режиму по відношенню до застосовуваних в іншому випадку положень національного права, які можуть передбачувати конкретні формальності укладання певних правочинів. Такі формальності можуть включати нотаріальне посвідчення й інші вимоги щодо письмової форми та можуть враховувати інші аргументи, пов'язані із публічним порядком, наприклад, необхідність забезпечувати захист певних сторін або попереджувати їх про існування конкретних ризиків [123].

Директива Європейського парламенту та Ради № 2000/31/ЄС від 8 червня 2000 р. у статті 9 передбачає, що держави-учасниці повинні забезпечувати допустимість договорів, які укладаються з використанням електронних засобів, зокрема щоб юридичні вимоги, які застосовуються до договірного процесу, не створювали перепон для їх використання та не призводили до відмови в юридичній чинності з тих причин, що вони були вчинені з використанням електронних засобів. Ця стаття зазначає, що держави-учасниці мають право передбачити у національному законодавстві, що вказане правило не буде застосовуватися до

всіх або певних договорів, що підпадають під одну з наступних категорій:

1) договори, які створюють або передають права на нерухоме майно, за виключенням прав оренди;
2) договори, які вимагають у відповідності із чинним законодавством залучення суду, публічних органів або осіб професій, які виконують публічні функції;
3) договори поруки та закладу цінних паперів, зобов'язаними за якими виступають особи, що діють за межами торгових або підприємницьких цілей;
4) договори, що регулюються сімейним або спадковим правом.

Аналогічні положення закріплені у законі Канади "Про електронну комерцію" (ст. 2 ч. 3), федеральному законі США "Про електронні підписи у міжнародних та внутрішньодержавних торгових відносинах" (ст. 103), у законі штату Юта США "Про електронні правочини" (параграф 46-4-103) тощо.

Чинний закон Республіки Бєларусь "Про електронний документ" від 10 січня 2000 р. у ст. 11 "Юридична сила електронного документа" передбачає, що у випадках, коли законодавством Республіки Бєларусь вимагаються нотаріальне посвідчення та (або) державна реєстрація документа, посвідченню та (або) реєстрації підлягають або електронний документ, або його копія на паперовому носії в порядку, встановленому законодавством республіки Бєларусь. Зазначена норма дає підстави зробити висновок про можливість вчинення через мережі електрозв'язку правочинів, які вимагають нотаріального посвідчення та (або) державної реєстрації. Аналогічна норма міститься в законі Туркменістану від 19 грудня 2000 р. "Про електронний документ" в ст. 9 "Юридична сила електронного документа".

У проекті закону Російської Федерації від 27 червня 2001 р. "Про електронний документ" [124] № 107599-3 не міститься норми, яка б регламентувала сферу, в якій використання електронних документів обмежується або виключається. В преамбулі цього закону зазначається лише, що з використанням електронних документів можуть вчинятися правочини, укладатися договори, здійснюватися розрахунки, листування та

передача інформації. Ряд інших законопроектів РФ пропонує закріпити імперативну норму, яка б виключала вчинення певних правочинів через мережі електрозв'язку під загрозу визнання їх нікчемними.

Так, законопроект РФ від 12 січня 2001 р. "Про електронну торгівлю" № 47432-3 в статті, що регламентує правове визнання електронних документів, передбачає, що правочини, які у відповідності із законодавством РФ повинні бути нотаріально посвідчені або підлягають державній реєстрації, не можуть бути вчинені шляхом обміну електронним документами; правочини вчинені із порушенням зазначеного положення, вважаються нікчемними. Аналогічна норма міститься у законопроекті РФ від 16 листопада 2000 року "Про правочини, які вчиняються за допомогою електронних засобів (про електронні правочини)" № 27813-3 в статті, яка присвячена регламентуванню дійсності електронних правочинів.

У законопроекті України "Про електронну торгівлю" не міститься виключення із загального правила про можливість вчинення правочинів через мережі електрозв'язку (шляхом обміну електронними документами), а зазначається, що у разі, коли законодавством передбачається вимога нотаріального завірення цивільно-правового правочину, такий правочин, оформлений шляхом складання електронного документа, повинен бути завірений нотаріусом з накладанням його електронного цифрового підпису на цей електронний документ.

Слід зазначити, що заборона особам, які здійснюють електронну комерцію, вчиняти правочини через мережі електрозв'язку, що підлягають нотаріальному посвідченню або державній реєстрації, є недоцільною. Це призведе до того, що зі сфери правового регулювання електронної комерції випаде істотна частка господарських договорів, предметом яких є, наприклад, нерухомість і які вимагають нотаріального посвідчення та державної реєстрації. Так, відповідно до ст. 657 ЦКУ договір купівлі-продажу земельної ділянки, єдиного майнового комплексу, житлового будинку (квартири) або іншого нерухомого майна укладається у письмовій формі і підлягає нотаріальному посвідченню та дер-

жавній реєстрації. Залучаючи цей вид договорів до сфери правового регулювання електронної комерції, ми дозволяємо контрагентам укладати договір купівлі-продажу об'єкта нерухомості через мережі електрозв'язку, що дозволяє скористатися контрагентам всіма перевагами, які з цього випливають. Нотаріус, уповноважений посвідчувати такі правочини, перевіривши їх законність, зокрема волевиявлення сторін на відчуження власності, своїм електронним цифровим підписом посвідчує такий правочин, а орган реєстрації на цей договір ставить свій ЕЦП, що може розцінюватися як виконання законодавчої вимоги про необхідність реєстрації договорів про відчуження нерухомості.

Вільний розвиток електронної комерції в Україні повинен спиратися на можливість укладання будь-яких цивільно-правових договорів, зокрема й тих, що вимагають нотаріального посвідчення та державної реєстрації. Нотаріальне посвідчення та державна реєстрація правочинів, які вчиняються через мережі електрозв'язку, у випадках, передбачених законодавством, повинні здійснюватися з використання ЕЦП нотаріуса та уповноваженої особи державного органу.

Реалізація принципу недискримінації правочинів, які вчиняються через мережі електрозв'язку, повинна означати, що правочин, об'єктивований у документі на паперовому носії письмової форми, та правочин, об'єктивований в електронному документі, мають однакову юридичну силу. Електронний носій письмової форми не може розглядатися як єдина причина для позбавлення господарського договору юридичної сили.

Гарантування судового захисту прав осіб, які здійснюють електронну комерцію, полягає в тому, щоб законодавчо закріпити як допустимість електронних документів в якості судових доказів при процесуальних діях, так і їх доказову силу. При вчиненні будь-яких процесуальних дій жодні положення норм доказового права не повинні застосовуватися таким чином, щоб виключалась допустимість електронних документів як доказів з тієї лише підстави, що вони вчинені на електронних носіях. При цьому оцінка доказової сили електронних документів повинна здійснюватися із врахуванням надійності спо-

собу, в який формувався, зберігався або передавався електронний документ, та інших відповідних факторів.

1.4. Законодавство, що регулює здійснення електронної комерції

В Україні законодавство, що регулює електронну комерцію, лише починає формуватися, що здійснюється в двох напрямках – вдосконалення чинного законодавства та прийняття нових нормативних актів.

У системі законодавства України є ряд нормативних актів, які так чи інакше торкаються окремих питань електронної комерції (порядок обміну електронними документами, використання ЕЦП тощо). Але вони, як правило, мають обмежену сферу дії. Так, Закон України від 5 квітня 2001 р. "Про платіжні системи та переказ грошей в Україні" містить визначення ЕЦП, але сфера його застосування пов'язана виключно з функціонування платіжних систем в Україні. З прийняттям Закону України "Про електронний цифровий підпис" до першого закону будуть внесені зміни в частині визначення ЕЦП, оскільки поняття ЕЦП повинно тлумачитися в системі законодавства одноманітно.

Закон України від 16 травня 1995 р. "Про зв'язок" через свій понятійний апарат (електрозв'язок, мережі зв'язку тощо) дає можливість проаналізувати та дати визначення такому поняттю, як Інтернет, що представляє собою одну з мереж електрозв'язку, які виступають середовищем вчинення правочинів у електронній комерції. В той же час необхідно зазначити, що з 1995 р. в галузі зв'язку відбулося чимало змін, що викликано запровадженням сучасних інформаційно – комунікаційних технологій у цій галузі господарської діяльності. Ці зміни відображені у законі України "Про телекомунікації", який замінив закон "Про зв'язок".

Серед нормативних актів, які б було доцільно прийняти, необхідно назвати, перш за все, Закон "Про електронну комерцію".

Виходячи із запропонованого визначення електронної комерції як системи взаємопов'язаних правовідносин у сфері вчинення правочинів шляхом обміну електронними документами, який здійснюється за допомогою використання мереж електрозв'язку, зокрема Інтернет, у системі законодавства України про електронну комерцію можна виділити загальне законодавство та спеціальне.

До загального законодавства відносяться нормативні акти, які регулюють право на зайняття господарською діяльністю, створення відповідного суб'єкта господарювання, правовий режим майна таких суб'єктів, обліку та звітності, відновлення платоспроможності боржника або визнання його банкрутом, господарські зобов'язання, господарсько-правову відповідальність, тощо. До таких нормативних актів можна віднести: Конституцію України [125], Господарський кодекс України, Цивільний кодекс України, Закон України "Про відновлення платоспроможності боржника або визнання його банкрутом"[126], Закон України "Про ліцензування окремих видів господарської діяльності" [127], інші нормативні акти.

Спеціальне законодавство повинно врегулювати особливості, пов'язані із використанням мереж електрозв'язку, зокрема Інтернет, при вчиненні правочинів, а саме: укладання договорів, умови договору, що вчиняється через мережі електрозв'язку, порядок використання електронних документів, їх оригінали, підтвердження одержання електронних документів, використання ЕЦП в електронній комерції тощо.

В Україні такого системного спеціального законодавства ще не створено. Існує лише ряд розрізнених нормативних актів, які намагаються врегулювати окремі питання укладання правочинів через мережі електрозв'язку, використання ЕЦП, обмін електронними документами у певних галузях господарської діяльності.

Серед актів загального законодавства України окремо необхідно зупинитися на Господарському кодексі України та Цивільному кодексі України.

Новий ЦК України зазначає (ст. 207), що "правочин вважається таким, що вчинений у письмовій формі, якщо його

зміст зафіксований в одному або кількох документах, у листах, телеграмах, якими обмінялися сторони. Правочин вважається таким, що вчинений у письмовій формі, якщо воля сторін виражена за допомогою телетайпного, електронного або іншого технічного засобу зв'язку". Вказані норми ст. 207 ЦКУ фактично встановлюють, що правочин, вчинений через мережі електрозв'язку (за допомогою електронного засобу зв'язку), є таким, що вчинений у письмовій формі. Норма аналогічного змісту закріплена, наприклад, й у ч. 2 ст. 434 ЦК РФ [92, с. 346]. Це положення є основоположним для правового регулювання електронної комерції в Україні.

Отже закон не містить критеріїв визначення письмової форми, зокрема, щодо видів матеріальних носіїв письмової форми, а тому вимога вчинення певних видів договорів у письмовій формі може розглядатися як загальне правило, щодо всіх видів матеріальних носіїв письмової форми. Таким чином, вітчизняний законодавець рпямо не вказує на можливість вчинення правочинів через мережі електрозв'язку, а тому існує два можливих варіанти усунення цієї прогалини: необхідно або зазначити на критерії, дотримання яких означає вчинення правочинів у письмовій формі, що дозволяє не прив'язувати законодавство до тієї чи іншої технології фіксації (матеріалізації) інформації, або перераховувати в цивільному кодексі всі можливі матеріальні носії письмової форми вчинення правочинів, що постійно буде мати загрозу відставання правового регулювання від розвитку сучасних інформаційних технологій, а отже, з часом, знову зможе призвести до виникнення юридичних перепон, пов'язаних зі створенням нових матеріальних носіїв письмової форми (саме такий шлях було реалізовано у вказаній вище ст. 207 ЦК України).

В той же час у новому ЦК України (ст. 207 ч. 3), можна зауважити, зроблена доктринальна помилка, оскільки використання електронного цифрового підпису розглядається як виключення, дозвіл на який спеціально повинен бути зазначений у законі (норма аналогічного змісту поспішно закріплена, й у ч. 2 ст. 160

ЦК РФ). Можливість використання ЕЦП повинна, навпаки, бути загальним правилом, а виключення повинні бути передбачені в законі, тобто передбачені випадки, коли він не може бути використаний. Таким чином, в цій частині ЦК України займає іншу позицію, ніж Типовий закон ЮНСІТРАЛ "Про електронну комерцію" (ст.7).

Господарський Кодекс України містить главу 20, яка регулює відносини у сфері господарських договорів. Необхідно зазначити, що жодна з восьми статей цієї глави не враховує сучасні інформаційні технології у сфері зв'язку та передачі інформації. Як наслідок цього, ч. 1 ст. 181 "Загальний порядок укладання господарських договорів" зазначає, що "господарський договір за загальним правилом викладається у формі єдиного документа, підписаного сторонами та скріпленого печатками. Допускається укладання господарських договорів у спрощений спосіб, тобто у вигляді комплекту документів (листів, факсограм, телеграм, телефонограм тощо) шляхом обміну цими документами, а також шляхом підтвердження прийняття до виконання замовлень". Не вносить ясності щодо можливості використання мереж електрозв'язку для вчинення господарських договорів і положення ч. 7 ст. 179 "Загальні умови укладання договорів, що породжують господарські зобов"язання", де вказується, що "Господарські договори укладаються за правилами, встановленими Цивільним кодексом України з урахуванням особливостей, передбачених цим Кодексом, іншими нормативно-правовими актами щодо окремих видів договорів".

Отже, досліджуючи питання відповідності правочинів, які вчиняються через мережі електрозв'язку, вимогам ГК України та ЦК України, можна зазначити, що вказані кодекси начебто легалізують використання електронних засобів зв'язку для вчинення правочинів, але фактично не регулюють використання електронних документів для вчинення таких правочинів, особливості істотних умов таких правочинів тощо. Отже, наявних у ЦК України та ГК України норм недостатньо для належного правового регулювання вчинення правочинів через мережі електрозв'язку.

Спеціальне законодавство повинно заповнити цю прогалину правового регулювання. До чинного в Україні спеціального законодавства відносяться:

1. Закон України від 2 жовтня 1992 р. "Про інформацію" встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону. Зазначений Закон у ст. 27 дає визначення документа в інформаційних відносинах: "...це передбачена матеріальна форма одержання, зберігання, використання і поширення інформації шляхом фіксації на папері, магнітній, кіно-, відео-, фотоплівці або на іншому носієві". Це визначення документа необхідне для дослідження такого поняття, як електронний документ, оскільки один з блоків правовідносин, що складають електронну комерцію, стосується використання електронних документів.

2. Закон України "Про зв'язок" встановлює правові, економічні і організаційні основи діяльності в галузі зв'язку в Україні. Зазначений Закон у ст. 1 визначає поняття електричного зв'язку (електрозв'язку): "...це передача, випромінювання або прийом знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах", а також поняття "мережа зв'язку": "...це сукупність засобів та споруд зв'язку, поєднаних в єдиному технологічному процесі для забезпечення інформаційного обміну". Цей закон через свій понятійний апарат (електрозв'язок, мережі зв'язку, тощо) дає можливість проаналізувати та дати визначення такого поняття, як Інтернет, що становить одну з мереж електрозв'язку, які виступають середовищем вчинення правочинів у електронній комерції.

3. Закон України "Про платіжні системи та переказ грошей в Україні" від 5 квітня 2001 р. визначає загальні засади функціонування платіжних систем в Україні. У ст. 1 Закону наводиться визначення електронного документа та електронного цифрового підпису. В ст. 18 Закону визна-

чається правовий режим електронного документа та електронного цифрового підпису, зокрема зазначається: "Електронний документ має однакову юридичну силу з паперовим документом. Електронний цифровий підпис на електронному документі має однакову юридичну силу з підписом на паперовому документі", крім того зазначається (ст. 18.4 Закону), що оригіналом електронного документа є примірник, підписаний електронним цифровим підписом. Стаття 19 цього закону регулює порядок і строки зберігання, процедуру знищення електронних документів, що застосовуються при проведенні переказу. Закон є першим нормативним актом у формі закону, який закріпив поняття електронного документа та ЕЦП. Незважаючи на досить вузьку сферу застосування цього закону, його положення в частині визначення та використання електронних документів та ЕЦП є дуже корисними для розробки комплексного закону "Про електронну комерцію".

4. Закон України від 22 травня 2003 р. "Про електронний цифровий підпис" покликаний врегулювати окремий блок відносин у сфері електронної комерції – використання ЕЦП. Так, вказаний закон вводить певну термінологічну базу, визначає поняття та правовий режим ЕЦП. Серед недоліків закону необхідно назвати занадто ускладнену систему провайдерів сертифікаційних послуг, процедуру їх акредитації тощо.

5. Положення "Про порядок здійснення криптографічного захисту інформації в Україні" [128], затверджене Указом Президента України від 22 травня 1998 р. № 505/98 (в редакції 27 вересня 1999 р.), яке визначає криптографічний захист як вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Державну політику щодо криптографічного захисту інформації відповідно до Указу Президента України від 11 лютого 1998 р. №110 реалізує Де-

партамент спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України. Відповідно до цього Положення ліцензування діяльності, пов'язаної з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації, здійснюється згідно із законодавством України. З метою визначення рівня захищеності від несанкціонованого доступу до інформації з обмеженим доступом проводяться сертифікаційні випробування криптосистем і засобів криптографічного захисту. Для криптографічного захисту конфіденційної інформації використовуються криптосистеми і засоби криптографічного захисту, які мають сертифікат відповідності. Діяльність, пов'язану з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації, можуть здійснювати суб'єкти підприємницької діяльності, зареєстровані в порядку, встановленому законодавством. Криптографічний захист інформації покладений в основу функціонування ЕЦП, використання яких складає окремий блок правовідносин електронної комерції. Зазначені нормативні акти встановлюють порядок створення, використання, реалізації засобів ЕЦП, з яких генерується власне ЕЦП. Передбачається ліцензування такої діяльності тощо.

6. Положення "Про Департамент спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України" [129] затверджене Указом Президента України від 6 жовтня 2000 р. В п. 1 Указу зазначено, що Департамент спеціальних телекомунікаційних систем та захисту інформації (далі – Департамент) є органом державного управління, що діє у складі Служби Безпеки України та їй підпорядковується; реалізовує державну політику у сфері захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації.

7. Указ Президента України від 31 липня 2000 р. "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні" № 928/2000, який розглядає розвиток національної складової глобальної інформаційної мережі Інтернет, забезпечення широкого доступу до цієї мережі громадян та юридичних осіб усіх форм власності в Україні як один з пріоритетних напрямків державної політики у сфері інформатизації, задоволення конституційних прав громадян на інформацію, розвитку підприємництва.

8. Інструкція "Про міжбанківські розрахунки в Україні", затверджена Постановою Правління НБУ України від 27 грудня 1999 р. (в редакції 23 квітня 2002 р.) № 621, яка визначає шляхи, умови та порядок проведення міжбанківських розрахунків у грошовій одиниці України та в іноземній валюті, а також порядок проведення розрахунків через систему електронних платежів Національного банку України. В п. 5 Загальних положень зазначеної Інструкції визначені поняття, які безпосередньо відносяться до електронної комерції, зокрема щодо можливості розрахунків за вчиненими правочинми через мережі електрозв'язку: електронні міжбанківські розрахунки[10], електронний цифровий підпис[11], банківський електронний документ[12], електронний розрахунковий документ[13] (міжбанківсь-

[10] Електронні міжбанківські розрахунки – міжбанківські розрахунки із застосуванням електронних засобів приймання, оброблення, передавання та захисту інформації про рух коштів.

[11] Електронний цифровий підпис (далі – ЕЦП) – сукупність даних, отримана за допомогою криптографічного перетворення вмісту електронного документа, яка дає змогу підтвердити його цілісність та ідентифікувати особу, яка його підписала.

[12] Банківський електронний документ – електронний розрахунковий документ, службове повідомлення СЕП, довідкове повідомлення інформаційно-пошукової системи Національного банку України (далі – ІПС), інформаційне повідомлення.

[13] Електронний розрахунковий документ (міжбанківський електронний розрахунковий документ) – документ на переказ, сформований банком на підставі розрахункових документів банку, клієнтів, документів на переказ готівки, доручень на договірне списання, та представлений у формі електронних даних, що включають відповідні реквізити документа, у тому числі й електронний цифровий підпис.

кий електронний розрахунковий документ), система електронних платежів Національного банку України[14] (СЕП), система електронної пошти Національного банку України[15] (система ЕП) тощо. Всі ці поняття є матеріалом для дослідження таких понять, як електронний документ, електронні розрахунки тощо, без яких електронна комерція як система взаємопов'язаних правовідносин у сфері вчинення правочинів шляхом обміну електронними документами, який здійснюється за допомогою використання мереж електрозв'язку, зокрема Інтернет, не може існувати.

9. Ліцензійні умови провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівлі і засобами криптографічного захисту інформації [130], затверджені спільним Наказом Державного комітету України з питань регуляторної політики та підприємництва і Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 29 грудня 2000 р. № 88/66. У ліцензійних умовах визначають організаційні, кваліфікаційні, технологічні та інші вимоги до суб'єктів господарювання, виконання яких є обов'язковою умовою провадження певних робіт і надання послуг у межах господарської діяльності з розроблення, виробництва, використання, екс-

[14] Система електронних платежів Національного банку України (СЕП) – загальнодержавна платіжна система, що забезпечує здійснення розрахунків між банківськими установами, органами державного казначейства на території України із застосуванням електронних засобів приймання, оброблення, передавання та захисту інформації. Програмне забезпечення СЕП складається із програмно-технічних комплексів – автоматизованих робочих місць (АРМ), що відповідають трьом рівням структури СЕП: Центральна розрахункова палата – АРМ-1, АРМ ІПС; розрахункові палати – АРМ-2; банківські установи – учасники СЕП – АРМ-НБУ.

[15] Система електронної пошти Національного банку України (система ЕП) – система програмно-технічних засобів та організаційно-технологічних заходів забезпечення інформаційної взаємодії між банківськими та іншими установами в електронній формі.

плуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівлі криптосистемами і засобами криптографічного захисту інформації. Дія Ліцензійних умов поширюється на суб'єктів господарювання, які здійснюють господарську діяльність у галузі криптографічного захисту інформації (КЗІ). Ліцензування господарської діяльності у галузі КЗІ здійснює Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України.

В розвиток та на виконання зазначеного спільного Наказу Державний комітет України з питань регуляторної політики та підприємництва і Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ прийняли Наказ від 12 грудня 2001 р. № 151/72, яким затвердили "Порядок контролю за додержанням ліцензійних умов провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівлі криптосистемами і засобами криптографічного захисту інформації" [131].

10. Положення "Про державну експертизу у сфері криптографічного захисту інформації" [132], затверджене Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 25 грудня 2000 р. № 62. Положення встановлює порядок організації та проведення державної експертизи у сфері криптографічного захисту інформації в Україні, що безпосередньо пов'язано із створенням та розповсюдження засобів ЕЦП, з яких генерується власне електронний цифровий підпис.

Підсумовуючи викладене, необхідно зазначити, що досвід багатьох держав світу свідчить про те, що комплексне регулювання відносин у сфері електронної комерції потребує прийняття закону "Про електронну комерцію".

У законопроекті України "Про електронну торгівлю", який повинен забезпечити правові умови для електронної торгівлі, необхідно вдосконалити термінологічну базу (щодо електронних торгівців, тощо); зазначити принципи, які б характеризували електронну комерцію як окреме правове явище, як певну сукупність правовідносин; визнати правочини, вчинені через мережі електрозв'язку, зокрема через мережі Інтернет, такими, що вчинені в письмовій формі; виключити регулювання відносин щодо використання ЕЦП, які на сьогоднішній день вже врегульовані окремим законом тощо.

Електронна комерція повинна розглядатися як система взаємопов'язаних правовідносин у сфері вчинення правочинів шляхом обміну електронними документами, який здійснюється за допомогою використання мереж електрозв'язку, зокрема Інтернет.

Електронна комерція охоплює три групи правовідносин:

- правовідносини, пов'язані із вчиненням правочинів через мережі електрозв'язку у сфері господарювання;
- правовідносини, пов'язані із використанням та обміном електронними документами;
- правовідносини, пов'язані із використанням електронних підписів.

Закон "Про електронну комерцію" повинен на законодавчому рівні закріпити ряд нових понять, які будуть застосовуватися до будь-якої сфери господарської діяльності, а саме: електронні носії; електронні документи; відправник електронного документа; одержувач електронного документа (адресат); інформаційна система; інформаційний посередник тощо.

До Закону України "Про електронний цифровий підпис" доцільно внести зміни та доповнення, що стосуються визначення ЕЦП та сфери його використання; системи провайдерів сертифікаційних послуг та їх акредитації.

Суб'єктами правовідносин у сфері електронної комерції являються особи, які здійснюють електронну комерцію (вчиняють правочини через мережі електрозв'язку, зокрема через Інтернет), інформаційні посередники, провайдери сертифікаційних послуг.

Відносини у сфері електронної комерції повинні ґрунтуватися як на загальногалузевих принципах господарського права, так і на принципах, властивих саме електронній комерції:

1) принципі вільного здійснення електронної комерції;
2) принципі недискримінації правочинів, що вчиняються через мережі електрозв'язку;
3) принципі відкритості, або технологічного нейтралітету;
4) принципі гарантування судового захисту прав особам, що здійснюють електронну комерцію.

Правове регулювання електронної комерції в Україні, повинно ґрунтуватися на комплексному законі "Про електронну комерцію", який повинен врегулювати основні питання вчинення правочинів через мережі електрозв'язку, та на спеціальному вже прийнятому законі України "Про електронний цифровий підпис", який регулює окрему складну та нову групу правовідносин електронної комерції – відносини, що виникають під час створення та використання ЕЦП.

РОЗДІЛ 2

Правове регулювання господарських договорів, що укладаються через мережі електрозв'язку

2.1. Поняття господарського договору та умови дійсності господарських договорів, що вчиняються через мережі електрозв'язку

Господарський договір – це засновані на згоді сторін і зафіксовані у встановленій законом формі зобов'язальні правовідносини між суб'єктами господарювання, змістом яких є взаємні права і обов'язки сторін у галузі господарської діяльності.

Господарський договір є комплексним поняттям, до якого відносяться договори різних видів – купівлі-продажу, поставки, перевезення, тощо, які мають подібні принципи правового регулювання.

Як правило, дослідження сутності господарського договору проводиться на ґрунті порівняння його із цивільно-правовим договором. Цивілістична наука розглядає господарські договори як вид цивільно-правових договорів, а саме його поняття – як таке, що знаходиться у відношенні субординації (підпорядкованості) з поняттям договору цивільно-правового [120, с. 7].

В той же час представники господарського права зазначають необхідність дослідження господарського договору через призму системно-функціонального методу, що дозволить дослідити господарський договір як систему взаємопов'язаних елементів, які виражають його якісні особливості, в процесі функціонування та розвитку [120, с. 12].

Чинне законодавство України, яке регулює окремі види договірних відносин в галузі економіки, не містить узагальнюючого визначення "господарський договір", яке повинно не тільки визначати зміст цього поняття, а й забезпечувати ясність та однозначність поняття, яке використовується в правозастосовній діяльності. Даний термін знайшов законодавче закріплення у ГКУ (глави 19, 20), але визначення цього поняття ГКУ також не містить.

У законодавстві та юридичній літературі термін "господарський договір" вживається в кількох значеннях, які витікають з теорії цивільного права, зокрема:

1) господарський договір як дво- або багатосторонній правочин, тобто дії сторін, що спрямовані на досягнення певного правового результату. В цьому випадку поняття господарського договору звужується до значення юридичного факту, який сам по собі не має матеріального змісту. Таке смислове значення не дозволяє виявити всі суттєві ознаки господарського договору, оскільки правочин сторін не є договірним відношенням, а лише переслідує мету його встановлення;
2) господарський договір як зобов'язальне правовідношення, змістом якого є взаємні права та кореспондуючі зобов'язання сторін. Особливості змісту господарського договірного зобов'язання об'єктивно обумовлені специфікою господарської діяльності. Сукупність особливостей господарського договору як правочину і як зобов'язального правовідношення дає змогу вивести поняття господарського договору як інституту господарського права;
3) господарський договір як правовий документ, в якому фіксується факт вчинення правочину та зміст зобов'язань сторін.

Зазначимо, що як у господарсько-правовій, так і в цивілістичній науці, питання про ознаки господарських договорів дискусійне. Так, до загальних ознак (властивостей) господарського договору відносять його юридичну обов'язковість для сторін, забезпечену заходами правового примусу [133, с. 25].

В той же час спеціальний суб'єктний склад господарського договору, як одна з кваліфікуючих ознак господарського договору, сумніву не піддавався [134, 135, с. 5–6, 136, с. 24–42, 137, с. 9–13, 138, с. 9, 139, с. 17, 140, с. 46, 48, 141, с. 9–10, 142, с.121–135, 143, с. 25, 117, с. 145].

Для визначення того чи іншого договору господарським необхідна наявність у його сторін правового статусу суб'єкта господарювання.

Питання про спеціальний суб'єктний склад господарських договорів безпосередньо пов'язане з поняттям суб'єкта господарювання. ГКУ у ч. 1 ст. 55 суб'єктами господарювання визнає учасників господарських відносин, які здійснюють господарську діяльність, реалізуючи господарську компетенцію (сукупність господарських прав та обов'язків), мають відокремлене майно і несуть відповідальність за своїми зобов'язаннями в межах цього майна, крім випадків, передбачених законодавством. Частина 2 даної статті ГКУ містить вичерпний перелік суб'єктів господарювання: а) господарські організації – юридичні особи, створені відповідно до ЦКУ, державні, комунальні та інші підприємства, створені відповідно до ГКУ, а також інші юридичні особи, які здійснюють господарську діяльність та зареєстровані у встановленому законом порядку; б) громадяни України, іноземці та особи без громадянства, які здійснюють господарську діяльність та зареєстровані відповідно до закону як підприємці; в) філії, представництва, інші відокремлені підрозділи господарських організацій (структурні одиниці), утворені ними для здійснення господарської діяльності.

Своєрідність господарського договору як зобов'язального правовідношення вбачається у природі господарських зв'язків, що проявляється через призму юридичних прав та обов'язків їх учасників [101, с. 34]. Вона виявляється в спрямованості цих договорів на обслуговування господарської діяльності та у поєднанні майнових і організаційних елементів у змісті господарських договорів.

У науковій літературі відзначалося, що особливість правового інституту господарського договору полягає у поєднанні двох ознак: економічної, яка проявляється в функції господарсь-

кого договору по обслуговуванню галузі господарювання, та юридичної, оскільки господарський договір зумовлює правову сторону змісту господарських відносин [144, с. 7].

Взаємна згода суб'єктів господарювання, які не знаходяться у відносинах субординації, є необхідною умовою встановлення господарських зв'язків між ними. Встановлення такого зв'язку, як правило, відбувається згідно з передбаченою законодавством типовою моделлю договірного зв'язку, хоча суб'єкти господарювання можуть моделювати договірне зобов'язання самостійно, керуючись загальнодозвільним принципом правового регулювання.

Господарські зв'язки, що опосередковані договором, набувають форми договірного правовідношення, яке надає цим зв'язкам стабільності та визначеності.

Чинне законодавство України виходить з того, що всім господарським зв'язкам, які формуються між не підпорядкованими суб'єктами господарювання, необхідно надавати договірної форми. Це правило зафіксоване в нормі ч. 1 ст. 21 Закону "Про підприємства в Україні", згідно з якою відносини підприємства з іншими підприємствами, організаціями та громадянами в усіх галузях господарської діяльності здійснюються на підставі договорів.

Господарські відносини між суб'єктами господарювання, які знаходяться в юридично нерівному становищі (відносинах субординації), можуть мати як договірний, так і не договірний характер.

Хоча орган господарського керівництва і має відносно суб'єктів господарювання владні повноваження, його правосуб'єктність обмежена законом за принципом "дозволено те, що прямо дозволено", що був нормативно закріплений ст. 27 Закону "Про підприємства в Україні". Це означає, що не субординація сама по собі надає органу господарського керівництва право вимагати певної дії від суб'єкта господарювання, а закон, що значною мірою згладжує юридичну нерівність сторін договірного відношення [145, с. 113, 120–121].

Характеризуючи особливості змісту господарського договірного зобов'язання, слід вказати на можливість визначення умов

договірного зобов'язання в актах планування. В юридичній літературі проблема співвідношення господарського договору та планового акта широко дискутувалася, а сама плановість (прямо чи опосередковано) розглядалася як ознака господарських договорів [145, 105, с. 110, 146, с. 491, 147, с. 73–74, 148, с. 128, 149, с. 124–129, 150, с. 158–159].

Плановість самої господарської діяльності зумовлює особливості господарського договірного зобов'язання. Планова сутність господарського договору проявляється як у тому випадку, коли господарський договір укладений на підставі акта планування, обов'язкового, принаймні, для однієї із сторін майбутнього договірно-господарського зв'язку, так і у випадку укладання його на підставі акта мікроекономічного планування, тобто на рівні окремого суб'єкта господарювання.

Планову сутність господарського договору можна визначити таким чином: зміст господарського договірного зобов'язання формується під впливом державних актів планування в тих випадках, коли обов'язковість укладання господарського договору передбачена чинним законодавством, й актів внутріфірмового планування, які самостійно розробляються суб'єктами господарювання [101, с. 42].

На підставі викладеного можна зробити висновок про те, що суттєвими ознаками господарського договору є його суб'єктний склад та особлива цільова спрямованість.

Сторонами (стороною) в господарському договорі можуть виступати господарські організації з правами юридичної особи, індивідуальні підприємці (як із статусом, так і без статусу юридичної особи), а також негосподарські організації – юридичні особи – при здійсненні ними господарської діяльності, необхідної для досягнення мети, передбаченої їх установчими документами; органи господарського управління – власники та/або уповноважені ними органи, які здійснюють в межах їх компетенції управління майном створених (придбаних) ними або підвідомчих ним господарських організацій.

Особлива цільова спрямованість господарського договору виявляється в обслуговуванні господарської діяльності. При

цьому такі договори опосередковують як ті господарські зв'язки, що встановлюються між автономними суб'єктами господарювання, так і ті, що складаються між ними та органами господарського управління з приводу руху матеріальних благ.

Тільки сукупність суттєвих ознак господарського договору може визначати відносини, що склалися між сторонами внаслідок правочину, як господарсько-договірні з поширенням на них норм спеціального законодавства, що регулює окремі види господарських договорів, порядок їх укладання і виконання, а також застосування різних видів господарсько-правової відповідальності за їх неналежне виконання.

Дійсність правочину означає визнання за ним якості юридичного факту, який породжує той правовий результат, до якого прагнули суб'єкти правочину [151, с. 342]. Дійсність правочину визначається законодавством такою сукупністю умов: законність змісту, здатність фізичних та юридичних осіб, що вчиняють його, до участі в правочині, відповідність волі та волевиявлення, дотримання форми правочину.

Правочини з вадою змісту визнаються недійсними внаслідок розходження умов правочину з вимогами закону та інших правових актів. У випадку колізії між нормами, що містяться у нормативних актах, законність змісту правочину визначається з врахуванням юридичної сили нормативних актів.

Встановлюючи законність змісту правочину, необхідно враховувати те, що ЦКУ допускає аналогію закону та аналогію права (ст. 8). Юридичні дії, що визнаються правочинами за аналогією закону, породжують цивільно-правові наслідки, оскільки їх зміст не суперечить сутності цивільного законодавства, що регулює подібні відносини. Юридичні дії, що визнаються правочинами за аналогією права, підлягають правовому захисту, оскільки їх зміст відповідає загальним засадам та змісту цивільного законодавства. Тобто зміст правочинів, що визнаються такими, за аналогією закону чи права, також визнається законним, оскільки санкціонований загальними нормами цивільного законодавства.

Вчинення правочинів через мережі електрозв'язку означає, що такий правочин укладається шляхом обміну електронними

документами, в яких об'єктивуються оферта, акцепт оферти. Якщо договір складається у вигляді одного документа (ч. 1 ст. 207 ЦКУ), він також об'єктивується у електронному документі, який підписується електронними підписами уповноважених на це осіб. Тобто, правочин, вчинений через мережу електрозв'язку, зокрема через Інтернет, повинен у повному обсязі відповідати положенням чинного законодавства щодо законності змісту правочину. Зазначене положення прямо передбачається рядом держав світу. Так, Закон штату Юта США "Про електронні правочини" в параграфі 4 закріплює, що умови контракту визначаються матеріальним правом, яке до нього застосовується.

Зміст правочину визначається сукупністю істотних, звичайних та випадкових умов правочину. Так, особи, що здійснюють електронну комерцію, відповідно до ст. 179, 180 ГКУ, які передбачають загальні умови укладання договорів, що породжують господарські зобов'язання, та істотні умови господарських договорів, при укладенні господарських договорів можуть визначити зміст договору на основі:

- вільного волевиявлення, коли особи, що здійснюють електронну комерцію, мають право погоджувати на свій розсуд будь-які умови договору, що не суперечать законодавству;
- примірного договору, рекомендованого органом управління суб'єктам господарювання для використання при укладенні ними договорів, коли сторони мають право за взаємною згодою змінювати окремі умови, передбачені примірним договором, або доповнювати його зміст;
- типового договору, затвердженого Кабінетом Міністрів України, чи у випадках, передбачених законом, іншим органом державної влади, коли контрагенти не можуть відступати від змісту;
- договору приєднання, запропонованого однією стороною для інших можливих суб'єктів, коли ці суб'єкти у разі вступу в договір не мають права наполягати на зміні його змісту.

Таким чином, особи, що здійснюють електронну комерцію, реалізуючи законодавчу вимогу забезпечення законності змісту правочинів, зокрема таких, що вчиняються через мережі електрозв'язку, можуть визначити зміст правочину, що вчиняється, на основі вільного волевиявлення, примірного або типового договору чи договору приєднання.

Оскільки правочин є волевою дією, вчиняти його можуть лише дієздатні фізичні особи та юридичні особи в межах своєї спеціальної правоздатності. Під спеціальною правоздатністю розуміється наявність у юридичної особи таких прав та обов'язків, які відповідають цілям та задачам її діяльності. Отже, якщо юридична особа вчиняє правочин, який не відповідає цілям її діяльності, то такий правочин може бути визнаний недійсним.

Тобто закон обмежує коло суб'єктів, які можуть виступати суб'єктами господарських договорів. Згідно зі ст. 50 ЦКУ та ч. 1 ст. 173 і ч. 1 ст. 55 ГК України суб'єктами господарських договорів є підприємства, установи, організації, інші юридичні особи, а також громадяни-підприємці.

Особи, які здійснюють електронну комерцію, створюються та існують у організаційно-правових формах, передбачених чинним законодавством. Право укладати договори, зокрема через мережі електрозв'язку, охоплюється поняттям правоздатності юридичної особи та належить суб'єктам господарювання в силу їх правового статусу.

Дійсність правочинів передбачає збіг волі та волевиявлення. Незбіг дійсних намірів особи та їх прояву є підставою визнання правочину недійсним. Необхідно зазначити, що правильно сформована внутрішня воля і адекватне її вираження у волевиявленні перебувають у нерозривній єдності. Волю та волевиявлення в реальній дійсності можливо відокремити лише на певному абстрактному рівні. Єдність волі та волевиявлення – обов'язкова умова дійсності правочинів [152, с.223, 153, с. 42].

Особа, яка вчиняє правочини через мережі електрозв'язку, використовуючи з цією метою обмін електронними документами, повинна, як і при вчиненні правочинів на паперовому носії, забезпечити єдність волі та волевиявлення. Тобто має переко-

натися, що намір, який сформувався у свідомості, адекватно відповідає її волевиявленню.

Правочин породжує права та обов'язки за умови дотримання форми, що вимагається. Правочини можуть вчинятися усно, в письмовій формі (звичайній чи нотаріальній), шляхом здійснення конклюдентних дій, мовчання (ст. 205 ЦКУ).

Вчинення правочинів у сфері господарювання, за загальним правилом, відбувається у письмовій формі (ст. 208 ЦК України, ч. 1 ст. 181 ГК України, пункт 6 Роз'яснення Вищого Господарського Суду України № 02-5/111 від 12.03.1999 р. "Про деякі питання практики вирішення спорів, пов'язаних з визнанням правочинів недійсними"). Отже, закон вимагає, щоб господарські договори укладалися письмово і були підписані уповноваженими особами.

Особи, що здійснюють електронну комерцію, укладаючи договори через мережі електрозв'язку, використовуючи з цією метою електронні документи, повинні дотримуватися законодавчої вимоги про письмову форму господарського договору.

Запровадження сучасних інформаційно-телекомунікаційних технологій у сферу господарювання, становлення та розвиток електронної комерції в Україні призвело до появи такого нового поняття як "електронна форма правочину". В юридичній літературі та чинному законодавстві не міститься визначення даного поняття, що створює юридичні перепони на шляху можливості вчинення правочинів через мережі електрозв'язку. Також в юридичній літературі мало приділяється уваги дослідженню поняття письмової форми правочину, що дало б підстави встановити співвідношення понять письмової форми правочину та електронної форми [134, с. 340–350, 154, с. 125, 155–156].

В юридичній літературі та законодавстві майже не приділяється увага питанню письмової форми господарського договору. Як правило, зазначається загальне правило про укладання договорів у письмовій формі, вказується на окремі випадки нотаріального посвідчення договорів та їх державної реєстрації.

ГК України прямо не передбачає укладання господарських договорів у письмовій формі, а містить відсильну норму ст. 179 (ч. 7), згідно з якою господарські договори укладаються за правилами, встановленими ЦК України. Частина 1 ст. 207 ЦКУ передбачає, що "правочин вважається таким, що вчинений у письмовій формі, якщо його зміст зафіксований в одному або кількох документах, у листах, телеграмах, якими обмінялися сторони. Правочин вважається таким, що вчинений у письмовій формі, якщо воля сторін виражена за допомогою телетайпного, електронного або іншого технічного засобу зв'язку."

Таким чином, ні ГК України, ні ЦК України не дають визначення письмової форми правочину чи договору, також не пропонують вони й критеріїв, дотримання яких є підставою вважати вимогу про укладання того чи іншого договору у письмовій формі – виконаною. Замість цього законодавець перераховує засоби зв'язку, які можуть бути використані для укладання договору у письмовій формі, що, з одного боку, покликано усунути юридичні перепони вчинення договорів через мережі електрозв'язку, а з іншого, – створює загрозу постійного відставання правового регулювання від розвитку сучасних інформаційних технологій, а отже, з часом знову зможе призвести до необхідності врахування нових засобів зв'язку для укладання договорів у письмовій формі.

Так, наприклад, відповідно до ст.134 Кодексу торговельного мореплавства [157] договір морського перевезення вантажу повинен бути укладений у письмовій формі. Документами, що підтверджують наявність і зміст договору морського перевезення вантажу, є рейсовий чартер – якщо договір передбачає умову надання для перевезення всього судна, його частини або окремих суднових приміщень; коносамент – якщо договір не передбачає зазначеної вище умови; інші письмові докази. Імперативна норма про укладання правочинів у письмовій формі міститься й в ряді інших законодавчих актів України.

Необхідність розгляду питання про письмову форму господарського договору пов'язана з тим, що використання новітніх інформаційно-телекомунікаційних технологій у галузі господа-

рювання в Україні створило технічні умови укладання господарських договорів через мережі електрозв'язку, зокрема через мережу Інтернет.

Фактично господарський договір, вчинений через мережі електрозв'язку, – це традиційні, засновані на домовленості сторін зобов'язальні правовідносини між суб'єктами господарювання, змістом яких є взаємні права та обов'язки сторін у галузі господарської діяльності. Його специфіка стосується матеріального носія, на якому фіксується договір.

Саме ця його властивість вимагає законодавчого закріплення правил, які б підтверджували законність господарських договорів, що вчиняються через мережі електрозв'язку, в межах діючого в державі правого механізму: сам факт укладання договору, волевиявлення сторін, тощо. Зафіксовані умови договору повинні відповідати певним правилам, які б дозволили за необхідності вимагати примусового виконання зобов'язання на підставі судового рішення.

Укладання господарського договору в електронній формі передбачає, що контрагенти позбавляються необхідності фізичного контакту один з одним. Вони можуть перебувати не тільки у різних частинах міста, країни, а навіть у різних частинах світу.

Фізично укладений господарський договір в електронній формі являє собою електронний документ, підписаний контрагентами шляхом накладення електронного підпису.

Отже виникає питання про те, що являє собою електронна форма господарського договору: нова форма поряд із вже існуючими письмовою та усною, або вона охоплюється поняттям письмової форми. Вирішення цього питання має як теоретичний, так й практичний інтерес.

Теоретичний інтерес пов'язаний із необхідністю нового осмислення поняття форми договору взагалі та письмової форми зокрема; якщо стати на позицію нової форми договору, то слід на науковому рівні дослідити, чим ця нова форма відрізняється від вже існуючих, які договори можуть вчинятися у такій формі, а які ні та з яких підстав, яким чином повинно відреагувати на це господарсько-процесуальне законодавство тощо.

Практичний інтерес вирішення цього питання пов'язаний з тим, що вже зараз суб'єкти господарювання звертаються до господарських судів за захистом своїх прав та законних інтересів, які випливають із електронних господарських договорів [73, с. 171–174].

Ми приєднуємося до точки зору тих авторів [158, 111, с. 79–81], які вважають, що електронна форма договору охоплюється існуючою письмовою формою. На доведення цього тезису можна навести наступну аргументацію.

Відповідно до загальнофілософського уявлення про форму зміст та форма – це категорії матеріалістичної діалектики. Зміст – сукупність елементів та процесів, які складають даний предмет або дане явище. Форма – спосіб існування, його внутрішня організація, зовнішній вираз. [159, с. 227] У діалектичному поєднанні змісту та форми визначальним є зміст. Але і форма не є пасивною. Коли вичерпуються можливості відображення змін у змісті, форма перестає йому відповідати, починає гальмувати розвиток змісту, що в кінцевому результаті призводить до заміни старої форми новою.

Будь-яка письмова форма, в тому числі і господарські договори, є продуктом інтелектуальної діяльності людини, результатом її цілеспрямованої діяльності. Всі вони створюються на базі людських уявлень про оточуючий світ та є об'єктивним відображенням їх у формі людських думок, закріплених на предметах за допомогою різних матеріальних слідів.

Створення господарського договору як юридично значущого документа у письмовій формі являє собою певний процес, який включає окремі етапи, починаючи із сприйняття фактів та закінчуючи відтворенням відомостей про них на різних предметах. Такий процес створення господарського договору називається його формуванням.

Сприйняття фактів, явищ дійсності передує вираженню зовні думок, образів, які з'явилися у свідомості, та складає першу стадію створення письмової форми. Відповідність знань людини фактичним обставинам, їх істинність залежать перш за все від стану та розвитку органів відчуття та мислення кожно-

го конкретного суб'єкта. Їх вади впливають на процес пізнання та призводять до викривлення фактів та явищ, які сприймаються, відхилення від істини.

Другою стадією створення письмової форми є закріплення відомостей про факти в об'єктивній формі. Все сприйняте суб'єктом втілюється у думки на ґрунті мовного матеріалу – термінів, слів, фраз, оскільки пізнавальна діяльність людини можлива лише на ґрунті мови. Думка одержує свій зміст з образів, сприйняттів, уявлень, які створюються в процесі відображення у свідомості об'єктивної дійсності. Без них думка існувати не може, проявляється думка у мові. У процесі спілкування людей її зміст виражається за допомогою сполучення звуків – слів та фраз.

Думки, ідеї, які сформувалися в голові у людини, можуть дістати об'єктивованої форми, тобто можуть бути відображені на предметах за допомогою різних умовних знаків та інших матеріальних слідів.

Точне відтворення на предметах думки, вираженої шляхом мовних термінів, – слів, фраз, можливе лише за наявності умовних знаків, які відповідають мовним термінам. При цьому умовні знаки (букви, ієрогліфи, цифри, тощо) повинні суворо відповідати звукам, їх сполучення – словам, фразам, окремим поняттям та повинні розташовуватися у певному порядку. Звідси й з'являється письмове джерело, в тому числі й господарський договір.

Переконавшись під впливом конкретних умов у необхідності виразити свої думки зовні, особа переносить уявлення про факти на предмет, зокрема на папір, де відображається узгоджена воля контрагентів на виникнення взаємних прав та обов'язків.

Таким чином, однією з істотних ознак, яка відображає особливості письмових джерел, є характер об'єктивування думки – писемність. Спосіб її – рукописний, машинописний (на друкарській машинці), механічний (типографський), тощо – не змінює їх сутності.

Підкреслимо, що для письма застосовуються умовні, тобто спеціально вироблені та загальноприйняті для фіксування думки знаки, а не будь-які матеріальні сліди. Такими знаками мо-

жуть бути букви, цифри, ієрогліфи, шифри, стенографічні та інші умовні позначення, які використовуються для складання слів, речень, виразу понять.

Матеріальним об'єктом письмової форми, який виступає в якості носія відомостей про факти, можуть бути будь-які предмети із різноманітного матеріалу. Параметри такого предмета (форма, вага, розміри, тощо) не мають жодного впливу на правову природу письмової форми [160, с. 28].

Закріпленням відомостей про факти на письмі закінчується процес створення письмової форми.

На підставі викладеного можна виділити ознаки такого поняття як письмова форма господарського договору, що дозволить запропонувати визначення поняття письмової форми господарського договору, а саме:

1) у письмовій формі об'єктивно закріплюється інформація, яка містить відомості про факти, що мають значення для виникнення, зміни або припинення зобов'язального правовідношення між суб'єктами господарювання;
2) матеріальним об'єктом, носієм письмової форми є будь-який предмет, незалежно від його форми, розміру, цілі, для якої він призначений, матеріалу, з якого він зроблений;
3) способом закріплення письмової форми на зазначених предметах є писемність у всіх її видах за допомогою всіх відомих людству умовних знаків, які розташовуються у певному порядку;
4) зміст письмової форми визначається взаємними правами і обов'язками сторін у галузі господарської діяльності.

На підставі викладеного можна визначити письмову форму господарського договору як спосіб об'єктивування за допомогою писемності та умовних знаків на різних носіях відомостей, зміст яких визначається взаємними правами і обов'язками сторін у галузі господарської діяльності.

Запропоноване визначення письмової форми не суперечить загальному уявленню про письмову форму, яке можна знайти у чинному законодавстві України. Так, в Законі України від 24 лютого 1994 р. "Про міжнародний комерційний арбітраж"

[161] зазначається, що арбітражний правочин вважається укладеним у письмовій формі, якщо він міститься в документі, підписаному сторонами, або укладений шляхом обміну листами, повідомленнями по телетайпу, телеграфу, або з використанням інших засобів електрозв'язку, що забезпечують фіксацію такого правочину, або шляхом обміну позовною заявою та відзивом на позов, в яких одна з сторін стверджує наявність правочину, а інша проти цього не заперечує.

Аналіз зазначеного в законі визначення також говорить про спосіб об'єктивування за допомогою письма та умовних знаків на різних носіях думок, зміст яких визначається взаємними правами і обов'язками сторін. Основна умова, яка висувається законодавцем до письмової форми, це забезпечення фіксації правочину. Використання різних засобів електрозв'язку для укладання правочинів означає використання різних носіїв, що є прогресивним для чинного законодавства України. Використання електронних носіїв для фіксації арбітражного правочину, виходячи з цього визначення, повністю охоплюється поняттям письмової форми. Все це повністю відповідає наведеному вище визначенню письмової форми господарського договору.

Проаналізуємо господарський договір, вчинений через мережі електрозв'язку, на предмет відповідності зазначеним вище ознакам письмової форми.

Відомості, які містяться у господарських договорах, укладених в електронній формі, являють собою людську думку (поняття, судження, умовивід тощо) про існуючу дійсність, зокрема про виникнення, зміну або припинення тих чи інших господарських правовідносин. Тобто за змістом (сукупністю прав та обов'язків сторін за договором) договір, укладений в електронній формі, та повністю аналогічний договір, укладений на папері, є тотожними. При цьому повністю дотримується принцип відносності доказів, закріплений господарським процесуальним правом України.

Господарський договір, вчинений через мережі електрозв'язку, має матеріальний носій, яким виступає вінчестер (жорсткий диск комп'ютера, на якому він зберігається), дискета, лазер-

ний диск, сервер, тощо. Відомості, які містяться в електронному господарському договорі, закріплюються за допомогою писемності, тобто набору загальновідомих умовних знаків, розташованих у певному порядку. Зміст таких відомостей також визначається взаємними правами і обов'язками сторін у галузі господарської діяльності.

Отже, специфіка електронної форми вбачається у матеріальному носії [162] – дискета, лазерний диск, жорсткий диск, тощо (електронні носії). Еволюція носія письмової форми не призводить до виникнення нової форми поряд із письмовою. Використання в якості матеріального носія письмової форми каменя, глиняних табличок, берести, пергаменту, паперу не створювало кам'яної, глиняної, берестяної, пергаментної чи паперової форми. Існувала одна й сама форма – письмова. При цьому акцент робиться не на носії форми, а на способі її закріплення – письмо за допомогою умовних знаків, які розташовуються у певному порядку.

Таким чином, доцільно говорити про еволюцію носіїв письмової форми (від каменя до електронних носіїв), а не про виникнення окремої нової форми чи різновиду письмової форми, а відповідно, господарський договір, вчинений через мережі електрозв'язку, є таким, що вчинений у письмовій формі.

Через призму наведеного висновку, на нашу думку стає наочною хибність висновків Постанови Вищого арбітражного суду України від 27 березня 2001 р. № 04-1/11-7/60. Так, судова колегія по перегляду рішень, ухвал, постанов Вищого арбітражного суду України розглянула заяву АТ "О..." (Латвія) про перевірку рішення арбітражного суду м. Києва від 25 грудня 2000 р. по справі № 5/20, яким визнаний недійсним депозитний договір від 15 вересня 1998 р., укладений по системі REYTERS DEALING між АТ "О..." (далі АТ) та АБ "У..." та про повернення заборгованості в розмірі 486 724 дол. США та 778 690, 21 дол. США відсотків за депозитним вкладом.

Свої вимоги заявник обґрунтовував тим, що відповідач АБ "У..." не виконав умов депозитного договору, укладеного по системі REYTERS DEALING. У повідомленні позивача від

15 вересня 1998 р., адресованому відповідачу, повідомлялося, що АО "О..." підтверджує вчинення з відповідачем грошового правочину, за умовами якого позивач надає відповідачу 2 млн 700 тис. доларів США з ставкою 65 відсотків на строк з 15 вересня 1998 р. по 29 вересня 1998 р. Позивач перераховує відповідачу зазначену суму на його рахунок у Bank of New York. Позивач вважає, що правочин від 15 вересня 1998 р. є продовженням та невід'ємною частиною договорів, укладених сторонами по справі раніше, починаючи з 7 липня 1998 р.

Заявник стверджував, що, визнаючи правочин від 15 вересня 1998 р. недійсним, суд неправомірно посилався на ст. ст. 45, 48, 153 ЦК УРСР [163], ст. 6 "Закону України "Про зовнішньоекономічну діяльність", оскільки спірні правовідносини регулюються спеціальним законодавством у банківській сфері. В зв'язку з тим, що в Україні нема закону, який регулює порядок укладання саме електронної форми правочину, такі правочини мають юридичну силу, оскільки така форма правочину не заборонена правовими нормами, а також, згідно зі ст. 42 ЦК УРСР, правочин, для якого законом не встановлена певна форма, вважається укладеним, якщо з поведінки особи вбачається її воля на укладання правочину (факт укладання та часткового виконання правочинів підтверджується кредитовими авізо, виписками по рахунку, передачею єврооблігацій).

Наведені обґрунтування заявника його вимог суд не взяв до відома і прийшов до висновку, що чинним законодавством України не передбачений спеціальний порядок і форма укладання правочинів між резидентом та нерезидентом, у тому числі депозитних правочинів в електронній формі; оспорюваний правочин є зовнішньоекономічним, а тому за відсутності спеціальної норми застосовуються загальні норми, в тому числі Закон України "Про зовнішньоекономічну діяльність"; відповіді НБУ, викладені у листах, про можливість укладання депозитних договорів в електронній формі, не можуть бути підставою для визнання оспорюваного правочину дійсним.

Таким чином, "електронна форма" правочинів поки ще не розглядається у судовій практиці не тільки як така, що охоплюється поняттям письмової форми правочину, а й така, що відповідає чинному законодавству. Пункт 6 Роз'яснень президії Вищого арбітражного суду України від 12 березня 1999 року №02-5/111 "Про деякі питання практики вирішення спорів, пов'язаних із визнанням правочинів недійсними" розглядає лише письмову та усну форму правочинів.

Вищий арбітражний суд поверхнево підійшов до вирішення зазначеного вище спору. Крім констатації відсутності у ЦК поняття "електронної форми" та відсутності у законодавстві норми, яка б передбачала можливість визнавати дійсними правочини, вчинені через мережі електрозв'язку (з використанням електронних засобів зв'язку), доцільно було також з'ясувати, що саме являє собою "електронна форма", чи охоплюється вона поняттям письмової форми, передбаченої чинним законодавством. Вирішення цих питань привело б до наведеного висновку про те, що особливість "електронної форми" ґрунтується на матеріальному носії – дискета, лазерний диск, тощо. Розвиток та видозміна носія письмової форми не призводить до виникнення нової форми поряд із письмовою. З часів виникнення у людської цивілізації писемності незалежно від її носія існувала одна й та сама форма – письмова.

Комісія ООН з права міжнародної торгівлі, приймаючи Типовий закон "Про електронну комерцію", визначила своє розуміння проблеми електронної форми. Вказуючи на те, що юридичні вимоги, які передбачають використання традиційних паперових документів, являють собою основну перепону розвитку сучасних методів передачі даних, Типовий закон не дає визначення ні паперового документа, ні письмової форми. Вирішення проблеми співвідношення традиційного паперового документа та документа, зафіксованого на електронних носіях, Типовий закон вбачає у так званому функціонально-еквівален-

тному підході, який ґрунтується на аналізі цілей[1] та функцій[2] традиційної вимоги до складання документів на папері для того, щоб встановити, яким чином ці цілі та функції можуть бути досягнуті або виконані за допомогою сучасних методів зв'язку.

Сукупність цілей та функцій, що висувається до складання документів на папері, дозволила авторам Типового закону у ст. 6 "Письмова форма" прийти до висновку про те, що якщо законодавство вимагає, щоб інформація була представлена у письмовій формі, ця вимога вважається виконаною шляхом надання електронного документа, якщо інформація, що в ньому міститься, є доступною для подальшого посилання на неї.

Типовий закон виділяє основну вимогу до оформлення документів на папері – можливість відтворення та прочитання інформації. Дотримання електронним документом такої вимоги дозволяє за Типовим законом забезпечити для електронних документів такий рівень юридичного визнання, який характерний для відповідних паперових документів.

Таким чином, Типовий закон ЮНСІТРАЛ "Про електронну комерцію" до поняття письмової форми включає як документи, зафіксовані на паперовому носієві, так і документи, зафіксовані на електронному носієві. Вимогу забезпечення можливості відтворення та прочитання інформації слід розуміти як таку, що відноситься не тільки до документів, зафіксованих на електронних носіях чи на папері, а в цілому до письмової форми.

На підставі викладеного можна зробити ряд висновків:

1) письмова форма господарського договору – це спосіб об'єктивування за допомогою письма та умовних знаків

[1] До цілей Типовий закон відносить, наприклад, забезпечення збереженості матеріальних доказів наявності та характеру намірів сторін прийняти на себе зобов'язання; сприяння кращому розумінню сторонами наслідків укладання контракту; забезпечення того, щоб документ був зрозумілим для всіх; тощо.

[2] До функцій Типовий закон відносить, наприклад, доказову функцію; попереджувальну функцію в контексті цивільного права; тощо.

на різних носіях інформації, зміст якої визначається взаємними правами і обов'язками сторін у галузі господарської діяльності;

2) доцільно говорити про еволюцію носіїв письмової форми (від каменя до електронних носіїв), а не про виникнення окремої нової форми чи різновиду письмової форми, а відповідно господарський договір, вчинений через мережі електрозв'язку, є таким, що вчинений в письмовій формі;
3) відповідні статті Цивільного кодексу України, які встановлюють вимоги щодо письмової форми правочинів, повинні містити критерії, дотримання яких є достатнім для визнання правочину таким, який вчинений в письмовій формі, незалежно від матеріального носія: а) у письмовій формі об'єктивно закріплюється думка, яка містить відомості про факти, що мають значення для виникнення, зміни або припинення зобов'язальних правовідносин між суб'єктами господарювання; б) матеріальним об'єктом, носієм письмової форми є будь-який предмет, незалежно від його форми, розміру, цілі, для якої він призначений, матеріалу, з якого він зроблений; в) способом закріплення письмової форми на зазначених предметах є письмо у всіх його видах за допомогою всіх відомих людству умовних знаків, які розташовуються у певному порядку; г) зміст письмової форми визначається взаємними правами і обов'язками сторін. Закріплення в законодавстві такої норми дозволить не прив'язуватися до тієї чи іншої технології фіксації (матеріалізації) інформації та не стримувати розвиток інформаційних технологій та господарських відносин, які все більше спираються на сучасні технології в галузі інформатизації;
4) вимога вчинення певних видів договорів у письмовій формі повинна розглядатися як загальне правило, щодо всіх видів матеріальних носіїв об'єктивування письмової форми, тобто як загальне правило повинна бути передбачена можливість вчинення правочинів через мережі електрозв'язку. Законодавче закріплення неможливості

вчинення через мережі електрозв'язку окремих правочинів, тобто об'єктивування письмової форми правочинів на тому чи іншому носії, повинно розглядатися як виняток із загального правила.

Така умова дійсності господарського договору, що вчиняється через мережі електрозв'язку, як дотримання його письмової форми, нерозривно пов'язана з використанням ЕЦП для підписання такого договору.

Як вже зазначалося, в основі електронної комерції, як комплексного правового явища, лежать, правовідносини у сфері вчинення правочинів через мережі електрозв'язку, які об'єктивуються у електронний документ, який набирає юридичної чинності завдяки застосуванню акту підписання – накладенню електронного підпису уповноваженої особи. Один із найважливіших етапів оформлення будь-якого договору, зокрема й договору, який укладається через мережі електрозв'язку, – його підписання як єдиного документа, оскільки підпис узаконює його.

Стаття 181 ГКУ "Загальний порядок укладання господарських договорів" передбачає, що господарський договір за загальним правилом викладається у вигляді єдиного документа, підписаного сторонами та скріпленого печатками. Правочин, який вчиняє юридична особа, підписується особами, уповноваженими на це її установчими документами, довіреністю, законом або іншими актами цивільного законодавства, та скріплюється печаткою (ст. 207 ч. 2 ЦКУ, п. 9 Роз'яснення Вищого Господарського суду України "Про деякі питання практики вирішення спорів, пов'язаних із визнанням правочинів недійсними" №02-5/111 від 12 березня 1999 р. [102]).

Чинне законодавство України не містить окремого нормативного акту, присвяченого правовому регулюванню створення, обігу та зберігання суб'єктами господарювання документів, пов'язаних із здійсненням їх діяльності. Тому вважаємо за можливе звернутися до "Інструкції з діловодства у міністерствах, інших центральних органах виконавчої влади, Раді Міністрів Автономної Республіки Крим, місцевих органах виконавчої влади" [164], затвердженої Постановою Кабінету Міністрів України від

17 жовтня 1997 р. (в редакції 28 липня 2003 р.) № 1153, яка встановлює загальні правила документування управлінської діяльності у вказаних органах та регламентує порядок роботи з документами з моменту їх створення або надходження до відправлення, або передачі в архів установи. Так, п. 4.6.1. Інструкції передбачає, що засвідчення документів здійснюється шляхом їх підписання, затвердження та поставлення печатки; документи підписуються посадовими особами установи відповідно до їх компетенції, встановленої чинними нормативно-правовими актами.

Акт підписання контрагентами вчиненого правочину узаконює його, надає юридичної чинності. Правочини, вчинені через мережі електрозв'язку, як і будь-які інші правочини, відповідно до чинного законодавства повинні бути підписані уповноваженою на те особою. Нерозривний фізичний зв'язок рукописного підпису з носієм інформації (рукописний підпис можливий лише на документах, які мають матеріальну природу, наприклад, документи, об'єктивовані на паперовому носії) робить його неприйнятним для використання у правочинах, вчинених через мережі електрозв'язку, оскільки електронні документи, в яких втілюються дані правочини, мають логічну природу. Вказана обставина стала підставою для використання електронного підпису уповноваженої особи для надання правочинам, вчиненим через мережі електрозв'язку, юридичної чинності.

Усвідомлюючи виключне значення електронних підписів для можливості здійснення електронної комерції, багато країн світу вже прийняли закони, що регулюють їх використання (Австрія, Італійська Республіка, Російська Федерація, Республіка Словенія, США, Україна та інші).

Ряд міжнародних організацій прийняли типові рекомендаційні акти щодо правового регулювання використання електронних підписів. Так, слід назвати типовий Закон ЮНСІТРАЛ від 5 червня 2001 р. "Про електронні підписи"; директиву ЄС від 13 грудня 1999 р. "Про правові підстави для використання електронних підписів"; модельний закон Міжпарламентської асамблеї країн–учасниць СНД від 9 грудня 2000 р. "Про електронний цифровий підпис".

Отже, використання ЕЦП для надання юридичної чинності правочинам, вчиненим через мережі електрозв'язку, є поширеною світовою практикою, про що свідчить згадане вище законодавство ряду держав світу, міжнародних організацій [165] та окремі судові прецеденти [166].

Типовий закон ЮНСІТРАЛ "Про електронний підпис" від 5 червня 2001 р. в ст. 6 передбачає, що в тих випадках, коли законодавець вимагає наявності підпису особи, ця вимога вважається виконаною щодо електронного документа, якщо використаний електронний підпис, який є настільки надійним, наскільки це відповідає меті, для якої електронний документ був підготовлений або переданий, з урахуванням всіх обставин, включаючи будь-які відповідні домовленості. Зазначене правило застосовується як в тих випадках, коли вимога наявності підпису виражена у формі обов'язку, так і в тих випадках, коли законодавство передбачає настання певних наслідків, якщо підпис відсутній.

Норма аналогічного змісту закріплена й у ч. 1 ст. 5 Директиви ЄС від 13 грудня 1999 р. "Про правові підстави для використання електронних підписів".

Стаття 4 Закону РФ "Про електронний цифровий підпис" від 10 січня 2002 р. передбачає, що ЕЦП в електронному документі рівнозначний власноручному підпису в документі на паперовому носії при одночасному дотриманні таких умов: а) сертифікат ключа підпису, який відноситься до даного ЕЦП, не втратив чинності на момент перевірки або на момент підписання електронного документа за наявності доказів, що визначають момент підписання; б) підтверджена дійсність ЕЦП в електронному документі; в) ЕЦП використовується у відповідно до відомостей, вказаних у сертифікаті ключа підпису.

Аналогічна норма міститься у Модельному законі Міжпарламентської асамблеї країн-учасниць СНД "Про електронний цифровий підпис" від 9 грудня 2000 р. в ст. 3 п. 4 та у Законі України від 22 травня 2003 р. "Про електронний цифровий підпис".

В Україні інфраструктура для використання електронного цифрового підпису у сфері господарювання лише починає ство-

рюватися. Необхідно відмітити вдалий досвід використання ЕЦП у сфері міжбанківських розрахунків, у сфері безготівкових розрахунків в Україні в національній валюті, у сфері організації захисту електронних банківських документів.

Так, виконання вимог щодо захисту банківської інформації є обов'язковим для всіх банків – учасників системи електронних платежів (СЕП). Система захисту електронних розрахункових документів складається з комплексу апаратно-програмних засобів криптографічного захисту та ключової системи до них, технологічних та організаційних заходів щодо захисту інформації в мережі. Апаратно-програмні засоби криптографічного захисту інформації в СЕП забезпечують аутентифікацію адресата та відправника електронних розрахункових документів, гарантують їх абсолютну достовірність та цілісність через неможливість підроблення або викривлення документів у шифрованому вигляді або за наявності електронного цифрового підпису. З цих підстав одним з обов'язкових реквізитів електронного розрахункового документа є названий ЕЦП, який дає змогу підтвердити цілісність такого документа та ідентифікувати особу, яка його підписала. Реалізація апаратно-програмних засобів криптографічного захисту виконується з урахуванням вимог міжнародних стандартів та має позитивні експертні оцінки державних служб України.

У юридичній літературі [93, 80, 81] та законодавстві України одночасно використовуються такі поняття, як електронний підпис, електронний цифровий підпис, цифровий підпис. Так, ч. 3 ст. 207 ЦКУ "Вимоги до письмової форми правочину" передбачає, що "використання при вчиненні правочинів факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, електронно-числового підпису[3] або іншого аналога власноручного підпису допускається у випад-

[3] Вважаємо, що вжитий у ЦК України термін "електронний числовий підпис" є помилковим перекладом з англійської мови "electronic digital signature". Жоден з нормативних актів світу та міжнародних організацій не містить такого поняття. Тому вважаємо за необхідне уточнити цей термін і називати його "електронний цифровий підпис".

ках, передбачених законом, іншими правовими актами або домовленістю сторін".

При цьому не приділяється увага співвідношенню цих понять, більш того, вони вживаються як синоніми, що не відповідає положенням спеціального Закону України від 22 травня 2003 р. "Про електронний цифровий підпис".

Вказаний закон вживає одночасно три поняття: електронний підпис, електронний цифровий підпис, цифровий підпис. Останні два поняття вживаються як синоніми, про що прямо зазначено в законі, і з цього приводу питань не виникає. Закріплюючи співвідношення поняття електронний підпис та електронний цифровий підпис (цифровий підпис), зазначається (ст. 1 закону), що ЕЦП є видом електронного підпису, під яким розуміються дані в електронній формі, які додаються до інших даних або логічно з ними пов'язані та призначені для ідентифікації підписувача електронного документа, і в преамбулі вказується, що дія даного закону не поширюється на відносини, що виникають під час використання інших видів електронного підпису, зокрема на переведене у цифрову форму зображення власноручного підпису.

Таким чином, поняття електронного підпису є родовим. Видами електронного підпису є ЕЦП, переведене у цифрову форму зображення власноручного підпису, інші символи, коди, паролі. ЕЦП за правовим режимом прирівнюється до власноручного підпису в силу прямої вказівки закону (ч. 1 ст. 3 Закону України "Про електронний цифровий підпис"). Інші види електронного підпису можуть бути прирівняні до власноручного підпису, якщо прийняті сторонами за взаємною згодою та з явним наміром підтвердити дійсність написаного, при цьому законодавство про електронні цифрові підписи на такі електронні підписи не поширюється. Правове регулювання використання таких електронних підписів здійснюється на підставі відповідних положень договору про порядок їх використання [167, 168, с. 109–128].

Вказаний підхід відповідає й Директиві Європейського парламенту та Ради 1999/93/ЄС від 13 грудня 1999 р. "Про правові

підстави Співдружності для використання електронних підписів", яка в ст. 2 виділяє електронний підпис – як дані в електронній формі, які приєднані або логічно пов'язані з іншими електронними даними, та які виступають в якості методу аутентифікації, та вдосконалений електронний підпис, під яким розуміється електронний підпис, що відповідає наступним вимогам: унікально пов'язаний з підписувачем; достатній для його ідентифікації; створюється з використанням засобів, що перебувають під виключним контролем підписувача; зв'язаний з електронним документом, до якого він відноситься, таким чином, що будь-яка наступна зміна електронного документа стає наочною.

Аналіз вказаної Директиви дозволяє стверджувати, що незважаючи на назву "вдосконалений електронний підпис", він з технічного боку ґрунтується на асиметричній криптографії, а з юридичного – має подібний правовий режим із електронним цифровим підписом, запровадженим, наприклад, у Російській Федерації, Німеччині, Україні. Аналогічно вказана Директива до поняття електронного підпису включає як вдосконалений електронний підпис, так і всі інші пов'язані з електронним документом символи, коди, паролі, тощо, якщо вони виконані та прийняті сторонами за взаємною згодою та з явним наміром підтвердити дійсність написаного.

Необхідно звернути увагу на те, що для укладання господарського договору на паперовому носії застосовується підпис уповноваженої особи та відбиток печатки (ч. 1 ст. 181 ГКУ), який підтверджує право даної особи діяти від імені підприємства, установи, організації. Зрозуміло, що поставити на електронному документі печатку неможливо фізично, через що відсутність печатки може бути підставою для визнання такого договору неукладеним.

Усуненню вказаної прогалини повинна сприяти норма, закріплена в ч. 5 ст. 5 Закону України від 22 травня 2003 р. "Про електронний цифровий підпис", яка передбачає, що у випадках, коли відповідно до законодавства необхідне засвідчення дійсності підпису на документах та відповідності копій документів оригіналам печаткою, на електронний документ накла-

дається ще один ЕЦП юридичної особи, спеціально призначений для таких цілей. Таким чином, укладаючи договір через мережі електрозв'язку, який об'єктивується в електронному документі, сторони повинні поставити по два ЕЦП (два ЕЦП, як аналоги власноручного підпису уповноважених осіб, і два ЕЦП замість печатки уповноважених осіб).

Але, таке положення вказаного закону України не зовсім коректне. Так, якщо певна особа, уповноважена від імені юридичної особи укладати господарські договори і бажає їх вчинювати з використанням електронних документів, тобто через мережі електрозв'язку, вона повинна звернутися до провайдера сертифікаційних послуг за одержанням ЕЦП з відповідним сертифікатом. У сертифікаті на підставі пред'явлення відповідних документів (виписки зі статуту, доручення тощо) буде зазначено, що ця особа уповноважена укладати від імені певної юридичної особи господарські договори. Якщо ця особа є посадовою особою підприємства, установи, організації, то це при підтвердженні відповідними документами також може бути вказано у сертифікаті. Крім того, в сертифікаті може бути зазначені цінові межі, в яких ця особа має право укладати правочини. Таким чином, сертифікат ЕЦП, виданий на ім'я уповноваженої особи юридичної особи, буде містити об'єктивні відомості про компетентність такої особи укласти той чи інший договір. А тому достатньо використовувати один ЕЦП, сертифікат якого буде містити відомості про компетентність вчиняти той чи інший господарський договір та буде підтверджувати право цієї особи діяти від імені певного підприємства, установи чи організації.

Саму таку позицію займає й Закон РФ "Про електронний цифровий підпис", який у ст. 19 передбачив, що електронний цифровий підпис у електронному документі, сертифікат якого містить необхідні при здійсненні цих відносин відомості про повноваження його володільця, визнається рівнозначним власноручному підпису особи у документі на паперовому носії, посвідченому печаткою.

На підставі викладеного та виходячи із запропонованого визначення ЕЦП, було б необхідним ч. 3 ст. 207 ЦКУ "Вимоги до письмової форми правочину" викласти в такій редакції: "Використання при вчиненні правочинів факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, електронно-цифрового підпису або іншого електронного підпису допускається у всіх випадках, крім тих, що прямо заборонені законом. Використання електронного цифрового підпису, а також інших видів електронного підпису, в порядку, передбаченому чинним законодавством України та (або) домовленістю сторін, юридично рівнозначно власноручному підпису уповноваженої особи".

Частину 5 ст. 5 Закону України "Про електронний цифровий підпис" доцільно викласти в такій редакції: "Електронний цифровий підпис у електронному документі, сертифікат якого містить необхідні при здійсненні даних відносин відомості про повноваження його володільця, визнається рівнозначним підпису особи в документі на паперовому носії, засвідченому печаткою".

Таким чином, особи, що здійснюють електронну комерцію, при вчиненні правочинів через мережі електрозв'язку повинні забезпечити виконання вимог закону щодо умов дійсності правочинів. Вказані правочини повністю відповідають законодавчим вимогам в частині законності змісту правочинів, здатності фізичних і юридичних осіб, що їх вчиняють, до участі в правочині, відповідності волі та волевиявлення. Виконання вимоги щодо дотримання письмової форми господарського договору, що вчиняється через мережі електрозв'язку, забезпечується використанням електронних документів та електронних підписів.

Підписання електронного документа, в якому об'єктивується господарський договір, вчинений через мережі електрозв'язку, відбувається із застосуванням електронного підпису, зокрема ЕЦП. Використання ЕЦП дозволяє ідентифікувати особу, яка підписує електронний документ, та однозначно встановити, що після акту підписання до електронного документа не вносилося змін та виправлень.

Використання електронних документів та електронних підписів, зокрема ЕЦП, для вчинення правочинів через мережі електрозв'язку, є необхідним та достатнім для забезпечення дотримання законодавчої вимоги про письмову форму господарського договору.

2.2. Порядок укладання договору через мережі електрозв'язку

Своєчасне та правильне укладання господарських договорів покликано сприяти впорядкуванню відносин між підприємствами, установами та організаціями, розвитку їх ділового співробітництва, більш ефективному використанню господарського договору [169, с. 20]. Саме тому в юридичній літературі чимало уваги приділялося питанням про порядок укладання договорів, оскільки вони мають глибокий теоретичний зміст та велике практичне значення [147, с. 216, 170, с. 19, 171, с. 76–79].

Можливість суб'єктів електронної комерції укладати договори через мережу електрозв'язку ґрунтується на досягненні згоди контрагентів, тобто один з них повинен зробити пропозицію про укладання договору (оферта), а інший повинен прийняти цю пропозицію (акцепт). Згідно з чинним цивільним законодавством договір вважається укладеним, коли між сторонами в потрібній у належних випадках формі досягнуто згоди по всіх істотних умовах (ч. 1 ст. 153 ЦК УРСР). Таким чином, порядок укладання господарських договорів підпорядковується перш за все загальному режиму, встановленому для цивільних договорів [142, с. 85, 34, с. 388].

Існуючі законодавчі та доктринальні вимоги до оферти та акцепту можна розділити на три групи. Перша група вимог стосується змісту (оферта та акцепт повинні виражати узгоджену волю сторін по всіх істотних умовах договору). Друга група вимог стосується форми вчинення оферти та акцепту (оферта та акцепт оферти вчиняються у формі, яка передбачена для вчинення відповідного договору – усна чи письмова). Третя група вимог стосується процедурних питань вчинення оферти

та акцепту оферти (ст. 155–158 ЦК УРСР), а саме: укладання договору за пропозицією, зробленою з зазначенням строку для відповіді, укладання договору за пропозицією, зробленою без зазначення строку для відповіді, відповідь про згоду на укладання договору, одержана із запізненням, відповідь про згоду укласти договір на інших умовах). Таким чином, для визнання оферти та акцепту такими, що породжують юридичні наслідки, сторони повинні забезпечити виконання всіх вимог, що висуваються до них (вимоги до змісту, форми та порядку вчинення) [172].

Доктрина господарського права визначає укладання господарського договору як зустрічні договірно-процедурні дії двох або більше суб'єктів господарювання щодо вироблення умов договору, які відповідають їх реальним намірам та економічним інтересам, а також юридичне оформлення договору як правового акта [173, с. 140]. Таким чином, оформлення договірних взаємовідносин здійснюється, як правило, шляхом складання одного документа, який підписується сторонами [174, с. 29].

Загальний порядок укладання господарських договорів та особливості укладання договорів певного виду (попередні договори, договори за державним замовленням, організаційно-господарські договори, тощо) врегульовані ГКУ (ст. ст. 181–187).

Як вже зазначалося раніше, особливість господарських договорів, що вчиняються через мережі електрозв'язку, полягає у використанні електронних документів, в яких вони об'єктивуються. Тобто матеріальним носієм письмової форми господарських договорів, що вчиняються через мережі електрозв'язку, виступають електронні носії. У зв'язку з цим виникає необхідність визначення поняття "електронного документа" та його співвідношення із традиційним документом на паперовому носії.

Документ (від лат. dokumentum – *повчальний приклад, взірець, свідчення, доказ*) – матеріальна форма відображення, поширення, використання і зберігання інформації, яка надає їй юридичну силу. Юридично значуще визначення поняття документа можна знайти у В.Я. Дорохова: "Документ – це письмовий акт встановленої або загальноприйнятої форми, складений певними та компетентними установами, підприємствами,

організаціями, посадовими особами, а також громадянами для викладення відомостей про факти або посвідчення фактів, які мають юридичне значення, або для підтвердження прав та обов'язків" [175, с. 55].

Поняття документа міститься у ряді нормативних актів. Найбільш вдалим є визначення, що міститься у Законі України "Про обов'язковий примірник документів" [176], згідно з яким документ визначається як матеріальна форма одержання, зберігання, використання і поширення інформації, зафіксованої на папері, магнітній, кіно-, фотоплівці, оптичному диску або іншому носієві. Таким чином, поняття документа розкривається через поняття інформації, визначення якої Закон України "Про обов'язковий примірник документів" не містить. Але це поняття закріплене в Законі України "Про інформацію" (ст. 1), в якому під інформацією розуміються документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Отже, інформація представляється у двох формах – документована (матеріалізована на певному носієві) та публічного оголошена (не матеріалізована). А звідси документом може виступати лише та частина інформації, яка закріплена на певному матеріальному носієві.

Якщо узагальнити наведені визначення, то документ можна визначити як складену певними та компетентними установами, підприємствами, організаціями, посадовими особами, а також громадянами матеріальну форму одержання, зберігання, використання і поширення юридично значущих відомостей про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі, зафіксованих на певному матеріальному носієві. Отже, документ – це, перш за все, матеріальна форма відображення, поширення тощо певної інформації, яка, в свою чергу, виступає змістом документа.

Виходячи з цього визначення, можна виділити вимоги, що висуваються до документа: 1) документом може бути не будь-яка інформація, зафіксована на матеріальному носієві, а лише

відомості певного характеру (вимога до змісту); 2) вимоги до форми – це, по суті, вимоги, які забезпечують доказову функцію документа (реквізитами форми можуть бути наявність печатки та підпису певної особи, особисті дані про особу, яка видала документ, а також вимоги до матеріального носія); 3) компетентність джерела документа – ця вимога пов'язує перші дві групи вимог, надає юридичного значення документу, оскільки документ, виданий некомпетентним органом, підписаний не уповноваженою на те особою або анонімний, не може підтверджувати викладені в ньому відомості про факти, посвідчувати факти або підтверджувати права та обов'язки.

Вказані вимоги дозволять дослідити співвідношення документа та електронного документа. Створення та використання електронних документів складає один з блоків правовідносин, який складає поняття електронної комерції. В нормативних актах України використовується термін "електронний документ", але з різними визначеннями. В юридичній літературі також наводяться різні визначення цього терміна, що ускладнює його розуміння та використання. Вказаний недолік може бути усунутий шляхом закріплення у Законі "Про електронну комерцію" визначення поняття електронного документа.

Так, наприклад, в юридичній літературі електронний документ визначають як інформацію, зафіксовану на електронних носіях та яка містить реквізити, що дозволяють її ідентифікувати [177, с. 40]; як інформацію, представлену у формі набору станів елементів електронної обчислювальної техніки, інших засобів обробки, зберігання та передачі інформації, яка може бути перетворена у форму, придатну для однозначного сприйняття людиною, та яка має атрибути ідентифікації документа [178].

О.О. Косовець пропонує визначати електронний документ як набір записаних даних у вигляді, що читається комп'ютером, для яких: існує визнана учасниками електронного документообігу або затверджена компетентними органами процедура, яка дозволяє однозначно перетворити ці дані в документ традиційного режиму; визнання зазначеної процедури учасниками системи електронного документообігу шляхом традиційного

(письмового) документа, або така процедура санкціонована уповноваженим державним органом [179, с. 53].

Законодавство України використовує поняття електронного документа переважно у вузькій сфері фінансових розрахункових відносин.

Так, Закон України "Про електронні документи та електронний документообіг" у ст. 5 визначає електронний документ як документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Наведене у законі визначення не зовсім вдале, оскільки воно не враховує вимог, що висуваються до документа взагалі, а також не акцентується увага на тому, що документ взагалі, та електронний документ зокрема, це матеріальна форма відображення, поширення, тощо інформації, яка виступає змістом документа. При цьому вказаний Закон не визначає поняття електронних даних, що також не полегшує розуміння цього поняття.

Закон України "Про платіжні системи та переказ грошей в Україні» в ст. 1 дає визначення поняття електронного документа як документа, інформація в якому представлена у формі електронних даних, включаючи відповідні реквізити документа, в тому числі і електронний цифровий підпис, який може бути сформований, переданий, збережений і перетворений електронними засобами у візуальну форму чи на папері. Відразу необхідно зазначити, що цей закон є спеціальним, призначеним для регулювання досить вузького кола відносин – загальних засад функціонування платіжних систем в Україні, а тому поняття електронного документа, визначення якого наводиться в цьому законі, також використовується саме в контексті зазначеного вузького кола правовідносин. В той же час наведене визначення справедливо підкреслює, що електронний документ є документом, особливість якого полягає у використанні електронних носіїв для фіксації інформації, що складає його зміст.

Інструкція від 27 грудня 1999 р. (в редакції 23 квітня 2002 р.) "Про міжбанківські розрахунки в Україні", затверджена Постановою Правління НБУ України № 621, у п. 5 "Загальних по-

ложень" використовує поняття електронного розрахункового документа, який визначається як документ на переказ, сформований банком на підставі розрахункових документів банку, клієнтів, документів на переказ готівки, доручень на договірне списання, та представлений у формі електронних даних, що включають відповідні реквізити документа, у тому числі й електронний цифровий підпис. Вказане поняття є вузькоспеціалізованим та використовується виключно при проведенні міжбанківських розрахунків, а також при проведенні розрахунків через систему електронних платежів Національного банку України.

Поняття електронного документа використовується і у ряді інших держав. Так, ст. 1 Закону Туркменістану від 19 грудня 2000 р. "Про електронний документ" визначає електронний документ як інформацію, зафіксовану на машинному носії, посвідчену електронним цифровим підписом відповідно до процедури створення такого підпису. Подібне визначення міститься у ст. 1 Закону Республіки Бєларусь " Про електронний документ". Закон штату Юта США від 3 липня 2000 р. "Про електронні правочини" визначає електронний документ як документ, створений, генерований, відісланий, переданий, отриманий або збережений за допомогою електронних пристроїв. Аналогічна норма міститься у ст. 1 закону Канади "Про електронну комерцію".

Отже, відсутній єдиний підхід до розуміння і визначення поняття електронного документа. Але можна виділити загальні ознаки, які присутні у всіх вищенаведених визначеннях електронного документа: 1) зміст електронного документа складає інформація, зафіксована на тому чи іншому електронному носії; 2) наявність погодженої або імперативно закріпленої процедури перетворення такого електронного документа у письмовий документ на паперовому носії.

Вирішуючи питання про співвідношення понять документа та електронного документа, необхідно зазначити, що єдина відмінність між ними полягає у виді матеріального носія, що використовується для фіксації його змісту (паперовий носій та

електронний носій). Усі вимоги, що висуваються до документа на паперовому носієві, повністю виконуються електронним документом. Так, електронний документ закріплює певні відомості про явища, які відбуваються між особами, що здійснюють електронну комерцію (вимога до змісту). Вчинення правочинів через мережі електрозв'язку означає, що вони матеріалізуються на електронному носієві (вінчестер, диск, дискета, сервер, тощо). Тобто завжди є матеріальний носій інформації. Електронні документи набувають правового значення лише за умови наявності повноважень осіб, які їх підписали, оскільки електронний документ, незалежно від того, на якому носієві він відображений, підписаний не уповноваженою на те особою або анонімний, не може підтверджувати викладені в ньому відомості і породжувати права та обов'язки. Процедура перетворення електронного документа у документ на паперовому носієві встановлюється імперативною нормою. Зміст електронного документа складає інформація, зафіксована на тому чи іншому електронному носієві.

Таким чином, доцільно визначати електронний документ як документ, складений певними та компетентними установами, підприємствами, організаціями, посадовими особами, а також громадянами, зміст якого складають юридично значущі відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі, що зафіксовані на електронному носії (магнітний диск, лазерний диск, тощо), який використовується для запису та зберігання інформації за допомогою електронно-обчислювальної техніки.

Запропоноване визначення електронного документа є доктринальним та охоплює всі вимоги, що висуваються до документів, акцентується увага на тому, що електронний документ – це документ, зміст якого складає інформація, що зафіксована на електронних носіях. Для врегулювання відносин щодо порядку створення та використання електронних документів доцільно залишити визначення електронного документа, закріпленого у ст. 1 Закону України "Про платіжні системи та переказ грошей в Україні» як документа, інформація в якому

представлена у формі електронних даних, включаючи відповідні реквізити документа, в тому числі і електронний цифровий підпис, який може бути сформований, переданий, збережений і перетворений електронними засобами у візуальну форму чи на папері.

Повертаючись до порядку укладення господарських договорів через мережі електрозв'язку, необхідно зазначити, що такий договір повинен за загальним правилом викладатися у вигляді єдиного електронного документа, підписаного сторонами шляхом накладання електронного підпису, зокрема ЕЦП. Проект такого договору може бути запропонований будь-якою з сторін та надісланий іншій стороні. Оскільки всі електронні документи, що ідентичні за змістом, є оригіналами, то вони не можуть мати копій на електронних носіях, а тому направляти стороні два ідентичних електронних документи з проектом договору недоцільно. Одержувач електронного документа з ЕЦП відправника сам в змозі скопіювати одержаний документ та отримати два оригінали з ЕЦП відправника.

Сторона, яка одержала проект договору, у разі згоди з його умовами повинна оформити договір відповідно до вимог ч. 1 ст. 181 ГКУ, тобто підписати його шляхом накладання свого електронного підпису, зокрема ЕЦП, і повернути один з оригіналів договору другій стороні у двадцятиденний строк.

Сторона, одержавши проект договору, підписаний за допомогою такого ЕЦП, звернеться до провайдерів з приводу перевірки сертифікату підпису підписувача електронного документа. Провайдер підтверджує дійсність сертифіката, і тим самим дає можливість стороні, яка одержала проект договору, переконатися у правомочності особи, яка підписала проект договору.

За наявності заперечень щодо окремих умов договору, що вчиняється через мережі електрозв'язку, сторона, яка одержала проект договору, складає протокол розбіжностей, про що робиться застереження у договорі, та у двадцятиденний строк надсилає другій стороні протокол розбіжностей разом з підписаним договором.

Сторона, яка одержала протокол розбіжностей до договору, що укладається у сфері електронної комерції, зобов'язана про-

тягом двадцяти днів розглянути його, в цей же строк вжити заходів для врегулювання розбіжностей з другою стороною та включити до договору всі прийняті пропозиції, а ті розбіжності, що залишилися неврегульованими, передати в цей же строк до суду, якщо на це є згода другої сторони.

У разі досягнення сторонами згоди щодо всіх або окремих умов, зазначених у протоколі розбіжностей, така згода підтверджується у письмовій формі. Вказана вимога повинна вважатися виконаною, якщо таке підтвердження одержане у вигляді електронного документа з електронним підписом уповноваженої особи.

При недосягненні сторонами згоди з усіх істотних умов господарського договору, що укладається через мережі електрозв'язку, такий договір повинен вважатися неукладеним. Якщо одна з сторін вчинила фактичні дії щодо його виконання, правові наслідки таких дій повинні визначатися відповідно до норм ЦК України.

Аналогічно законодавче регулювання використання електронних документів дозволяє виконувати всі вимоги ГКУ щодо особливостей укладання попередніх господарських договорів, за державним замовленням тощо, що здійснюється через мережі електрозв'язку.

Так, наприклад, одна з послуг, яку надають інформаційні посередники особам, що здійснюють електронну комерцію, надання доступу до мереж електрозв'язку, зокрема до мережі Інтернет, що юридично може оформлюватися укладанням господарського договору Інтернет-провайдингу [118, с. 4], зокрема через мережі електрозв'язку, який за своєю природою є різновидом договору про надання послуг.

Пропозиція на укладання такого договору, як правило, розміщується в телекомунікаційній мережі Інтернет на сайті інформаційного посередника. Пропозиція містить повну інформацію про послугу, яка надається, та порядок її оплати, що є достатнім для визнання такої пропозиції офертою. Пропозиція носить відкритий характер та направлена будькому, тобто таку оферту можна розглядати як публічну

(інформаційний посередник зобов'язується надати послугу будь-якій особі, яка до нього звернулася та згодна з умовами договору Інтернет-провайдингу). Умови такого договору є однаковими для всіх послугоодержувачів. Інформаційні посередники, як правило, пропонують гнучкі умови та можливість індивідуального підбору конкретного виду послуг, при цьому загальні умови та сама можливість вибору надається всім потенційним контрагентам на рівних умовах. За загальним правилом, інформаційні посередники не можуть надавати переваг одному потенційному контрагенту перед іншим при укладенні договору – щодо ціни, порядку надання доступу до мережі електрозв'язку тощо.

Інформаційні посередники розміщують на своїх сайтах в мережі електрозв'язку умови договору Інтернте-провайдингу, які містять вичерпну інформацію про послугу, яка надається – порядок надання доступу до мережі Інтернет, основні та додаткові послуги, порядок оплати тощо. Потенційному контрагенту достатньо лише обрати умови, які найбільше його задовольняють (часто інформаційні посередники пропонують своїм контрагентам набори послуг у вигляді "пакетів"), та підписати договір за допомогою електронного підпису.

Договір Інтернет-провайдингу в більшості випадків нагадує договір про приєднання, за яким сторона, що його підписує, не має права наполягати на зміні його змісту, а тому внесення яких-небудь інших умов, ніж ті, що пропонуються інформаційним посередником, як правило, не передбачається договором. Більшість проектів договорів, які пропонуються інформаційними посередниками, містять умову, згідно з якою акцептування запропонованого проекту договору означає, що контрагент згодний зі всіма його положеннями.

При використанні електронних документів у сфері електронної комерції виникає питання про те, чи дійсно електронний документ було направлено особою, зазначеною в якості відправника [180, 181, с. 92]. У разі передачі документа на паперовому носії така проблема може виникнути в результаті можливої фальсифікації підпису відправника. В умовах засто-

сування електронних засобів (мереж електрозв'язку) електронний документ може бути відправлений:

- самим відправником;
- іншою уповноваженою особою; або
- інформаційною системою, запрограмованою функціонувати в автоматичному режимі.

Так, електронний документ повинен вважатися електронним документом відправника, якщо він був відправлений самим відправником, тобто якщо він дійсно відправив такий документ.

У відносинах між відправником та адресатом електронний документ вважається електронним документом відправника, якщо він був відправлений: особою, яка мала повноваження діяти від імені відправника щодо даного електронного документа; або інформаційною системою, запрограмованою відправником функціонувати в автоматичному режимі. Зазначене правило стосується ситуації, коли електронний документ був відправлений не відправником, а іншою особою, яка мала повноваження діяти від імені відправника.

В цих випадках цілісність електронного документа може бути точно встановлена адресатом за допомогою застосування процедури, узгодженої з відправником. З цією метою відправник та адресат попередньо узгоджують процедуру підтвердження цілісності електронного документа. Зазначений висновок відповідає положенням ст. 13 Типового закону "Про електронну торгівлю". Так, наприклад, адресат та відправник можуть обумовити використання ЕЦП чи іншого виду електронного підпису для підтвердження цілісності електронного документа. У випадку використання ЕЦП для підтвердження цілісності електронного документа відправнику та адресату достатньо послатися на ст. 4 та 3 Закону України "Про електронний цифровий підпис", які передбачають застосування ЕЦП для ідентифікації відправника електронного документа та встановлення цілісності самого документа.

Якщо адресат та відправник обрали для підтвердження цілісності електронного документа інший вид електронного підпису, вони повинні попередньо детально узгодити вид елек-

тронного підпису, що використовується, порядок його перевірки, порядок узгодження розбіжностей, які можуть з'явитися при виникненні спору про наявність договору, підписаного даним видом електронного підпису, на яку сторону покладається обов'язок доведення тих чи інших фактів та достовірності електронного підпису. З урахуванням цієї процедури суд зможе перевірити достовірність наданих сторонами доказів. Аналогічні висновки містяться у Листі Вищого Арбітражного Суду РФ від 19 серпня 1994 р. № С1-7/оп-578 [182], де передбачено, що у випадку, коли між сторонами виник спір про наявність договору та інших документів, підписаних цифровим (електронним) підписом, арбітражний суд повинен запитати у сторін виписку з договору, в якій вказана процедура порядку узгодження розбіжностей, на яку сторону покладається обов'язок доведення тих чи інших фактів та достовірності підпису. З урахуванням цієї процедури арбітражний суд перевіряє достовірність наданих сторонами доказів. За необхідності арбітражний суд вправі призначити експертизу по спірному питанню, використовуючи при цьому передбачену договором процедуру.

У випадку відсутності попередньо узгодженої процедури підтвердження цілісності електронного документа, коли відправник чи адресат оспорює наявність підписаного електронного документа, суд не зможе прийняти в якості доказів документи, підписані таким електронним підписом.

Мета закріплення положення про перевірку цілісності електронного документа з використання попередньо узгодженої процедури полягає в тому, щоб адресату надати право діяти на підставі припущення про те, що електронний документ є електронним документом відправника, до моменту отримання від відправника повідомлення про те, що такий електронний документ не є електронним документом відправника, та мати в своєму розпорядженні розумно необхідний час для вчинення належних дій.

У випадку, коли адресату стало відомо або повинно було стати відомо про те, що електронний документ не є електронним документом відправника, припущення про належність електронного документа відправникові повинно переставати

діяти. Аналогічний наслідок повинен наступати й у тому випадку, коли в результаті перевірки оригінальності електронного документа за допомогою процедури, попередньо узгодженої з відправником для цієї мети, оригінальність електронного документа не була підтверджена.

Отже, якщо адресат застосував процедури перевірки цілісності, попередньо узгоджені з відправником, і в результаті застосування таких процедур було належним чином перевірено, що джерелом електронного документа є відправник, даний електронний документ вважається електронним документом відправника.

З положення про необхідність перевірки цілісності електронного документа з використання попередньо узгодженої процедури можна зробити висновок про те, що якщо адресат одержав повідомлення відправника про те, що такий електронний документ не є електронним документом відправника, адресат не має права вважати, що електронний документ є документом відправника та діяти, виходячи з цього припущення. Тобто, одержання такого електронного документа не може мати зворотньої сили щодо попереднього електронного документа. Таким чином, відправник звільняється від наслідків у зв'язку з електронним документом після того, як був одержаний електронний документ, але не до цього моменту.

З наведеного можна зробити ще один висновок, а саме: нема підстав визнавати електронний документ, який був фактично відправлений відправником, і адресат належним чином застосував узгоджену процедуру перевірки цілісності такого документа, таким, що надісланий іншою особою, коли відправник повідомляє адресату, що одержаний ним електронний документ не є електронним документом відправника.

Тобто, якщо в результаті такої перевірки адресат одержить підтвердження того, що даний електронний документ є електронним документом відправника, то повинне застосовуватися правило про те, що електронний документ вважається електронним документом відправника, якщо він був відправлений самим відправником.

На підставі викладеного необхідно зазначити, що закон "Про електронну комерцію", який покликаний врегулювати, зокрема, порядок використання електронних документів для вчинення правочинів через мережі електрозв'язку, повинен містити норми, які б закріплювали правові підстави вважати електронний документ таким, що надісланий відправником. Зокрема повинно бути передбачено, що електронний документ вважається таким, що виходить від відправника, коли він надісланий самим відправником, іншою уповноваженою особою, або інформаційною системою, запрограмованою функціонувати в автоматичному режимі.

При укладанні господарських договорів через мережі електрозв'язку важливого значення набуває практика використання функціональних підтверджень одержання електронного документа. Враховуючи комерційну цінність системи підтвердження одержання електронних документів та широке використання таких систем в контексті електронної комерції, доцільно у законі "Про електронну комерцію" вирішити ряд правових питань, що виникають в результаті використання процедур підтвердження.

Необхідно зазначити, що законопроект "Про електронну торгівлю" не вимагає від осіб, які здійснюють електронну комерцію, підтверджувати одержання електронних документів. Також не згадується можливість використання підтвердження одержання електронного документа за взаємною згодою сторін. Такий підхід є не зовсім вдалим, оскільки для вчинення правочинів через мережі електрозв'язку має істотне значення не тільки сам факт одержання електронного документа, а й час його одержання, крім цього такий підхід не відповідає Типовому закону ЮНСІТРАЛ "Про електронну комерцію", який у ст. 14 дозволяє використовувати процедуру підтвердження у випадку, коли сторони про це попередньо домовилися.

Цікаву позицію з даного питання займають законопроекти РФ "Про електронну торгівлю" та "Про правочини, що вчиняються за допомогою електронних засобів зв'язку (електронні правочини)", які передбачають, що одержання електронних документів повин-

но бути підтверджене адресатом, якщо інше не передбачене домовленістю між відправником та адресатом електронного документа; електронні документи вважаються невідправленими до тих пір, поки відправник не одержав підтвердження адресата, якщо інше не передбачене домовленістю між відправником та адресатом електронного документа. Такий підхід є правильним. Він враховує те, що електронна комерція перебуває в Україні на етапі становлення, відсутня чітка судова практика щодо правочинів, які вчиняються через мережі електрозв'язку.

Поняття підтвердження охоплює різні процедури – від простого підтвердження одержання електронного документа до виявлення згоди зі змістом конкретного електронного документа. У багатьох випадках процедура підтвердження може заміняти систему, відому в поштовій справі як "вимагається підтвердження одержання".

Вимога про підтвердження одержання може міститися у різних джерелах: в самому електронному документі, двосторонніх або багатосторонніх правочинах про обмін електронними документами, законодавстві. Закріплення вимоги про необхідність підтвердження одержання електронного документа не стосується правових наслідків, які можуть виникнути у зв'язку з відправленням підтвердження одержання. Підтвердження одержання означає виключно факт одержання електронного документа. Наприклад, коли відправник надсилає електронний документ, в якому міститься оферта, та просить підтвердити одержання, підтвердження одержання означає лише те, що оферта одержана. Питання про те, чи можна вважати направлення цього підтвердження акцептом оферти, регулюється нормами чинного цивільного права України.

У випадку, коли відправник не домовився з адресатом про те, що підтвердження буде здійснено в якій-небудь конкретній формі або шляхом конкретного способу, підтвердження може бути здійснено шляхом:

1) направлення будь-якого електронного документа з боку адресата, який направляється автоматизованим або іншим способом; або

2) вчинення будь-яких дій з боку адресата, достатніх для того, щоб показати відправнику, що електронний документ було одержано.

Таким чином, юридично визнається факт підтвердження за допомогою будь-якого електронного документа або будь-яких дій адресата (наприклад, відвантаження товарів в якості підтвердження одержання замовлення на поставку) у випадку, коли відправник не направив запит про представлення такого підтвердження в якій-небудь конкретній формі.

У випадку, коли відправник в односторонньому порядку вимагає підтвердження в конкретній формі, то адресат не має права підтверджувати одержання електронного документа за допомогою будь-якого електронного документа чи будь-яких дій, достатніх для вказівки відправнику на одержання електронного документа.

Вимога відправника надіслати адресату підтвердження одержання відправленого електронного документа означає, що електронний документ вважається невідправленим до тих пір, поки не буде одержано підтвердження одержання. Звідси випливає, що не підтвердження одержання електронного документа адресатом не залежить від того, передбачив чи ні відправник, що таке підтвердження повинно бути одержано протягом певного строку.

З факту одержання відправником від адресата підтвердження одержання випливає, що відповідний електронний документ був одержаний адресатом. Причому така презумпція не означає, що відправлений електронний документ відповідає одержаному електронному документу. У відносинах між відправником та адресатом, коли електронний документ являється електронним документом відправника, адресат має право вважати, що одержаний електронний документ є таким, яким відправник його відправив, та діяти, виходячи з цього припущення. Тобто невідповідність між текстом відправленого електронного документа та одержаного електронного документа означає, що переважну силу буде мати одержаний текст.

На підставі викладеного можна зробити висновок про те, що використання процедури підтвердження одержання електронних документів є поширеною практикою у сфері електронної

комерції у всьому світі. Це дає можливість говорити про доцільність введення до закону "Про електронну комерцію", ряду положень, які б законодавчо закріпили процедуру підтвердження одержання електронних документів:

1) одержання документа на електронному носії повинно бути підтверджено адресатом. Якщо відправник не домовився з адресатом про певну форму чи спосіб підтвердження, підтвердження може бути здійснено шляхом: а) відправлення будь-якого електронного документа з боку адресата; б) вчинення будь-яких дій з боку адресата, достатніх для того, щоб показати відправнику, що електронний документ був одержаний;
2) електронний документ вважається невідправленим до тих пір, поки відправник не одержав підтвердження адресата. У сфері укладання господарських договорів через мережі електрозв'язку виключно важливого значення набуває питання оригіналу та копій електронних документів, в яких об'єктивується такий договір.

Якщо визначати оригінал як носій, на якому відбувається перший запис інформації, то говорити про оригінальність електронного документа неможливо, оскільки адресат електронного документа завжди буде одержувати його копію. [183, с. 192] В електронній комерції вимога представлення оригіналів є однією з перепон на шляху її розвитку, і тому вирішення питання оригіналу та копії електронних документів є необхідним, оскільки на практиці багато спорів пов'язано із питанням оригінальності документів.

Законодавче закріплення положень про оригінал електронного документа може мати безпосереднє відношення до галузі цивільного та господарського права, де існують вимоги щодо реєстрації чи нотаріального посвідчення письмової форми, а також до товаророзпорядчих та оборотних документів, стосовно яких поняття унікальності має особливе значення. Прикладами документів, які повинні надаватися в оригіналі, є торгові документи, наприклад сертифікати ваги, сільськогосподарські сертифікати, сертифікати якості або кількості, страхові свідоц-

тва, тощо. Хоча такі документи не відносяться до числа оборотних і не використовуються для передачі прав або титулу, важливо, щоб вони передавалися у незмінному вигляді, тобто в їх оригінальній формі, для того, щоб інші учасники господарської діяльності могли покладатися на їх зміст. У випадку використання вказаних документів на паперовому носії вони приймаються тільки в тому випадку, якщо вони є оригіналами, для того, щоб зменшити можливість внесення до них змін, що було б важко виявити на копіях. Існує цілий ряд технічних засобів для підтвердження оригінальності змісту електронного документа. Без таких засобів купівля-продаж товарів з використанням електронної комерції була б утруднена в зв'язку з тим, що емітенти таких документів будь-який раз повинні були б повторно передавати свої електронні документи при продажу товарів або ж сторони були б змушені використовувати паперові документи в доповнення до правочинів, вчинених через мережі електрозв'язку.

Закон України від 22 травня 2003 р. "Про електронні документи та електронний документообіг" передбачає, що всі екземпляри електронного документа, підписані за допомогою електронного підпису, є оригіналами. Подібну норму містить Закон Республіки Бєларусь "Про електронний документ" (ст. 8), Законопроект України "Про електронну торгівлю", законопроекти РФ "Про електронну торгівлю", "Про правочини, що вчиняються за допомогою електронних засобів зв'язку (електронні правочини)".

Законопроект РФ "Про електронний документ" пропонує закріпити аналогічну норму, при цьому уточнюючи, що при використанні електронного документа не вимагається надання його копії на паперовому носії, за виключенням випадків, передбачених законодавством або домовленістю сторін. Таке уточнення є доцільним, оскільки дублювання електронних документів на паперових носіях буде зводити нанівець всі переваги електронної комерції та стримувати її розвиток.

Таким чином, можна зробити висновок про те, що і у законопроектах нашої держави, і у законопроектах Російської Федерації та ряду інших держав світу поняття оригіналу електрон-

ного документа визначається однаково. При прийнятті в Україні закону "Про електронну комерцію" доцільно передбачити розуміння оригіналу електронного документа, яке міститься у законопроекті України "Про електронну торгівлю" – всі екземпляри електронного документа, підписані за допомогою електронного підпису, є оригіналами.

З даного розуміння оригіналу електронного документа можна зробити два висновки. Перший стосується того, що у разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації, кожний з електронних примірників вважається оригіналом електронного документа та має однакову юридичну силу. Другий полягає в тому, що якщо підписувачем створюються ідентичні за змістом та реквізитами електронний документ та звичайний документ на папері, кожен з документів є оригіналом.

Стаття 8 Типового закону ЮНСІТРАЛ "Про електронну комерцію" та ст. 11 Акта від 30 серпня 1999 р. "Про електронну комерцію" Канади [184] встановлюють вимоги, яким повинен відповідати оригінал електронного документа: а) давати змогу довести його цілісність згідно з процедурою, передбаченою законодавством; б) у визначених законом випадках документ може бути пред'явлений у візуальній формі, у тому числі на паперовому носії.

Цілісність оригіналу електронного документа означає збереження інформації в повному та незмінному вигляді, без врахування будь-яких змін, що відбуваються при нормальному процесі передачі, зберіганні та представленні. Вказуючи на цілісність електронного документа, збереження інформації у незмінному вигляді, ми зробили виняток для необхідних додатків до оригінального електронного документа, наприклад електронних підписів, зокрема ЕЦП. До тих пір, поки зміст електронного документа залишається повним та незміненим, необхідні додатки до цього електронного документа не будуть впливати на його оригінальність. Так, коли в кінці оригінального електронного документа додається ЕЦП для підтвердження його оригінальності або коли комп'ютерні

системи автоматично додають дані на початку та в кінці електронного документа для його передачі, такі додатки повинні розглядатися як такі, як би вони були додатковою паперовою сторінкою до оригінальної паперової сторінки або як конверт та марка, що використовуються для пересилання такої оригінальної паперової сторінки.

Вже згадуваний законопроект України "Про електронну торгівлю", вирішуючи питання про копії електронних документів, пропонує закріпити положення про те, що електронний документ не може мати копій в електронному виді; копії електронного документа можуть бути виготовлені (роздруковані) у виді паперового документа і завірені власноручним підписом уповноваженої особи.

Аналогічну позицію з цього питання займає Закон Республіки Бєларусь "Про електронний документ" (ст. ст. 8, 9), вже згадувані законопроекти РФ "Про електронну торгівлю", "Про правочини, що вчиняються за допомогою електронних засобів зв'язку (електронні правочини)".

На підставі викладеного необхідно зазначити, що викладене у законопроекті України "Про електронну торгівлю" розуміння понять оригіналу та копії електронного документа є загальнопоширеним, сприйнятим у законодавстві окремих держав світу, що дає підстави вважати доцільним закріпити у законі "Про електронну комерцію" такі положення:

- всі екземпляри електронного документа, підписані за допомогою електронного підпису, є оригіналами;
- оригінал електронного документа повинен відповідати таким вимогам: а) його цілісність може бути доведеною згідно з процедурою, передбаченою законодавством або домовленістю сторін; б) він може бути представлений у візуальній формі, у тому числі на паперовому носії, у визначених законом випадках;
- електронний документ не може мати копій в електронному виді; копії електронного документа можуть бути виготовлені (роздруковані) у виді паперового документа і завірені власноручним підписом уповноваженої особи.

Відсутність законодавчого закріплення правил зберігання електронних документів, наприклад з метою звітності або оподаткування, є одною з перепон розвитку електронної комерції в Україні. Її подоланню може сприяти закріплення правила про те, що у випадку, коли законом чи іншим нормативним актом вимагається збереження певних документів або інформації, ця вимога вважається виконаною шляхом зберігання електронних документів. Це положення знайшло відображення у законопроекті України "Про електронну торгівлю" й законопроектах РФ "Про електронну торгівлю" та "Про правочини, що вчиняються за допомогою електронних засобів зв'язку (електронні правочини) в частині збереження електронних документів.

Вказані законопроекти та ст. 10 Типового закону ЮНСІТРАЛ "Про електронну комерцію" передбачають ряд умов, які повинні виконуватися при збереженні електронних документів:

а) інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;
б) електронний документ повинен зберігатися у тому форматі, в якому він був підготовлений, відправлений або одержаний;
в) інформація повинна давати змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Необхідно звернути увагу на те, що пункт "б" не говорить про необхідність збереження інформації у незмінному вигляді, якщо інформація, що зберігається, точно відтворює електронний документ, який був відправлений. Було б недоцільно вимагати, щоб інформація зберігалася у незміненому вигляді, оскільки, як правило, для цілей зберігання електронні документи розшифровуються, ущільнюються або перетворюються.

Пункт "в" повинен охоплювати всю ту інформацію, яку необхідно зберігати, та яка включає окрім власне електронного документа певну супровідну інформацію для ідентифікації електронного документа.

Таким чином можна зробити висновок про те, що необхідність зберігання електронних документів, обмін якими

дозволяє вчиняти правочини через мережі електрозв'язку, є очевидною та безспірною. Цю точку зору розділяють й автори законопроекту України "Про електронну торгівлю" (який повинен врегулювати здійснення електронної комерції в Україні, зокрема відносини з використання з цією метою електронних документів), який серед умов, які висуваються до збереження електронних документів, називає те, що: інформація, яка міститься в електронному документі, повинна бути доступною для її подальшого використання; електронний документ повинен зберігатися у тому форматі, в якому він був підготовлений, відправлений або одержаний; інформація повинна давати змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Висвітлення питання часу і місця відправлення та одержання електронних документів необхідне у зв'язку з тим, що для укладання правочинів через мережі електрозв'язку важливе значення має встановлення часу і місця одержання електронного документа. Законодавці різних держав світу, які вже врегулювали відносини у сфері електронної комерції, або лише тільки починають це робити, не залишають це питання без уваги.

Законопроект України "Про електронну торгівлю", вирішуючи питання про час та місце відправлення і одержання електронних документів, зазначає, що електронний документ вважається відправленим, коли він надходить до інформаційної системи, яка не перебуває під контролем відправника; якщо інше не погоджено між адресатом та відправником, електронний документ вважається відправленим у місці, де зазвичай перебуває відправник, і вважається отриманим у місці, де зазвичай перебуває адресат. Дана норма фактично була запозичена та повністю відповідає положенням ст. 15 Типового закону ЮНСІТРАЛ "Про електронну комерцію". Аналогічні норми пропонується закріпити у законодавстві РФ, що відображено у законопроектах РФ "Про електронну торгівлю" та "Про правочини, що вчиняються за допомогою електронних засобів зв'язку (електронні правочини)".

Момент одержання електронного документа може бути встановлений так:

1) якщо адресат вказав інформаційну систему з метою одержання таких документів, одержання відбувається: а) в момент, коли електронний документ надходить до вказаної інформаційної системи; або б) якщо електронний документ направляється до інформаційної системи адресата, яка не є вказаною інформаційною системою, – в момент, коли електронний документ вилучається адресатом з даної системи;
2) якщо адресат не вказав інформаційну систему, одержання відбувається в момент, коли електронний документ надходить до якої-небудь інформаційної системи адресата.

У даному випадку розглядається ситуація, коли адресат у односторонньому порядку вказує конкретну інформаційну систему для одержання електронного документа, і електронний документ надходить до інформаційної системи адресата, яка не є вказаною системою. Одержання має місце в такій ситуації в той день, коли електронний документ вилучається адресатом з даної системи. Причому в даному випадку під "вказаною інформаційною системою" необхідно розуміти систему, яка була конкретно вказана стороною, наприклад у випадку, коли в оферті прямо зазначається адреса, на яку повинен бути направлений акцепт. Проста наявність адреси електронної пошти на бланку чи іншому документі не повинна розглядатися як пряма вказівка однієї або кількох інформаційних систем.

Окремо слід звернути увагу на поняття "надходження" до інформаційної системи, яке використовується як у зв'язку з відправленням, так і в зв'язку з одержанням електронного документа. Електронний документ надходить до інформаційної системи в той момент, коли з'являється можливість для його обробки в цій інформаційній системі, незалежно від того, чи є у адресата можливість для прочитання та використання електронного документа.

Таким чином, правове регулювання відносин щодо використання електронних документів безпосередньо пов'язано з

можливістю вчинення правочинів через мережі електрозв'язку та з врегулюванням у цілому електронної комерції як комплексного явища. З цією метою необхідно прийняти закон "Про електронну комерцію", який, зокрема, повинен містити положення, які б врегулювали всю сукупність питань, пов'язаних із використанням електронних документів для вчинення правочинів через мережі електрозв'язку.

Так, повинно бути передбачене визначення електронного документа, закріплення процедур визначення відправника електронного документа, а також збереження останніх буде сприяти стійкості договірних відносин між особами, які здійснюють електронну комерцію. Визначення понять оригіналу та копії електронного документа також буде сприяти розвитку електронної комерції в Україні, оскільки буде легальна можливість фіксувати на електронних носіях документи, щодо яких висувається законодавча вимога існування в оригіналі. Закріплення процедури підтвердження одержання електронних документів та встановлення порядку визначення часу та місця їх відправлення і одержання також буде сприяти розвитку електронної комерції, зокрема буде допомагати особам, які здійснюють електронну комерцію, у випадку судового захисту прав та законних інтересів.

Отже, використання електронних документів для укладання правочинів у сфері електронної комерції дозволяє в повному обсязі виконати загальні та спеціальні законодавчі вимоги, що висуваються до укладання господарських договорів.

Типовий закон ЮНСІТРАЛ "Про електронну комерцію" передбачає, що у сфері укладання договорів, якщо сторони не домовилися про інше, оферта та акцепт оферти можуть вчинятися з використанням електронних документів (ст. 11).

Аналогічну норму пропонує закріпити законопроект України "Про електронну торгівлю" та законопроекти РФ "Про електронну торгівлю" та "Про правочини, що вчиняються за допомогою електронних засобів (електронні правочини)". Зокрема передбачається, що договір може бути укладений шляхом обміну електронними документами, що дозволяють чітко встано-

вити, що документ виходить від сторони за договором; при укладанні договору оферта однієї зі сторін і її акцепт іншою стороною можуть бути відправлені й отримані у вигляді електронних документів.

Таким чином, для здійснення можливості вчиняти правочини через мережі електрозв'язку необхідно на рівні закону "Про електронну комерцію" закріпити правило про те, що оферта та акцепт оферти можуть здійснюватися з використанням електронних документів, якщо сторони не домовилися про інше. Тобто, у випадку, коли для укладання договору використовуються електронні документи, такий договір не може бути визнаний недійсним лише з тих підстав, що з цією метою використовувалися електронні документи.

Законодавче закріплення вказаного правила не переслідує мети встановити переважний правовий режим по відношенню до норм цивільного та господарського права, які стосуються укладання договорів. Його мета полягає у сприянні розвитку електронної комерції шляхом забезпечення більшої правової впевненості сторін у тому, що стосується використання електронних документів для укладання договорів.

Запровадження вказаного правила позитивно вирішує правову невизначеність у сфері можливості укладання договорів через мережі електрозв'язку, що пов'язано у чинному законодавстві України з тим фактом, що в ряді випадків електронний документ, який містить оферту та акцепт оферти, готується комп'ютерами без безпосереднього втручання людини, через що виникає сумнів щодо волевиявлення сторін, а також з тим фактом, що власне спосіб передачі електронного документа не вимагає наявності документа на паперовому носієві. Крім того, вказане правило дозволить передбачити, що оферта та акцепт оферти, як і будь-яке інше волевиявлення, можуть передаватися за допомогою будь-яких засобів, включаючи електронні документи.

Законодавче закріплення можливості здійснити оферту та акцепт оферти з використанням електронних документів тісно пов'язано і логічно продовжує правила, розглянуті у цьому розділі, а саме: неможливість позбавлення юридичної сили

оферти та акцепту оферти лише з тієї підстави, що вона представлена електронним документом, а отже, електронні документи, якими представлені оферта та акцепт оферти, повинні мати необхідну юридичну силу для використання їх в якості доказів для захисту в суді свого порушеного права.

Можливість використання електронного документа в якості оферти та акцепту оферти повинно включати не тільки випадки, коли і оферта, і акцепт вчиняються через мережі електрозв'язку, але й випадки, коли тільки оферта, або тільки акцепт вчинено через мережі електрозв'язку.

Необхідно звернути увагу на те, що правило про можливість використання електронного документа в якості оферти та акцепту оферти у сфері укладання господарських договорів повинно бути представлено диспозитивною нормою – якщо сторони не домовилися про інше. Зазначена обставина буде підкреслювати автономію сторін при укладанні правочинів та закріплювати неможливість нав'язування використання мереж електрозв'язку тим сторонам, які для укладання правочинів використовують документи на паперових носіях. Отже вказане правило не повинно тлумачитися як таке, що обмежує якимнебудь чином автономію сторін стосовно інших сторін, які не беруть участі у використанні мереж електрозв'язку для передачі документів на електронних носіях.

Окремо необхідно зазначити, що М.І. Брагінський ще у 1990 р. вказував, що в умовах, коли розширюється право підприємств та організацій на вибір контрагентів та на визначення за власною волею варіантів окремих договірних умов, безсумнівно підвищується значення договірно-правової техніки, з чим пов'язана необхідність запровадження комп'ютерної техніки до договірної практики [142, с. 91]. Розвиваючи цю думку, М.І. Брагінський посилається на Інструктивні вказівки Держарбітражу СРСР від 29 червня 1979 р. "Про використання в якості доказів по арбітражних справах документів, підготовлених за допомогою електронно-обчислювальної техніки" [185, с. 47], які передбачають, що всі такого роду документи, тобто підготовлені за допомогою електронної обчислювальної техні-

ки, повинні прийматися органами арбітражу на загальних підставах в якості письмових доказів, оскільки вони містять дані про обставини, що мають значення для справи. Необхідно особливо виділити ту частину інструктивних вказівок, в якій містилася наступна вимога: "При вирішенні питання, чи перебувають сторони у договірних відносинах, виходити з того, що угодою в письмовій формі, передбаченою ст. 44 ЦК РФСР, являється також укладена сторонами угода, коли її умови передані або фіксовані за допомогою засобів електронно-обчислювальної техніки".

Інший фахівець в галузі господарського права В.В. Луць передбачав, що великі перспективи для скорочення часу та трудових витрат на укладання договорів відкриваються в зв'язку із запровадженням до народного господарства автоматизованих систем управління [174, с. 35].

Таким чином, законодавство СРСР ще з 1979 р. не тільки вказувало на можливість та необхідність застосування сучасних на той період досягнень інформаційних технологій у сфері господарювання, зокрема при укладанні господарських договорів, а й закріплювало правило про те, що правочином у письмовій формі є і такий правочин, умови якого передані або зафіксовані за допомогою засобів електронно-обчислювальної техніки. Тобто необхідно продовжити практику запровадження інформаційних технологій до сфери господарювання з урахуванням її сучасних можливостей.

На підставі викладеного можна зробити висновок про те, що з метою усунення юридичних перепон на шляху розвитку електронної комерції та сприяння забезпеченню більшої правової впевненості сторін у тому, що стосується використання електронних документів для укладання договорів, необхідно внести зміни до ч. 2 ст. 638 ЦКУ "Укладання договору", додавши правило про те, що при укладанні договорів оферта та її акцепт можуть здійснюватися з використанням електронних документів, якщо сторони не домовилися про інше. Спеціальний закон "Про електронну комерцію" повинен містити положення про те, що договір у сфері електронної комерції може бути

укладений шляхом обміну електронними документами, підписаними електронними підписами уповноважених осіб; якщо при укладанні договору використовуються електронні документи, то такий договір не може бути визнаний неукладеним або таким, що не породжує передбачені в ньому правові наслідки, тільки з тих підстав, що він укладений шляхом обміну електронними документами.

Пропозиція суб'єкта правовідносин у сфері електронної комерції укласти договір (оферта), зроблена через мережі електрозв'язку, повинна містити всі істотні умови договору відповідно до чинного законодавства України, а також звичайні умови, передбачені законодавством України у сфері електронної комерції.

З визначення електронної комерції, запропонованого у розділі першому, вбачається, що вчинення правочинів шляхом обміну електронними документами, який здійснюється за допомогою використання мереж електрозв'язку, зокрема Інтернет, складає основний зміст електронної комерції. А тому визначення особливих істотних умов господарських договорів, що вчиняються у зазначений спосіб, набуває виключно важливого значення.

В юридичній літературі проблема додаткових особливих істотних умов договору, що вчиняється через мережі електрозв'язку, не досліджувалася. Аналіз законопроекту України від 17 лютого 2003 р. "Про електронну торгівлю" свідчить про неоднозначність питання визначення істотних умов договору, що вчиняється через мережі електрозв'язку[4]. А тому, вважаємо за необхідне почати з загальнотеоретичних начал про умови договору.

З точки зору умов, які формують договори в цілому та їх окремі види, доктрина цивільного права [186, с. 403, 187, с. 370–371, 188, с. 45, 189, с. 449, 190, с. 146, 191, с. 29–34] всі умови

[4] Аналіз законопроектів РФ "Про електронну торгівлю" та "Про правочини, що вчиняються за допомогою електронних засобів зв'язку (електронні правочини)", на взірець яких був розроблений законопроект України "Про електронну торгівлю", також говорить про наявність такого спірного підходу до визначення умов договору, який вчиняється через мережі електрозв'язку.

поділяє на істотні, звичайні та випадкові. Істотними є умови про предмет договору, умови, які визначені законом як істотні або є необхідними для договорів даного виду, а також усі ті умови, щодо яких за заявою хоча б однієї із сторін має бути досягнуто згоди (ч. 1 ст. 638 ЦКУ). Отже, істотними визнаються умови, які необхідні та достатні для того, щоб вважати договір укладеним та здатним породити права та обов'язки у його сторін [134, с. 295–296].

Частина 1 ст. 180 ГКУ передбачає, що зміст господарського договору становлять умови договору, визначені домовленістю його сторін, спрямованою на встановлення, зміну або припинення господарських зобов'язань, як погоджені сторонами, так і ті, що приймаються ними як обов'язкові умови договору відповідно до законодавства.

Отже, для того, щоб договір вважався укладеним, необхідно узгодити всі його істотні умови, які поділяються на три групи: а) умови, які визнані істотними в силу закону; б) умови, необхідні для договорів даного виду; в) умови, щодо яких за заявою однієї з сторін повинна бути досягнута згода (ч. 2 ст. 180 ГКУ).

Виходячи з цього, наочною стає спірність підходу розробників вищезгадуваного законопроекту України "Про електронну торгівлю" в частині визначення умов договору, що вчиняється через мережі електрозв'язку. Так, зазначений законопроект пропонує закріпити, що "Договір, в електронній торгівлі повинен містити наступні обов"язкові умови: 1) технологію (процедуру) укладання договору; 2) можливість і порядок внесення змін при узгодженні умов договору; 3) спосіб і порядок акцепту; 4) спосіб зберігання та пред'явлення електронних документів і умови електронного доступу до такої документації, а також умови надання паперових копій електронних документів."

Такий підхід викликає певні зауваження. По-перше, зазначений вище законопроект оперує поняттям обов'язкових умов, використання якого не відповідає ні чинному законодавству України, ні доктринам цивільного та господарського права. По-друге, зазначені умови не враховують того, що вже набрали чинності Закон України від 22 травня 2003 р. "Про ЕЦП" та Закон

України від 22 травня 2003 р. "Про електронний документ та електронний документообіг", які врегулювали ряд питань, які зазначений законопроект відносить до "обов'язкових умов" (відправлення та передавання електронних документів, їх одержання та зберігання тощо). По-третє, наведена вище редакція "обов'язкових умов" є не зовсім коректною та складною для застосування, а отже, буде породжувати численні труднощі на практиці[5]. По-четверте, наведені чотири умови є недостатніми для належного правового регулювання господарських договорів, що вчиняються через мережі електрозв'язку, оскільки неврегульованими залишаються питання про волевиявлення сторін на використання електронного підпису, зокрема ЕЦП,[6] а також питання про процедуру узгодження розбіжностей з приводу дійсності одержаних електронних документів.

Отже, на нашу думку, для з'ясування питання про додаткові особливі істотні умови господарських договорів, що вчиняються через мережі електрозв'язку, необхідно переглянути названі вище чотири умови таких договорів та виходити з особливого порядку їх укладання, пов'язаного з обміном електронними докумен-

[5] Незрозуміло викладено, чим саме відрізняється процедура від порядку укладання договору та в чому полягає їх особливість порівняно з загальним порядком укладання господарських договорів, регламентованим ст. 181 ГКУ. Також не коректно викладена умова про спосіб і порядок акцепту, оскільки не зрозуміло, мова йде про використання електронних документів для акцепту чи мається на увазі інший порядок акцепту, ніж він передбачений ЦКУ. Закон України "Про електронні документи та електронний документообіг" не передбачає кілька різних способів зберігання електронних документів, навпаки, ст. 13 вказаного Закону зобов'язує суб'єктів електронного документообігу зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

[6] Так, наприклад, законопроект РФ "Про правочини, що вчиняються за допомогою електронних засобів зв'язку (електронні правочини)" також оперує поняттям обов'язкових умов договору і окрім тих умов, що названі такими у законопроекті України "Про електронну торгівлю", називає ще: 1) технологію та процедуру використання аналогів власноручного підпису; 2) спосіб та порядок відклику можливого помилкового акцепту; 3) вказівки на умови, що включаються у договір шляхом відсилки до інших електронних документів, та порядок технічного доступу до відповідної відсилки.

тами через мережі електрозв'язку, зокрема через мережу Інтернет, і чинного на сьогоднішній день законодавства України.

Як уже зазначалося, особливість господарських договорів у сфері електронної комерції полягає у використанні електронних носіїв письмової форми, тобто у використанні електронних документів, в яких об'єктивується вчинений господарський договір.

У зв'язку з цим сукупність істотних умов, необхідних та достатніх для укладання того чи іншого господарського договору через мережі електрозв'язку, змінюється порівняно з господарськими договорами, що укладаються на паперових носіях. Ці зміни пов'язані з необхідністю узгодження сторонами використання електронних документів та електронних підписів для вчинення таких договорів. Тобто це додаткові умови, існування яких обумовлено використанням засобів електрозв'язку для вчинення господарських договорів, а саме використанням електронних документів та електронних підписів. З'ясування цих умов дозволить сторонам у майбутньому безспірно довести існування такого договору.

Саме ці умови якісно відокремлюють господарські договори, що вчиняються через мережі електрозв'язку (шляхом обміну електронними документами), від таких саме договорів, але які вчиняються на паперових носіях інформації.

Узгодження сторонами за договором умови про використання електронних документів необхідна в зв'язку з тим, що ні ЦКУ, ні ГКУ прямо не передбачають можливості сторін використовувати електронні документи для вчинення договорів. В той же час ст. 11 Типового закону ЮНСІТРАЛ "Про електронну комерцію" передбачає, що в контексті укладення договорів, якщо сторони не домовилися про інше, оферта та акцепт оферти можуть здійснюватися з використанням електронних документів. Тобто за Типовим законом використання електронних документів для вчинення договорів передбачено як загальне правило: це є правом особи, а тому її волевиявлення на реалізацію цього права має бути чітко сформульоване.

У зв'язку з тим, що 22 травня 2003 р. в Україні був прийнятий закон "Про електронні документи та електронний доку-

ментообіг", сторонам нема необхідності переписувати у договорі всі положення цього закону. Достатньо лише послатися у договорі на те, що правовідносини, які виникають при створенні та використанні електронних документів, регулюються відповідно до названого закону. В той же час сторони мають можливість в договорі узгодити ті питання, які у зазначеному законі врегульовані диспозитивною нормою.

Так, наприклад, електронний документ вважається одержаним адресатом з часу надходження відправнику повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між суб'єктами електронного документообігу (ст. 11 зазначеного закону). При цьому, якщо попередньою домовленістю між суб'єктами електронного документообігу не визначено порядок підтвердження факту одержання електронного документа, таке підтвердження може бути здійснено в будь-якому порядку автоматизованим чи іншим способом в електронній формі або у формі документа на папері (ч. 2 ст. 11 цього закону). Отже, контрагенти, узгоджуючи використання електронних документів для юридичного оформлення договірних відносин між собою, можуть домовитися про, наприклад, невикористання системи підтвердження одержання електронних документів, або обрати певний спосіб підтвердження одержання електронних документів.

Окремо необхідно звернути увагу на те, що доцільно в межах угоди сторін про використання електронних документів визначити порядок узгодження розбіжностей з приводу дійсності одержаних електронних документів. Слід зауважити, що така практика в Україні вже почала складатися, про що свідчить досвід договірної роботи окремих суб'єктів господарювання (ПП Адграфікс-Україна Україна, м. Хмельницький) [5]. Необхідність визначення порядку узгодження розбіжностей щодо дійсності одержаних електронних документів пов'язана з тим, що її відсутність зробить об'єктивно неможливим довести у суді існування такого договору. Крім того, згадуваний вище Закон України

"Про електронний документ та електронний документообіг" не передбачає такої процедури.

Про обґрунтованість такого підходу свідчить судова практика РФ. Так, Вищий арбітражний суд РФ у своєму листі від 19 серпня 1994 р. № С1-7/оп-578 зазначив: "Якщо між сторонами виник спір про наявність договору та інших документів, підписаних цифровим (електронним) підписом, арбітражний суд повинен запитати у сторін виписку з договору, в якій вказана процедура порядку узгодження розбіжностей, на якій стороні лежить обов'язок доведення тих чи інших фактів та достовірності підпису. З врахуванням цієї процедури арбітражний суд перевіряє достовірність наданих сторонами доказів. За необхідності арбітражний суд має право призначити експертизу по спірному питанню, використовуючи при цьому передбачену договором процедуру. У випадку відсутності у такому договорі процедури узгодження розбіжностей та порядку доведення достовірності договору та інших документів, а одна з сторін оспорює наявність підписаного договору та інших документів, арбітражний суд має право не приймати в якості доказів документи, підписані електронним (цифровим) підписом".

Отже, контрагенти укладаючи господарський договір через мережі електрозв'язку, повинні узгодити використання сторонами електронних документів, в межах чого вони повинні передбачити наступну процедуру узгодження розбіжностей щодо дійсності електронних документів, підписаних ЕЦП.

У випадку виникнення розбіжностей між сторонами з приводу дійсності електронних документів, підписаних ЕЦП, застосовується процедура узгодження розбіжностей, передбачена угодою сторін. Доведення розбіжностей покладається на сторону, яка заявила про порушення її прав і законних інтересів.

Якщо одна із сторін стверджує, що електронний документ, підписаний її ЕЦП, є дійсним, а друга сторона цей підпис не визнає, створюється комісія з узгодження з рівною кількістю представників від обох сторін. Повноваження членів комісії з узгодження підтверджуються дорученням.

Комісії з узгодження надаються такі матеріали: сторона, яка наполягає на недостовірності ЦП, надає такий підпис на дискеті у вигляді файлу; сторони надають власні екземпляри програмного забезпечення для перевірки ЕЦП; контрольні та робочі екземпляри відкритих ключів, які зберігаються у сторін.

Для перевірки електронного документа з ЕЦП, що оспорюється, комісія з узгодження виконує такі дії: порівнює відкриті ключі, надані сторонами, із зразками, які передаються у вигляді паперового документа, завіреного підписами і печатками сторін; порівнює екземпляри програмного забезпечення, які використовуються для перевірки ЕЦП. Для запобігання різночитання при подальшій перевірці, комісія з узгодження використовує програмне забезпечення, отримане безпосередньо від розробника; перевіряє достовірність ЕЦП під оспорюваним електронним документом, використовуючи програму, надану розробником, з використанням відкритого ключа, достовірність якого вже встановлено.

Висновки роботи комісії з узгодження відображаються в акті, що підписується усіма членами комісії. Члени комісії з узгодження, які не погоджуються з висновками більшості, підписують акти із зауваженнями, які додаються до нього.

Підпис визнається недійсним або дійсним в залежності від результатів перевірки. Комісія з узгодження робить висновок про вину сторін в причинах виникнення розбіжностей. Рішення комісії з узгодження сторони визнають для себе обов'язковим.

Акт комісії з узгодження є підставою для висування претензій до сторони, винної в порушенні інтересів іншої сторони. Акт комісії з узгодження є доказом у випадку вирішення конфлікту у суді.

Порядок визначення дійсності електронного документа і ЕЦП, встановлений угодою сторін, обов'язковий для комісії з узгодження.

У випадку ухилення однієї із сторін від створення комісії з узгодження друга сторона має право самостійно призначити трьох незалежних експертів для того, щоб зробити висновки з питання дійсності оспорюваного ЕЦП. Висновок експертів обов'язковий для сторін.

Витрати на проведення процедури узгодження покладаються на сторону, що заявила про порушення її прав і законних інтересів. У випадку визнання вимог сторони, яка заявила про порушення її прав та інтересів правомірними, сторона, винна у порушені прав, повинна на протязі 5 (п'яти) днів від дня складення акту комісії з узгодження або винесення висновків експертами відшкодувати їй усі витрати, пов'язані з проведенням процедури узгодження.

Підсумовуючи викладене, необхідно зазначити, що першою істотною умовою господарського договору, що укладається через мережі електрозв'язку, є угода сторін про використання електронних документів з процедурою вирішення розбіжностей щодо дійсності електронних документів, підписаних ЕЦП.

Другою істотною умовою такого договору є угода про обрання певного виду електронного підпису.

Типовий закон ЮНСІТРАЛ "Про електронну комерцію" закріплює такий принцип електронної комерції як відкритість або технологічний нейтралітет, який має гарантувати відсутність переваг тільки одному виду технології. Тобто Типовий закон в контексті електронної комерції дозволяє використовувати будь-які види електронного підпису за умови, що вони використовуються на підставі узгодженого волевиявлення сторін, є надійними та такими, що відповідають меті, для якої електронний документ створюється і використовується.

Отже, сторони повинні чітко визначити, який саме вид електронного підпису вони обрали: електронний цифровий підпис або інший вид електронного підпису. Наявність такої угоди сторін має виключно важливе значення і в той же час не створює для контрагентів зайвих клопотів. Так, якщо сторони обрали використання ЕЦП, то в договорі достатньо лише зазначити це, оскільки регулювання відносин, пов'язаних із використанням ЕЦП, відбувається на підставі Закону України від 22 травня 2003 р. "Про електронний цифровий підпис".

Дещо складніше буде складатися ситуація, коли сторони вирішать використовувати інший вид електронного підпису. Зазначений вище Закон України від 22 травня 2003 р. "Про

електронний цифровий підпис" в преамбулі зазначає, що його дія не поширюється на відносини, що виникають під час використання інших видів електронного підпису. А тому угода сторін про використання такого підпису повинна включати:

- правовий режим електронного підпису, а саме, що обраний вид електронного підпису за правовим режимом прирівнюється до власноручного підпису за умови, що такий підпис використовується на підставі узгодженого волевиявлення сторін, є надійним та таким, що відповідає меті, для якої електронний документ створюється і використовується;
- призначення електронного підпису, а саме в якій сфері правовідносин сторони погоджуються використовувати цей вид електронного підпису;
- особливості застосування, а саме порядок накладання та перевірки електронного підпису; розподіл ризиків збитків, які можуть бути завдані сторонам або третім особам; сторона, на якій лежить обов'язок доведення достовірності електронного підпису.

Узгодження сторонами зазначених умов є необхідним та достатнім для визнання використаного електронного підпису рівнозначним власноручному підпису, а отже при оспорюванні договору, підписаного таким електронним підписом, дозволить довести волевиявлення сторони на укладання відповідного договору.

Необхідно зазначити, що окремі суб'єкти господарювання вже сьогодні при укладанні договору на обслуговування за системою "Клієнт–Банк" узгоджують зазначену умову про використання певного виду електронного підпису. Так, ВАТ "Кредитпромбанк"[144] укладаючи з клієнтом такий договір, обумовлює, що у системі "Клієнт – Банк" використовуються електронні цифрові ключі для накладення ЕЦП першої особи, електронні цифрові ключі для накладення ЕЦП другої особи і електронний цифровий ключ адміністратора. Система "Клієнт – Банк" для кожної посадової особи клієнта генерує пару електронних цифрових ключів, особистий (таємний) ключ і відкритий ключ. Ці електронні цифрові ключі є унікальними. Особистий (таємний) ключ

використовується в системі "Клієнт – Банк" для накладання ЕЦП, який, в свою чергу, використовується для ідентифікації особи, що накладає ЕЦП, і підтвердження цілісності електронного документа, що передається в банк. Відкритий цифровий ключ відправляється в банк для сертифікації і використовується в банку для перевірки ЕЦП посадової особи клієнта на електронних розрахункових документах. Сертифікація електронних цифрових ключів клієнта в банку проводиться на підставі письмової заяви клієнта з власноручним підписом посадової особи – власника електронного цифрового ключа.

На підставі викладеного можна зробити висновок про те, що сторони, укладаючи господарський договір шляхом обміну електронними документами через мережі електрозв'язку, зокрема через мережу Інтернет, повинні узгодити використання електронних документів для вчинення таких господарських договорів та обраний ними вид електронного підпису. Невиконання цього правила призведе до неможливості контрагентів у випадку невиконання чи неналежного виконання обов'язків довести існування такого договору, підтвердити свої права та обов'язки, що випливають з договору, а отже, і захистити їх.

Закріплення вказаної імперативної вимоги дозволить передбачити в законодавстві і санкцію за порушення такої вимоги – визнання договору неукладеним (ч. 8 ст. 181 ГКУ). В цій частині справедлива точка зору Рабинович Н.В., який розмежовуючи підстави недійсних правочинів та правочинів, які не відбулися, вказав, що недійсний правочин – це правочин, який відбувся, але через притаманні йому недоліки визнається позбавленим юридичної сили; правочин, що не відбувся, ніколи не існував, й існувати не може, через що правової сили не має, тому позбавлений її бути не може [192, с. 21].

Отже, доцільно закріпити в законі України "Про електронну комерцію" норму такого змісту: "Умови договору, що укладається у сфері електронної комерції, визначаються матеріальним правом, яке до нього застосовується, та повинні обов'язково містити наступні додаткові істотні умови: угоду сторін про використання електронних документів та угоду

сторін про обраний вид електронного підпису. У разі, якщо сторони не досягли згоди з цих умов договору, такий договір вважається неукладеним".

2.3. Правовий статус інформаційних посередників

Запропоноване у першому розділі визначення електронної комерції в Україні як системи взаємопов'язаних правовідносин у сфері вчинення правочинів шляхом обміну електронними документами, який здійснюється за допомогою використання мереж електрозв'язку, зокрема Інтернет, дозволяє розглядати інформаційних посередників, як осіб, що забезпечують відправлення, одержання або зберігання електронних документів, як одного з суб'єктів електронної комерції.

Надання інформаційними посередниками послуг, які забезпечують механізми, що дозволяють пошук, доступ та отримання інформації; послуг, що складаються з передачі інформації через мережу зв'язку, надання доступу до мережі зв'язку чи послуг по розміщенню інформації, що надається одержувачем послуг, відправлення електронних документів за допомогою електронної пошти – створює фізичну можливість здійснення електронної комерції.

Розглянемо ті аспекти діяльності інформаційних посередників, які безпосередньо пов'язані із вчиненням господарських правочинів через мережі електрозв'язку, тобто відносини між відправником та адресатом електронного документа. В той же час істотного значення в контексті даної роботи набуває роль інформаційних посередників у сфері передачі електронних документів.

Директива Ради ЄС від 8 червня 2000 р. "Про деякі правові аспекти послуг інформаційного суспільства, в тому числі електронної комерції, на внутрішньому ринку" розглядає інформаційних посередників в контексті правового регулювання вчи-

нення правочинів через мережі електрозв'язку, акцентуючи увагу на їх відповідальності за передачу та зберігання електронних документів (ст. 12–14 Директиви).

Законопроект України "Про електронну торгівлю", як і законопроекти РФ "Про електронну торгівлю" та "Про правочини, що вчиняються за допомогою електронних засобів зв'язку (електронні правочини)", також розглядають інформаційного посередника як суб'єкта електронної комерції, який надає послуги особам, що здійснюють електронну комерцію, з метою обміну та збереження електронних документів. Послуги інформаційних посередників полягають у передачі електронних документів мережами електрозв'язку, а також наданні особам, що здійснюють електронну комерцію, доступу до мережі електрозв'язку, зокрема Інтернет.

У цілому вищезгадані Європейська Директива та законопроекти одностайно вказують на такі основні функції інформаційних посередників в контексті передачі електронних документів, як: одержання, передача, зберігання електронних документів від імені іншої особи. Інформаційні посередники можуть також надавати інші послуги, наприклад, форматування, переклад, підтвердження і збереження електронних документів, тощо. Термін "інформаційний посередник" використовується не як родове поняття, а стосовно кожного окремого електронного документа, а звідси випливає, що одна й та ж особа може одночасно виступати відправником або адресатом одного електронного документа та інформаційним посередником відносно іншого електронного документа.

Виходячи із вказаних основних функцій інформаційних посередників, можна говорити про їх відповідальність у трьох випадках: у разі надання суб'єктам електронної комерції послуг доступу до мережі електрозв'язку; тимчасового зберігання електронного документа з метою його передачі; тривалого зберігання електронного документа з метою його передачі.

У випадку, коли послуга інформаційного посередника полягає у наданні суб'єктам електронної комерції доступу до мереж електрозв'язку, він не повинен нести відповідальності за інформацію, що ним передається, за умови, що інформаційний посередник:

- не починає передачу інформації;
- не обирає адресата інформації, що ним передається;
- не обирає та не змінює змісту інформації, яка міститься у електронному документі, що ним передається.

Надання інформаційним посередником вказаної послуги означає автоматичне та транзитне зберігання інформації, що передається, протягом часу, коли зберігання здійснюється виключно з метою передачі інформації мережею електрозв'язку, та за умови, що інформація не зберігається довше, ніж це розумно необхідно для передачі інформації.

У випадку, коли послуга інформаційного посередника полягає у передачі мережею електрозв'язку інформації, що міститься в електронному документі, наданому відправником, інформаційний посередник не повинен нести відповідальності за тимчасове зберігання такої інформації, що здійснюється з виключною метою підвищення ефективності подальшої передачі інформації адресату, за умови, що інформаційний посередник [193]:

- не змінює змісту інформації, яка міститься у електронному документі, що ним передається;
- дотримує умови доступу до такої інформації;
- вилучає інформацію, що зберігається, або припиняє доступ до неї, при одержанні дійсних відомостей про факт вилучення інформації із мережі електрозв'язку у початковому джерелі її передачі, або доступ до неї припинений, або суд чи інший адміністративний орган прийняли рішення про таке вилучення чи припинення доступу.

У випадку, коли послуга інформаційного посередника полягає у тривалому зберіганні інформації, що міститься у електронному документі, наданому відправником, інформаційний посередник не повинен нести відповідальності за інформацію, що зберігається ним за умови, що:

- інформаційний посередник не володів дійсними відомостями про незаконний характер діяльності чи інформації та не попереджений про факти та обставини, виходячи з яких стає наочним незаконний характер діяльності чи інформації; або

- ♦ інформаційний посередник при одержанні таких дійсних відомостей або попередження негайно вилучає інформацію або припиняє доступ до неї.
- ♦ не обирає та не змінює змісту інформації, яка міститься у електронному документі, що ним передається.

У вищезгаданих законопроектах України та РФ передбачено також, що інформаційний посередник не зобов'язаний контролювати та перевіряти законність електронних документів, що передаються та зберігаються, за виключенням випадків, передбачених законодавством.

Аналогічна норма міститься й у ст. 15 Директиви ЄС від 8 червня 2000 р. "Відсутність загального обов'язку моніторингу". В той же час ч. 2 цієї статті передбачає, що інформаційні посередники можуть бути зобов'язаними своєчасно інформувати уповноважені державні органи про заплановану незаконну діяльність чи інформацію, що надається адресату чи відправнику. Запровадження аналогічної норми до законодавства України буде сприяти укріпленню правопорядку не тільки у сфері електронної комерції, а взагалі в країні.

Законопроект України "Про електронну торгівлю" цілком справедливо вказує на такий обов'язок інформаційного посередника, як обов'язок розкривати інформацію, яку він передає чи зберігає, за вимогою органів прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України у випадках порушення кримінальної справи.

Закріплення такого правила не позбавляє можливості суд чи інший уповноважений орган відповідно до норм чинного законодавства України та норм ст. 34 Конституції України[7] вимагати від інформаційного посередника припинення або запобігання правопорушенню.

Таким чином, правове регулювання відносин щодо вчинення правочинів через мережі електрозв'язку, що здійснюється

[7] Стаття 34 Конституції в частинах 2–3 передбачає, що кожен має право вільно збирати, зберігати, використовувати та поширювати інформацію усно, письмово або в інший спосіб на свій вибір.

шляхом обміну електронними документами, неможливе без визначення міри відповідальності інформаційних посередників, що надають послуги з передачі електронних документів та послуги доступу до мережі електрозв'язку, зокрема Інтернет.

Доцільним є запровадження не тільки обов'язку інформаційних посередників надавати за вимогою уповноважених державних органів певну інформацію, а й обов'язку повідомляти ці органи про здійснювану чи плановану незаконну діяльність чи поширювану інформацію.

Окремо необхідно звернути увагу на таку послугу, що надається інформаційним посередником, як послуга доступу до мереж електрозв'язку, зокрема до мережі Інтернет. Надання доступу до мережі Інтернет здійснюється на підставі договору, який у юридичній літературі називають договором Інтернет-провайдінгу [118]. Господарська діяльність інформаційного посередника в частині надання доступу до мереж електрозв'язку, в тому числі до мережі Інтернет, має виключно важливе значення як для суб'єктів правовідносин у сфері електронної комерції, так і для держави в цілому, яка зацікавлена у впорядкуванні функціонування мереж електрозв'язку, формуванні умов забезпечення інформаційної безпеки держави та контролі за розвитком інформаційних мереж в Україні. Вказані обставини вимагають державного регулювання зазначених відносин, що відбувається за допомогою ліцензування.

У законодавстві ряду держав світу, як правило, передбачено ліцензування діяльності, пов'язаної з наданням послуг доступу до мереж електрозв'язку, зокрема Інтернет. Так, Закон РФ від 16 лютого 1995 р. "Про зв'язок" [194, с. 423], визначаючи мережі електрозв'язку як технологічні системи, що забезпечують один чи декілька видів передач: телефонну, телеграфну, передачу даних та інших видів документальних повідомлень, включаючи обмін інформацією між ЕОМ тощо, у ст. 15 "Ліцензування діяльності в галузі зв'язку" передбачає ліцензування діяльності фізичних та юридичних осіб, пов'язаної з наданням послуг зв'язку.

Закон України від 16 травня 1995 р. "Про зв'язок" з наступними змінами та доповненнями в ст. 24 передбачає, що

діяльність юридичних і фізичних осіб в галузі зв'язку здійснюється за ліцензією згідно з чинним законодавством про підприємництво. Електричний зв'язок даним законом визначається як передача, випромінювання або прийом знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах.

Оскільки наведене визначення електричного зв'язку не змінювалося з часу прийняття даного закону, воно застаріле і не враховує розвитку сучасних технологій зв'язку. Відсутність у наведеному визначенні вказівки на те, що поняття електричного зв'язку охоплює, зокрема, обмін інформацією між ЕОМ, призвело до того, що надання послуг доступу до такої мережі електрозв'язку як Інтернет випадає з видів діяльності, що підлягають ліцензуванню.

Закон України "Про телекомунікації" передбачає, що здійснення господарської діяльності у галузі телекомунікацій[8] відбувається на підставі ліцензії. Так, ліцензуванню підлягають послуги передавання даних, що надаються з використанням мереж телекомунікацій загального користування[9], за винятком мереж Інтернет. Останнє запропоноване положення закону є некоректним, оскільки єдиною різницею між мережею телекомунікацій загального користування та мережею Інтернет є глобальність, величезна розгалуженість останньої.

Таким чином, доцільним є уточнення поняття електричного зв'язку та мереж електрозв'язку з тим, щоб визначення цих понять чітко вказували на охоплення ними глобальної мережі Інтернет та, таким чином, передбачали запровадження ліцензування доступу до всіх мереж загального користування, в тому числі до мережі Інтернет.

[8] Законопроект пропонує визначати телекомунікації (електрозв'язок) як передавання та приймання електромагнітних сигналів, що є носіями інформації, із застосуванням проводових, радіо, оптичних чи інших електромагнітних систем.
[9] Законопроект пропонує визначати мережі телекомунікацій загального користування як мережі телекомунікацій, відкриті для одержання телекомунікаційних послуг будь-яким користувачам.

Розглянемо докладніше схему діяльності інформаційних посередників у частині надання послуг доступу до мереж електрозв'язку в Україні. Зв'язок є однією з пріоритетних галузей України та покликаний задовольняти потреби користувачів, органів державної влади та місцевого самоврядування, оборони та безпеки держави в засобах та послугах зв'язку. Існують такі види зв'язку: електричний, поштовий, спеціальний та фельд'єгерський (ст.ст. 1, 26 Закону України "Про зв'язок").

Правова основа господарської діяльності у сфері зв'язку представлена нормативними актами господарського законодавства, а саме: ГК України, законом "Про захист економічної конкуренції" та іншими, а також іншими нормативними актами, що регулюють відносини у сфері зв'язку, зокрема законом України "Про зв'язок" від 16 травня 1995 р.

Господарська діяльність у сфері зв'язку здійснюється багатьма суб'єктами господарювання різних форм власності та організаційно-правових форм, серед яких Закон України "Про зв'язок" виділяє підприємства (оператори) зв'язку. До них відносяться підприємства, які здійснюють свою господарську діяльність для забезпечення функціонування засобів, споруд та мереж зв'язку з метою надання послуг зв'язку як продукту діяльності з прийому, обробки, передачі та доставки поштових відправлень або повідомлень електрозв'язку. Серед основних операторів електричного зв'язку особливе місце займає ВАТ "Укртелеком".

Указом Президента від 22 квітня 1998 р. "Про деякі заходи захисту інтересів держави в інформаційній сфері" [195] встановлено, що з метою впорядкування функціонування мереж передачі даних, формування умов забезпечення інформаційної безпеки держави та контролю за розвитком інформаційних мереж та мереж передачі даних в Україні вихід у закордонні мережі передачі даних здійснюється лише через мережі підприємств (операторів) "Укртелеком", "Укркосмос" та "Інфоком".

Державне управління господарської діяльності у сфері зв'язку здійснюється за допомогою таких важелів: ліцензування, тарифікація, стандартизація та сертифікація. Відповідно до Закону України "Про ліцензування певних видів господарської

діяльності" від 1 червня 2000 р. ліцензуванню підлягають, зокрема, такі види господарської діяльності, як надання послуг радіозв'язку (з використанням радіочастот) та надання послуг телефонного зв'язку (крім відомчих об'єктів) (п. 47, 48 ст. 9).

Ліцензування діяльності у сфері зв'язку введено з метою здійснення єдиної державної політики у цій сфері та захисту прав споживачів, координації діяльності різних підприємств у сфері створення та розвитку мереж, систем та служб зв'язку для забезпечення їх взаємодії між собою та з мережами загального користування, сприяння демонополізації діяльності у сфері зв'язку, розвитку підприємництва та конкуренції, забезпечення високого рівня якості послуг зв'язку.

Для реалізації своєї діяльності інформаційні посередники укладають з підприємствами зв'язку договори про оренду каналів зв'язку, оскільки створювати власну мережу зв'язку, прокладати нові оптоволоконні кабелі тощо є для інформаційних посередників недоцільним та дуже дорогим кроком. Тобто фізично доступ до мережі Інтернет здійснюється через існуючу систему електричного зв'язку (кабелі, радіочастоти тощо).

Для того, щоб на підставі укладеного договору Інтернет-провайдингу права та обов'язки контрагентів за цим договором регулювалися законодавством України, інформаційний посередник повинен бути "прив'язаний" до правового режиму Української держави. Фізична прив'язка здійснюється шляхом легалізації відповідного суб'єкта, тобто шляхом державної реєстрації як суб'єкта господарювання. Згадаємо, що послуга доступу до мереж електрозв'язку дає суб'єктам електронної комерції фізичну можливість використання інших послуг інформаційного посередника, наприклад, відправлення, одержання та зберігання електронних документів тощо, що здійснюється саме в інформаційній мережі Інтернет, а тому український сегмент Інтернет повинен бути ідентифікований саме як український, а не якої-небудь іншої країни. Така прив'язка відбувається шляхом одержання інформаційними посередниками спеціального дозволу (ліцензії) на здійснення діяльності, пов'язаної з наданням послуг зв'язку

(доступу) до мережі Інтернет, чого чинним законодавством нашої країни ще не передбачено.

Запровадження ліцензування нового виду господарської діяльності ніяким чином не протирічить Концепції розвитку державної системи ліцензування підприємницької діяльності за її видами, затвердженої Постановою Кабінету Міністрів України від 23 вересня 1996 р. № 1164 [196]. Згадаємо, що ліцензування підприємницької діяльності за її видами є складовою частиною державного регулювання підприємництва України, спрямованим на забезпечення єдиної державної політики у цій сфері та захист економічних і соціальних інтересів громадян. Запровадження ліцензування здійснюється на підставі Конституції України щодо права кожного на здійснення підприємницької діяльності, яка не заборонена законом. Концепція встановлює, що регулюванню повинні підлягати лише ті види підприємницької діяльності, які безпосередньо впливають на здоров'я людини, навколишнє середовище та безпеку держави. Діяльність, пов'язана з наданням послуг доступу до мереж електрозв'язку безпосередньо стосується інформаційної безпеки держави. Саме з цих підстав у країнах, де вже існує компетентний правопорядок регулювання діяльності, пов'язаної з використанням мережі Інтернет, встановлено ліцензування діяльності, пов'язаної з наданням доступу до неї.

Таким чином, запровадження в Україні ліцензування послуг доступу до мереж електрозв'язку загального користування, зокрема мережі Інтернет, що надаються інформаційними посередниками, дозволить забезпечити здійснення єдиної державної політики у цій сфері, координацію діяльності різних підприємств у сфері електронної комерції, розвиток підприємництва та конкуренції, високий рівень якості послуг.

Отже, правове регулювання відносин у сфері електронної комерції в Україні має ґрунтуватися на законі "Про електронну комерцію", який повинен закріпити права і обов'язки осіб, що здійснюють електронну торгівлю, визначити правила виконання правочинів з використанням електронних документів, а

також визнати електронні документи як допустимі судові докази. З цією метою такий закон повинен закріпити наступні положення.

Правочини та інші юридичні дії суб'єктів господарювання можуть вчинятися через мережі електрозв'язку, зокрема через мережу Інтернет, з дотриманням вимог цього закону та інших нормативних правових актів України.

Господарські договори не можуть бути визнані недійсними лише з тих підстав, що вони вчинені через мережі електрозв'язку. Винятки з цього правила можуть бути встановлені лише законом.

У сфері вчинення господарських правочинів через мережі електрозв'язку, якщо сторони не домовилися про інше, оферта та акцепт оферти можуть вчинятися з використанням електронних документів.

Законодавче закріплення повинен одержати перелік особливих додаткових істотних умов, з'ясування яких є обов'язковим для укладання правочинів через мережі електрозв'язку.

Господарський договір, вчинений через мережі електрозв'язку, вважається таким, що вчинений у простій письмовій формі.

Використання ЕЦП, а також інших видів електронного підпису в порядку, передбаченому законодавством України та (або) домовленістю сторін, юридично рівнозначне власноручному підпису уповноваженої особи.

У законі повинно бути детерміновано, за яких умов електронний документ вважається електронним документом відправника, а також законодавчо врегульоване питання представлення та зберігання оригіналів електронних документів (порядок ведення журналів обміну електронними документами).

Окремо в законі доцільно зазначити обов'язковість підтвердження адресатом одержання електронного документа, а також форму та спосіб, в які таке підтвердження може бути зроблено.

Повинні бути врегульовані також питання, пов'язані з визначенням моменту та місця відправлення й одержання електронного документа.

Вимагає законодавчого закріплення й положення про можливість осіб, що здійснюють електронну комерцію, використовувати послуги інформаційного посередника з метою зберігання електронних документів та надання інших послуг. Також повинні бути врегульовані питання про умови, за яких інформаційний посередник не несе відповідальності за зміст електронних документів, які ним передаються або зберігаються, та випадки, коли інформаційні посередники можуть бути зобов'язаними своєчасно інформувати уповноважені державні органи про заплановану незаконну діяльність чи інформацію, що надаються адресату чи відправнику.

Статтю 9 Закону України від 1 червня 2000 р. "Про ліцензування певних видів господарської діяльності" доповнити пунктом: "Ліцензуванню підлягає надання послуг передавання даних, що надаються з використанням мереж телекомунікацій загального користування, в тому числі мереж Інтернет".

РОЗДІЛ 3

Використання електронних підписів в електронній комерції

3.1. Поняття та правовий режим ЕЦП

У розділі 1 вже зверталася увага на природний тісний зв'язок між ЕЦП, електронними документами та електронною комерцією, в зв'язку з чим суспільство висуває до держави високі вимоги щодо захисту прав та законних інтересів учасників правовідносин у сфері використання електронного цифрового підпису.

При розробленні законодавства, призначеного для регулювання електронної комерції, особлива увага повинна приділятися нормам, присвяченим застосуванню ЕЦП. Довіра до електронного цифрового підпису та його правове визнання є обов'язковим для вчинення юридично значущих дій за допомогою мереж електрозв'язку, зокрема мережі Інтернет, а тому актуальним є питання визначення поняття ЕЦП.

У багатьох державах світу поняття електронного цифрового підпису вже знайшло законодавче закріплення. Так, прийнятий на 16 пленарному засіданні Міжпарламентської Асамблеї країн-учасниць СНД (постанова № 16-10) від 9 грудня 2000 р. модельний закон "Про електронний цифровий підпис" визначає електронний цифровий підпис як електронні дані, одержані внаслідок перетворення вихідних електронних даних з використанням закритого ключа підпису, які за допомогою відповідної процедури з використанням відкритого ключа підпису дозволяють: а) підтвердити незмінність вихідних даних після підписання їх електронним цифровим підписом; б) встановити, що електронний цифровий підпис створений з використанням закритого ключа, відповідає відкритому; в) встановити володільця реєстраційного свідоцтва на відкритий ключ електронного цифрового підпису за наявності такого свідоцтва.

Одним з поширених на європейському рівні актів у цій сфері є Директива Європейського парламенту та Ради 1999/93/ЄС від 13 грудня 1999 р. "Про правові підстави Співдружності для використання електронних підписів", яка створює правові підстави використання електронних підписів. Стаття 2 Директиви визначає вдосконалений електронний підпис як електронний підпис, що відповідає таким вимогам: а) унікально пов'язаний з особою, яка підписує; б) достатній для її ідентифікації; в) створюється з використанням засобів, які перебувають під виключним контролем особи, яка підписала; г) пов'язаний з даними, до яких він відноситься, таким чином, що наступні зміни даних стають наочними.

Закон Російської Федерації від 10 січня 2002 р. "Про електронний цифровий підпис" використовує поняття ЕЦП, яке визначає як реквізит електронного документа, призначений для захисту електронного документа від підробки, одержаний в результаті криптографічного перетворення інформації з використанням закритого ключа електронного цифрового підпису та який дозволяє ідентифікувати володільця сертифіката ключа підпису, а також встановити відсутність виправлення інформації в електронному документі.

Закон Республіки Бєларусь від 10 січня 2000 р. "Про електронний документ" дає дещо інше визначення ЕЦП, під яким розуміється набір символів, який одержується за допомогою засобів електронного цифрового підпису, та є невід'ємною частиною електронного документа. Причому засоби електронного цифрового підпису пропонують розуміти як програмні та технічні засоби, які забезпечують вироблення та перевірку електронного цифрового підпису та мають сертифікат відповідності або посвідчення про визнання сертифіката, який видається в національній системі сертифікації Республіки Бєларусь.

Наведені визначення об'єднує те, що всі вони містять вказівку на технічний та юридичний аспекти поняття "ЕЦП". Так, узагальнюючи досвід зазначених держав, можна стверджувати, що ЕЦП з технічної точки зору ґрунтуються на асиметричній криптографії (закритий та відкритий ключі). Юридичний ас-

пект наведених визначень ЕЦП розкривається через такі категорії, як функція ЕЦП, спосіб легалізації, сфера використання ЕЦП, юридичний статус ЕЦП:

1) щодо функції ЕЦП, то в більшості поширених визначень функція електронного цифрового підпису вбачається у визначенні володільця ключа підпису, встановленні істинності даних та захисті електронного документа від підробки;
2) відносно способу легалізації ЕЦП, то, як правило, у наведених визначеннях зазначається, що легалізація електронного цифрового підпису відбувається через видачу сертифікуючим центром (реєстраційним центром) або державною установою сертифіката (або реєстраційного свідоцтва) на відкритий ключ підпису;
3) сферою використання ЕЦП визначаються перш за все контракти чи інші документи, які логічно пов'язуються з контрактом;
4) юридичний статус ЕЦП з точки зору багатьох визначень полягає в тому, що він є офіційним підписом відправника електронного документа.

У законодавстві України до травня 2003 р. єдиного підходу до визначення ЕЦП не було. Так, першим нормативним актом в Україні, який закріпив поняття цифрового підпису, стала Концепція створення Єдиної державної автоматизованої паспортної системи, затверджена Постановою Кабінету Міністрів України від 20 січня 1997 р. № 40 [197]. Цифровий підпис відповідно до цього акта визначається як відомості, що додаються до блоку даних або отримані в результаті його криптографічного перетворення, які дають змогу адресату пересвідчитися в цілісності блоку даних і достовірності їх джерела.

Наступним кроком стало затвердження Постановою Національного банку України від 27 грудня 1999 р. Інструкції "Про міжбанківські розрахунки в Україні" № 621. Згідно з Інструкцією ЕЦП визначається як сукупність даних, отримана за допомогою криптографічного перетворення вмісту електронного документа, яка дає змогу підтвердити його цілісність та ідентифікувати особу, яка його підписала.

Через рік поняття ЕЦП було вже закріплене на рівні закону, а саме в Законі України від 5 квітня 2001 р. "Про платіжні системи та переказ грошей в Україні". Вперше на законодавчому рівні в Україні закріплене поняття ЕЦП, під яким розуміють сукупність даних, отриману за допомогою криптографічного перетворення вмісту електронного документа, яка дає змогу підтвердити його цілісність та ідентифікувати особу, яка його підписала. Тобто це визначення дослівно повторює визначення, наведене у Інструкції НБУ. Зазначимо відразу, що всі наведені вітчизняні акти, які містять визначення ЕЦП, є вузькоспеціалізованими, дозволяють використовувати ЕЦП лише при здійсненні міжбанківських розрахунків, для функціонування платіжних систем в Україні, для створення Єдиної державної автоматизованої паспортної системи. В інших відносинах за цими актами можливість застосування ЕЦП не передбачається. Із визначення, що міститься у вказаному законі України, виділимо ознаки ЕЦП:

1) ЕЦП одержується шляхом криптографічного перетворення вмісту електронного документа;
2) ЕЦП підтверджує цілісність електронного документа;
3) за допомогою ЕЦП відбувається ідентифікація особи, яка підписала електронний документ.

ЦК України відреагував на сучасні технології у сфері комунікацій та закріпив у ст. 207, присвяченій письмовій формі правочину, положення про те, що при вчиненні правочину в письмовій формі воля сторін може виражатися за допомогою, зокрема, електронного та іншого технічного засобу зв'язку. Таке положення є дійсно прогресивним, оскільки воно закріплює існуючу можливість укладання правочинів через мережі електрозв'язку.

Але та ж сама стаття допускає використання ЕЦП при вчиненні правочинів лише у випадках, передбачених законом, іншими правовими актами або домовленістю сторін. Так, зокрема зазначається, що "використання при вчиненні правочинів... електронного цифрового підпису допускається у випадках, встановлених законом, іншими актами цивільного законодавства, або за письмовою згодою сторін, у якій мають міститися зразки відповідного аналога їхніх власноручних підписів". Таким чином, використання ЕЦП законом

розглядається як виключення із загального правила. З цього випливає, що право на використання ЕЦП для вчинення правочинів через мережі електрозв'язку повинно зазначатися у спеціальному законі, присвяченому регулюванню того чи іншого кола правовідносин, що буде негативно відбиватися на практиці укладання таких правочинів, буде їх штучно стримувати.

Зазначене положення ЦК України протирічить Типовому закону ЮНСІТРАЛ "Про електронну комерцію", оскільки вказаний закон передбачає загальнодозвільне правило щодо вчинення правочинів через мережі електрозв'язку (шляхом обміну електронними документами), виключення з якого встановлюються законом. Обов'язковим реквізитом правочину, що вчиняється через мережу електрозв'язку, являється електронний підпис, зокрема ЕЦП. Таким чином, з'являється колізія, коли за загально дозвільним правилом правочини через мережі електрозв'язку вчиняти можна, а підписувати їх за допомогою, наприклад ЕЦП, заборонено, оскільки це прямо не передбачено законом.

Таким чином, ЦКУ містить базові норми, які дають можливість вчиняти правочини через мережі електрозв'язку, використовуючи, відповідно, електронні носії об'єктивування письмової форми.

Закон України від 22 травня 2003 р. "Про електронний цифровий підпис" у ст. 1 визначає ЕЦП як вид електронного підпису[1], 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. Недоліком даного визначення є його завантаженість технічними термінами.

Слід також згадати окремі визначення ЕЦП, які зустрічаються у науковій доктрині. Так, Є.А. Суханов визначає ЕЦП як самостійний аналог власноручного підпису поряд з аналогом, одержаним в результаті факсимільного відтворення підпису за допомогою засобів механічного чи іншого копіювання [150, с. 349].

[1] Вказаний закон визначає електронний підпис як дані в електронній формі, які додаються до інших даних або логічно з ними пов'язані та призначені для ідентифікації підписувача електронного документа.

Наведене визначення цілком справедливо вказує на таку ознаку ЕЦП, як самостійність від інших аналогів власноручного підпису, але цієї однієї ознаки замало для визначення поняття ЕЦП, що поєднує в собі як технічні, так і юридичні аспекти.

М.М. Дутов визначає ЕЦП як електроні дані, отримані внаслідок перетворення початкових електронних даних з використанням особистого ключа, який за допомогою відкритого ключа дозволяє: підтвердити незмінність початкових електронних даних після підписання їх ЕЦП; встановити, що ЕЦП створений з використанням особистого ключа, який відповідає відкритому; встановити власника сертифіката відкритого ключа ЕЦП [93, с. 8]. Вказане визначення, з одного боку, намагається охопити як технічні, так й юридичні аспекти ЕЦП, а з іншого боку, використовує не тільки забагато технічної термінології, а й використовує поняття, які не використовуються системою законодавства України для регулювання електронної комерції (електронні дані, початкові електронні дані), що ще більше ускладнює сприйняття запропонованого визначення.

Якщо проаналізувати вказані вище найбільш поширені визначення ЕЦП, які зустрічаються у чинних нормативних актах України та в юридичній літературі, то можна зазначити, що всі визначення, як й у інших країнах світу, містять технічні та юридичні аспекти цього поняття. Тому доцільно розглянути ЕЦП у цих двох аспектах: технічному та юридичному, що дозволить більш ретельно визначитися з таким новим для юридичної літератури поняттям, як ЕЦП.

Отже, якщо взяти будь-яке існуюче в юридичній літературі визначення ЕЦП, то в ньому обов'язково будуть відомості про технічний бік цього питання[2]. Необхідність розгляду технічно-

[2] ЕЦП – це цифрове представлення будь-якої інформації, яка сприймається ЕОМ; електронний підпис це електронне позначення, символ або прийом; цифровий підпис визначається як печатка, яка створена за допомогою приватного ключа; з технічної точки зору ЕЦП є набором символів (послідовністю чисел); такі дані приєднані або логічно пов'язані з іншими електронними даними. Спосіб одержання ЕЦП – криптографічне перетворення інформації з використанням закритого ключа електронного цифрового підпису.

го аспекту електронного цифрового підпису пов'язана з тим, що існують деякі методи підтвердження оригінальності електронних документів, які не використовують асиметричну криптосистему, наприклад, переведені у цифрове зображення рукописного підпису тощо. З технічної точки зору використання ЕЦП ґрунтується на двох основних інструментах: шифруванні з відкритим ключем та хеш-коді документа[3].

Юридичний аспект наведених визначень ЕЦП розкривається через такі категорії, як функція ЕЦП, спосіб легалізації, сфера використання ЕЦП, юридичний статус ЕЦП.

Виходячи з наведеного, можна запропонувати визначення ЕЦП як виду електронного підпису, представленого у формі електронних даних, одержаних шляхом криптографічного перетворення інформації, який дозволяє ідентифікувати володільця сертифіката ключа підпису та встановити істинність електронного документа, відкритий ключ якого має чинний на момент використання сертифікат.

Спираючись на визначення ЕЦП, прослідкуємо розвиток законодавства в зарубіжних державах та міжнародного права у цій сфері, який йде шляхом гармонізації, вироблення єдиних принципів з метою створення універсальної правової інфраструктури ЕЦП в електронній комерції [199].

Необхідно зазначити, що в світі існує два підходи до регулювання відносин, пов'язаних з використанням електронного підпису: прийняття окремого нормативного акта в цій сфері або

[3] Власне електронний цифровий підпис несе в собі інформацію про його автора, зашифровану за допомогою закритого (приватного) ключа. Це дає можливість володільцю відкритого ключа переконатися в тому, що автором повідомлення є та особа, від імені якої воно надійшло. Поряд з цим існує технічна можливість включити в склад ЕЦП дані, які характеризують саме повідомлення, щоб виключити можливість внесення до нього змін в процесі передачі (аутентифікація повідомлення). Сучасній математиці відомі спеціальні функції, які не мають властивості зворотності. Вони дозволяють з однієї послідовності чисел (з одного повідомлення) одержати іншу послідовність (інше повідомлення) таким чином, що зворотнє перетворення неможливе. Такі функції, що використовуються в криптографії, називаються хеш-функціями.

включення норм, що регулюють дані правовідносини, до нормативних актів у сфері телекомунікацій чи електронної комерції.

Так, серед країн, що прийняли окремі нормативні акти, які врегулювали використання ЕЦП, можна назвати: Італію, Ізраїль, Словенію, Російську Федерацію, США, Україну, Естонію тощо.

Гармонізація законодавства у сфері регулювання відносин, пов'язаних з використанням ЕЦП, яскраво вбачається в таких актах, як Директива ЄС від 13 грудня 1999 р. "Про правові підстави для використання електронних підписів", Типовий закон ЮНСІТРАЛ "Про електронні підписи", Модельний Закон Міжпарламентської асамблеї країн–учасниць СНД від 9 грудня 2000 р. "Про електронний цифровий підпис".

В Україні 22 травня 2003 р. був прийнятий спеціальний закон "Про електронний цифровий підпис", який набрав чинності з 1 січня 2004 р. Даний закон визначає правовий статус ЕЦП та регулює відносини, що виникають при використанні ЕЦП. Прийняття даного закону забезпечило базові умови для застосування ЕЦП, що дозволить:

1) дотримуватися правових норм, що містять вимоги до письмової форми документа і його оригіналу;
2) зберегти всі традиційні функції підпису, у тому числі: посвідчення повноважень сторони, що підписала; встановлення особи, що підписала, і змісту повідомлення; роль підпису в якості судового доказу;
3) визнати ЕЦП достовірним, а також точно встановити наявну або відсутню підробку чи фальсифікацію електронного документа;
4) надати юридичні гарантії безпеки передачі інформації через мережі загального користування;
5) визнати засоби створення ЕЦП надійними;
6) забезпечити охорону персональної інформації.

У той же час вказаний закон містить ряд спірних положень, що стосуються, перш за все, функціонування системи провайдерів сертифікаційних послуг (центри сертифікації ключів, акредитовані центри сертифікації ключів, засвідчувальний центр) та їх акредитації у випадках, передбачених даним законом.

У законодавчих актах вищезгаданих держав світу передбачено, що вони встановлюють правові умови використання в електронних документах саме такого виду електронного підпису, як електронний цифровий підпис, що пов'язано з його особливою надійністю [200], при дотриманні яких ЕЦП в електронному документі визнається рівнозначним власноручному підпису на документі на паперовому носієві. При цьому передбачається, що дія таких законодавчих актів не поширюється на відносини, які виникають при використанні інших видів електронного підпису.

Типовий закон ЮНСІТРАЛ "Про електронні підписи" спробував взагалі не прив'язуватися до того чи іншого виду електронного підпису. Так, у Типовому законі зазначається, що не дозволяється обмеження або позбавлення юридичної сили будь-якого методу створення електронного підпису, якщо такий підпис є настільки надійним, що відповідає меті, для якої документ на електронному носії був підготовлений або переданий, включаючи всі відповідні домовленості (ч. 1 ст. 6). Тобто обраний електронний підпис повинен бути надійним та відповідати тим правовідносинам, для реалізації яких він застосовується (відповідати меті електронного документа). Така позиція Типового закону пов'язана з його призначенням – спроба гармонізації та уніфікації правового регулювання у даній сфері, усунення правових перепон на шляху залучення новітніх інформаційних технологій до господарської сфери. Зазначений підхід був повністю сприйнятий Австралією, Республікою Філіппіни та іншими країнами світу [201].

Аналогічну позицію займає й Директива ЄС від 13 грудня 1999 р. "Про правові підстави для використання електронних підписів", але намагаючись полегшити використання електронних підписів та сприяючи їх правовому визнанню, Директива, дозволяючи використання всіх можливих електронних підписів, основну увагу приділяє правовому регулюванню використання саме вдосконаленого електронного підпису, який за своїм змістом є все тим же електронним цифровим підписом (ґрунтується на асиметричній криптографії (закритий та відкри-

тий ключі)). Такий підхід теж був запозичений рядом країн світу, зокрема Австрією [35, sec. 2 § 3].

Закон України "Про електронний цифровий підпис" у ч. 1 ст. 3 передбачає, що ЕЦП за правовим статусом прирівнюється до власноручного підпису, якщо: ЕЦП підтверджено за допомогою посиленого сертифіката; а також якщо на час перевірки використовувався посилений сертифікат ключа, чинний на момент накладання ЕЦП. Отже, створюється ситуація, коли законодавець, з одного боку, дозволяє використовувати ЕЦП із звичайним сертифікатом, або взагалі ЕЦП без сертифіката (ст. 5), а з іншого – передбачає, що лише ЕЦП з посиленим сертифікатом прирівнюється до власноручного підпису.

Частина 2 ст. 3 зазначеного закону України передбачає, що електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа. В той же час закон ні в цій нормі, ні у нормах інших статей не передбачає, що електронний підпис за правовим статус прирівнюється до власноручного підпису. Таким чином, фактично законодавець виключає можливість використання будь-якого виду електронного підпису, окрім ЕЦП з посиленим сертифікатом, а тому у зазначеному законі України відсутні критерії, дотримання яких є достатнім для прирівнювання електронного підпису до власноручного підпису особи. Таке положення йде в розріз з принципами електронної комерції, зокрема з принципом відкритості та технологічного нейтралітету.

Більш послідовно до вирішення цього питання підійшли автори законопроекту України "Про електронну торгівлю", передбачивши, що електронний підпис за своїм статусом має юридичну силу власноручного підпису. Тобто, при укладанні договорів особи самостійно обирають вид електронного підпису, що його будуть застосовувати, і самостійно несуть будь-які ризики, пов'язані з правовими наслідками підписання та виконання правочинів з використанням обраного електронного підпису [202].

Вимоги, що висуваються до електронного підпису, за вказаним законопроектом окреслені не коректно. Так, передба-

чається, що електронний підпис в електронній торгівлі повинен забезпечувати: 1) неможливість з боку підписувача відмовитися від підписаного електронного документа; 2) неможливість підроблення електронного підпису – тільки особа, яка володіє ключем підпису, могла підписати цей електронний документ; 3) неможливість внесення будь-яких змін в підписаний документ, які можуть бути виявлені шляхом перевірки підпису; 4) можливість будь-кому, хто має зразок підпису у вигляді сертифіката ключа, перевірити оригінальність, справжність, цілісність підписаного документа.

Таким чином, диспозиція такої норми передбачає, що всі ці вимоги повинні бути дотримані електронним підписом, що застосовується в електронній комерції. При цьому лише перша та третя вимоги стосуються всіх електронних підписів, а друга та четверта вимоги стосуються такого виду електронного підпису, як ЕЦП, що пов'язано з використанням асиметричної криптографії (відкритий та закритий ключі) в його основі. Отже, вимогами, що висуваються до електронних підписів з метою визнання їх за юридичним статусом рівнозначними власноручному підпису, являються неможливість підписувача відмовитися від підписаного електронного документа та неможливість внесення змін до такого документа.

Типовий закон ЮНСІТРАЛ "Про електронну комерцію" (ст. 7), закон Австралії "Про електронні правочини" (ст. 10) вказують на більш широке розуміння критеріїв, що висуваються з цією ж метою. Зокрема передбачається, що електронний підпис повинен бути як надійним, так і таким, що відповідає меті, з якою такий електронний документ був створений. Отже, метод, який особа обирає для задоволення вимоги щодо підпису, повинен ідентифікувати особу, а також вказувати її згоду зі змістом електронного документа, а не тільки вказувати на неможливість підписувача відмовитися від нього. При встановленні особистості певної особи електронний підпис не обов'язково повинен бути унікальним ідентифікатором. Замість цього він повинен достатньо ідентифікувати особу для цілей цього електронного документа. Окремі види електронного підпису

(ЕЦП) будуть у зв'язку з принципом своєї дії також перевіряти цілісність електронного документа. Але норми вказаних законів вимагають лише того, щоб електронний підпис давав особі можливість вказати, що вона згодна із інформацією, що міститься в документі, – при цьому вказані норми не вимагають, щоб електронний підпис перевіряв цілісність електронного документа. Згода особи з інформацією в електронному документі означає демонстрацію наміру застосувати свій підпис до інформації, що міститься в електронному документі.

Вимогу надійності електронного підпису для цілей, з якими був створений електронний документ, доцільно встановлювати з врахуванням усіх відповідних обставин на момент використання певного виду електронного підпису. Розвиток технології може означати, що певний вид електронного підпису перестає бути прийнятним, навіть якщо раніше він вважався прийнятним для вчинення певного правочину. Прив'язка такої вимоги до часу, коли був використаний певний вид електронного підпису, необхідна для того, щоб вид електронного підпису, який був прийнятний на момент його використання, пізніше не був визнаний неприйнятним. Встановлення базових вимог щодо електронних підписів замість того, щоб встановлювати деталізовані стандарти для окремих видів електронного підпису, відповідає принципу технологічного нейтралітету та встановлює можливість того, що види електронного підпису будуть відповідати об'єктивним стандартам, які будуть прийнятними на той час, коли вони будуть використовуватися.

При визначенні прийнятності виду електронного підпису до уваги можуть братися ряд факторів, які можуть включати: тип правочину, можливість та складність відповідної комунікаційної системи та значення і важливість інформації, що міститься в електронному документі. Така вимога означає, що для різних видів правочинів необхідні різні рівні безпеки. Вона дозволяє обрати такий вид електронного підпису, який забезпечує прийнятний рівень безпеки до даного правочину.

Отже для законодавства повинна бути неприйнятною практика приписування використання або надання законодавчих

переваг певним видам електронного підпису, наприклад ЕЦП. Більш прийнятна практика, коли ринок самостійно оцінює прийнятність певних видів електронного підпису для окремих цілей замість того, щоб у законодавчому порядку встановлювати прийнятні технології [203, 204].

Таким чином, при регулюванні відносин у сфері використання електронних підписів раціональним є законодавче закріплення норми, яка дозволяє особам, що здійснюють електронну комерцію, використовувати будь-які види електронного підпису за умови, що вони використовуються на підставі узгодженого волевиявлення сторін, є надійними та такими, що відповідають меті, з якою електронний документ створюється і використовується.

В той же час чинне законодавство України вже містить ретельно описану процедуру створення та використання такого виду електронного підпису, як ЕЦП, оскільки цей вид електронного підпису на сьогодні є найбільш надійним та таким, який у максимальному ступені може захищати інтереси та безпеку суспільства й держави. Водночас повинна бути усунена пряма законодавча вимога використовувати саме цей вид електронного підпису (ст. 3 Закону України "Про електронний цифровий підпис").

Необхідно звернути увагу на те, що правило про можливість використання будь-якого виду електронного підпису, а не тільки ЕЦП у сфері укладання господарських договорів через мережі електрозв'язку, повинно бути представлено саме диспозитивною нормою. Зазначена обставина буде підкреслювати автономію сторін при укладенні правочинів і призначена для того, щоб закріпити неможливість нав'язування використання того чи іншого виду електронного підпису. Отже закріплення такої норми не буде обмежувати яким-небудь чином автономію сторін при обранні певного виду електронного підпису для надання юридичної сили електронним документам.

Таким чином, прийняття зазначеної вище моделі правового регулювання створить необхідні та достатні правові умови використання електронних підписів у сфері електронної ко-

мерції в Україні, а саме: якщо сторони домовилися використовувати не ЕЦП, а будь-який інший надійний вид електронного підпису, то такі правовідносини будуть регулюватися як загальною нормою, що дозволяє використовувати будь-які види електронного підпису, а також відповідними положеннями договору, що встановлюють процедуру використання такого виду підпису (взірцем такої процедури можуть виступати, наприклад, положення Типового ЮНСІТРАЛ "Про електронні підписи"), при цьому законодавство про електронні цифрові підписи на такі електронні підписи не буде поширюватися; якщо сторони домовилися використовувати у своїх відносинах електронний цифровий підпис, то такі правовідносини будуть регулюватися як загальною нормою, що дозволяє використовувати будь-які види електронного підпису, спеціальним законодавством, що встановлює компетентний правопорядок регулювання відносин у сфері ЕЦП, а також відповідними положеннями договору, якщо диспозитивні норми спеціального законодавства надають сторонам таку можливість.

Законодавчого закріплення можливості суб'єктів правовідносин у сфері електронної комерції використовувати будь-які види електронного підпису недостатньо для того, щоб вимога наявності на електронному документі електронного підпису була виконаною. Уніфіковане законодавство [20, ст. 5, 18, ст. 6, 32, с. 2] та законодавство ряду країн світу [37, ст. 4] в цій частині передбачають ряд справедливих вимог, дотримання яких дає підстави визнавати ЕЦП рівнозначним власноручному підпису. Причому зміст таких вимог у зазначених нормативних актах не відрізняється і по суті є однаковим.

Вимоги, дотримання яких дає підстави визнавати ЕЦП рівнозначним власноручному підпису, полягають в наступному:

1) сертифікат ключа підпису повинен бути дійсним на момент підписання електронного документа;
2) ЕЦП повинен пройти перевірку на оригінальність (дійсність) за допомогою відкритого ключа ЕЦП, який повинен мати відповідний сертифікат провайдера сертифікаційних послуг;

3) особа, яка підписала електронний документ за допомогою ЕЦП, повинна правомірно володіти закритим ключем, який використовується для створення ЕЦП;
4) ЕЦП повинен використовуватися відповідно до відомостей, зазначених у сертифікаті ключа підпису.

Легалізація ЕЦП відбувається через видачу провайдером сертифікаційних послуг сертифіката на відкритий ключ підпису, який підтверджує дійсність ЕЦП та ідентифікує володільця сертифіката ключа підпису [205]. Провайдери сертифікаційних послуг зобов'язані вести загально доступний реєстр сертифікатів ключів підписів, які видаються ними. Зацікавлена особа може звернутися, зокрема через мережу електрозв'язку, до відповідного провайдера сертифікаційних послуг та перевірити, чи дійсно даний сертифікат виданий певній особі, на яких умовах, та перевірити чинність такого сертифіката.

Одна з основних презумпцій, на якій ґрунтується використання ЕЦП, це те, що особа зобов'язана зберігати свій закритий ключ ЕЦП у таємниці, а відповідно негайно вимагати від провайдера сертифікаційних послуг призупиняти дію сертифіката ключа підпису, якщо вона має достатні підстави вважати, що таємниця закритого ключа ЕЦП порушена (ст. 7 Закону України "Про електронний цифровий підпис"). Таким чином, закріплюється презумпція, що закритий ключ ЕЦП перебуває у законного власника, якщо інше не встановлено у передбаченому законом порядку. Власник закритого ключа ЕЦП має право передавати повноваження на підписання електронного документа за допомогою його ЕЦП уповноваженому представнику в порядку, передбаченому чинним законодавством України.

У більшості чинних актів, присвячених правовому регулюванню відносин у сфері використання ЕЦП [8, ст. 8–9, 32, ст. 7, 20, ст. 2, 37, ст. 6], закріплюються вимоги до сертифікатів, а також перелік обов'язкових відомостей, які повинні в ньому міститися., зокрема: найменування та реквізити провайдера сертифікаційних послуг, який видав сертифікат; унікальний реєстраційний номер сертифіката; основні реквізити особи-підписувача; дату і час початку та закінчення строку чинності

сертифіката; відкритий ключ; найменування криптографічного алгоритму, що використовується власником особистого ключа; інформацію про обмеження використання підпису.

За згодою провайдера сертифікаційних послуг особа-заявник у письмовій формі може просити про включення до сертифіката додаткових відомостей, які не входять до кола обов'язкових, зокрема, кваліфікації, посади (з вказівкою найменування та місця знаходження організації, в якій встановлена така посада), інших відомостей. Ці та інші відомості підтверджуються наданням відповідних документів.

Закон України "Про електронний цифровий підпис" безпосередньо не вказує, скільки ЕЦП може мати особа. Звідси випливає, що особа може мати будь-яку кількість електронних цифрових підписів та, відповідно, будь-яку кількість сертифікатів відкритого ключа ЕЦП. Єдина умова, яка при цьому повинна бути виконаною, це створення єдиної бази даних сертифікатів ключів підписів, які повинні видаватися провайдерами сертифікаційних послуг України. Запровадження такої бази даних унеможливить вчинення протиправних дій з використанням ЕЦП, особливо у сфері розрахункових правовідносин.

Таким чином, правове регулювання електронної комерції в Україні, зокрема блоку відносин щодо використання ЕЦП, повинно ґрунтуватися на можливості осіб, що здійснюють електронну комерцію, використовувати будь-які види електронного підпису, зокрема ЕЦП, за умови, що вони використовуються на підставі узгодженого волевиявлення сторін, є надійними та такими, що відповідають меті, для якої електронний документ створюється і використовується.

Особа, що здійснює електронну комерцію, повинна мати право володіти будь-якою кількістю ЕЦП чи інших видів електронного підпису.

Визначення правового режиму ЕЦП невід'ємно пов'язане з питанням засобів електронного цифрового підпису, з яких генерується ЕЦП, і від яких залежить надійність функціонування ЕЦП. Розглядаючи питання про засоби електронного цифрового підпису, доцільним буде почати з визначення самого

поняття "засоби ЕЦП". Існуючі в юридичній літературі та чинному законодавстві окремих держав визначення цього поняття не дуже відрізняються одне від одного. Основна різниця полягає в ступені деталізації технічних питань поняття засобів ЕЦП. Визначення засобів ЕЦП наводилося у розділі першому посібника відповідно до якого це програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів та/або перевірки ЕЦП.

Незважаючи на те, що саме поняття засобів ЕЦП є сугубо технічним поняттям, жоден нормативний акт, присвячений регулювання використання ЕЦП, не залишає його поза увагою. Це пов'язано з тим, що від алгоритмів, на підставі яких діють засоби ЕЦП, залежить надійність та стійкість самого ЕЦП.

Таку позицію займає і Закон України "Про електронний цифровий підпис", який передбачає, що акредитований центр сертифікації виконує всі обов'язки та вимоги, встановлені законодавством для центру сертифікації, та додатково зобов'язаний використовувати для надання послуг ЕЦП надійні засоби ЕЦП (ч. 3 ст. 9). Тобто акредитований центр сертифікації, обслуговуючи сертифікати відкритих ключів ЕЦП, повинен використовувати надійні засоби ЕЦП.

Поняття надійних засобів передбачено вказаним законом України в ст. 1 та визначено як засіб ЕЦП, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються у порядку, визначеному законодавством.

Таким чином, засоби електронного цифрового підпису, з яких генерується власне ЕЦП, повинні бути сертифіковані або мати позитивний висновок державної експертизи.

Сертифікація – це один із ефективних методів, який широко застосовується у світовій практиці і дозволяє на основі випробування продукції в спеціалізованих лабораторіях (центрах) забезпечити захист прав споживача шляхом одержання ним достовірної та об'єктивної інформації про її властивості, харак-

теристики й відповідності стандартам. Вона стимулює виготовлювача задовольняти вимоги споживача і ринку до якості продукції і підвищувати організаційно-технічний рівень виробництва, що, в свою чергу, незмінно сприятиме створенню умов для випуску конкурентоспроможної продукції і розширенню ринку збуту її за кордоном.

Указом Президента України від 22 травня 1998 р. № 505/98 було затверджено Положення "Про порядок здійснення криптографічного захисту інформації в Україні", п. 6 якого передбачає, що "з метою визначення рівня захищеності від несанкціонованого доступу до інформації з обмеженим доступом проводяться сертифікаційні випробування криптосистем і засобів криптографічного захисту інформації".

Загальні правові та організаційні засади підтвердження відповідності продукції, систем якості встановлені законом України "Про підтвердження відповідності" [206], який спрямований на забезпечення єдиної державної технічної політики у сфері підтвердження відповідності.

Особливості сертифікації такого виду продукції, як засоби криптографічного захисту інформації (КЗІ), передбачені "Порядком проведення сертифікації засобів криптографічного захисту інформації" (далі – Порядок) від 15 грудня 1999 р., затвердженого Комітетом України з питань стандартизації, метрології та сертифікації.

Згідно з вказаним Порядком здійснення сертифікації засобів криптографічного захисту інформації в Україні покладено виключно на орган із сертифікації засобів криптографічного захисту інформації, який підпорядкований і діє в складі СБУ.

Частина 4 Порядку передбачає, що проведення сертифікації засобів КЗІ включає: подання заявки підприємствами, організаціями та установами щодо сертифікації засобів КЗІ і розгляд її органом із сертифікації засобів криптографічного захисту інформації; аналіз наданої документації; прийняття рішення за заявкою із зазначенням схеми (моделі) сертифікації засобів КЗІ; обстеження виробництва або атестація виробництва засобів КЗІ, що сертифікуються (при необхідності); відбір, ідентифіка-

ція зразків засобів КЗІ; сертифікаційні випробування; аналіз отриманих результатів та прийняття рішення про можливість видачі сертифіката відповідності; видача сертифіката відповідності та занесення сертифікованих засобів КЗІ до Реєстру системи; технічний нагляд за сертифікованими засобами КЗІ під час їх виробництва; інформування про результати робіт із сертифікації засобів КЗІ. Кожен з етапів проведення сертифікації засобів КЗІ детально регламентований Порядком.

Серед недоліків зазначеного Порядку необхідно назвати те, що він не містить чітко визначеного обсягу повноважень самого органу із сертифікації засобів КЗІ. В цій частині Російська Федерація поступила більш послідовно, передбачивши у Положенні "Про сертифікацію засобів захисту інформації" [207] повноваження федерального органу із сертифікації засобів КЗІ, які включають: створення системи сертифікації; вибір способу підтвердження відповідності засобів захисту інформації вимогам нормативних документів; закріплення правил акредитації центральних органів систем сертифікації (даний орган створюється за необхідності та очолює систему сертифікації однорідної продукції), органів сертифікації засобів захисту інформації (органи, що проводять сертифікацію певного виду продукції) та випробувальних лабораторій (проводять окремі етапи сертифікаційних випробувань певного виду продукції); встановлення правил акредитації центральних органів систем сертифікації, органів з сертифікації засобів захисту інформації та випробувальних лабораторій; визначення центрального органу для кожної системи сертифікації; ведення державного реєстру учасників сертифікації та сертифікованих засобів захисту інформації; здійснення державного нагляду та контролю за дотриманням учасниками сертифікації правил сертифікації та за сертифікованими засобами захисту інформації, а також встановлення порядку інспекційного контролю; розгляд апеляцій з питань сертифікації; визначення порядку визнання іноземних сертифікатів; призупинення або скасування дії виданих сертифікатів.

Можна вважати за доцільне передбачити аналогічні за змістом повноваження органу із сертифікації засобів КЗІ у вказаному вище Порядку.

Порядок проведення державної експертизи у галузі КЗІ встановлений Положенням "Про державну експертизу у сфері криптографічного захисту інформації", затвердженим Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 25 грудня 2000 р. № 62. Державна експертиза у сфері криптографічного захисту інформації являє собою діяльність, метою якої є підготовка висновків і надання рекомендацій для прийняття рішення про використання (застосування) об'єктів експертизи та яка включає перевірку відповідності об'єктів експертизи вимогам нормативних документів, оцінку рівня захисту інформації об'єктами експертизи або науково-технічного рівня об'єктів експертизи.

Таким чином, в Україні створені необхідні правові умови, які дозволяють відповідно до чинного законодавства встановити надійність того чи іншого засобу ЕЦП за допомогою проходження сертифікації засобів ЕЦП або одержання позитивного висновку державної експертизи у цій сфері.

З технічної точки зору засоби ЕЦП відносяться до криптографічних засобів захисту інформації [208]. Основне призначення засобів ЕЦП – це обслуговування ЕЦП (створення, перевірка), таким чином, юридично значущий ЕЦП може бути створений лише на ґрунті таких засобів, які відповідають встановленим щодо них вимогам чинного законодавства.

Таким чином, підставою розгляду діяльності з криптографічного захисту інформації в контексті засобів ЕЦП є те, що відповідно до визначень ЕЦП у Законі України від 22 травня 2003 р. "Про електронний цифровий підпис" в основі технології ЕЦП лежить певне криптографічне перетворення; засоби ЕЦП повинні мати сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації (ст.1). Виходячи з цього, не можна погодитися з висновком М.М. Дутова [93, с. 7] про те, що ЕЦП не відноситься до засобів криптографічного захисту інформації.

Державну політику у сфері криптографічного захисту інформації реалізовує Департамент спеціальних телекомунікаційних

систем та захисту інформації Служби Безпеки України (далі – Департамент), який діє на підставі Положення "Про Департамент спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України", затвердженого Указом Президента від 6 жовтня 2000 р. № 1120/2000, і згідно з яким Департамент є органом державного управління, який діє у складі Служби Безпеки України та їй підпорядковується. Слід зазначити, що деякі автори цілком справедливо зазначають, що державну політику у сфері криптографічного захисту інформації, зокрема щодо сертифікації засобів ЕЦП, повинен проводити Державний Комітет України по стандартизації, метрології і сертифікації, а не Департамент [93, с.11, 209, с. 19-29].

Обґрунтовуючи свою позицію, М.М. Дутов вказує, що "участь спецслужб у даній сфері комерційних відносин представляється не зовсім коректною, що може призвести до монополізації перспективного ринку електронної комерції. Єдиним випадком, коли таке втручання може бути припустимим – це встановлення стандартів використання засобів ЕЦП у сфері, що стосується державної таємниці або конфіденційної інформації, яка є власністю держави". Автор також посилається на те, що в Україні діє ряд державних стандартів в галузі криптографічного захисту інформації [210, 211], а тому виникає питання, чому перевірку відповідності засобів ЕЦП даним стандартам повинен проводити Департамент, а не Держстандарт України. Причому в самому Департаменті сертифікаційні роботи провадяться Органом по сертифікації засобів криптографічного захисту інформації, який був створений спільним наказом СБУ та Держстандарту. Вказаний автор називає такий крок половинчастим, та вказує, що "Держстандарт повинен займатися вирішенням питань відповідності конкретних засобів ДОСТу, виняток складе криптографічний захист інформації у відносинах з державними органами та захист інформації, яка складає державну таємницю".

Відповідної до п. 14 ст. 9 Закону України «Про ліцензування певних видів господарської діяльності», з урахуванням вимог законів України «Про інформацію», «Про державну таємницю», Положення "Про порядок здійснення криптографічного

захисту інформації в Україні, затвердженого Указом Президента України від 22 травня 1998 р. №505, Постанови Кабінету Міністрів України від 14 листопада 2000 р. "Про затвердження переліку органів ліцензування" № 1698 Наказом Державного комітету України з питань регуляторної політики та підприємництва, Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 29 грудня 2000 р. № 88/66 були затверджені "Ліцензійні умови провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівлі криптосистемами і засобами криптографічного захисту інформації" (далі – Ліцензійні умови).

Зазначені Ліцензійні умови визначають організаційні, кваліфікаційні, технологічні та інші вимоги до суб'єктів господарювання, виконання яких є обов'язковою умовою провадження певних робіт і надання послуг у межах господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівлі криптосистемами і засобами криптографічного захисту інформації (далі – господарська діяльність у галузі КЗІ). Дія Ліцензійних умов поширюється на суб'єктів господарювання, які здійснюють господарську діяльність у галузі КЗІ. Ліцензування господарської діяльності у галузі КЗІ здійснює Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ.

Таким чином, суб'єкти господарювання, які здійснюють господарську діяльність у галузі КЗІ, одержують у встановленому законодавствам порядку в Департаменті відповідну ліцензію. Департамент не тільки видає ліцензію, контролює виконання суб'єктами ліцензійних умов, а й здійснює контрольно-наглядові функції за діяльністю суб'єктів, які займаються вказаними вище видами господарської діяльності. Отже, у компетенції

Департаменту поєднані повноваження і на ліцензування, і контрольно-наглядові повноваження. Таке поєднання є позитивним моментом, оскільки це не тільки економить державні кошти, а, головним чином, робить прозорим та зручним в реалізації на практиці державної стратегії розвитку засобів криптографічного захисту інформації.

Порядок проведення розробки, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів КЗІ, надання послуг у галузі КЗІ, торгівлі криптосистемами і засобами КЗІ, визначається окремими нормативно-правовими актами та є обов'язковим до виконання всіма суб'єктами господарювання [212, 132].

Зазначені нормативні акти в цілому необхідні і достатні для правового регулювання створення та використання засобів ЕЦП.

Виходячи з наведеного, можна зробити такий висновок: ЕЦП генерується з засобів ЕЦП, які відповідають державним технічним стандартам надійності. Провайдер сертифікаційних послуг, який здійснює сертифікацію відкритих ключів ЕЦП, може сам, використовуючи власні засоби ЕЦП, створювати електронні цифрові підписи, на які потім сам провайдер й буде видавати сертифікати відкритих ключів; або окремий суб'єкт господарської діяльності може створювати з своїх власних засобів ЕЦП електронні цифрові підписи. Встановлення відповідності засобів ЕЦП, використаних для виготовлених електронних цифрових підписів, технічним стандартам може встановлюватися двома шляхами – видачею компетентним органом сертифіката відповідності на дані засоби; або проведенням експертизи на предмет встановлення відповідності використаних засобів ЕЦП вимогам нормативних документів, оцінки їх надійності або науково-технічного рівня. Враховуючи виключно важливе значення господарської діяльності у сфері криптографічного захисту інформації, зокрема виготовлення засобів ЕЦП, їх сертифікація, проведення експертизи, для інтересів суспільства та держави, вказані види господарсь-

кої діяльності підлягають ліцензуванню в порядку, встановленому чинним законодавством України.

Отже, стає наочною некоректність підходу Закону України "Про електронний цифровий підпис" до виділення окремо понять "засобів ЕЦП" та "надійних засобів ЕЦП" (рис. 3.1).

Рис. 3.1. ЕЦП та засоби ЕЦП за Законом України "Про електронний цифровий підпис"

Так, як було з'ясовано в даному підрозділі, в основі засобів ЕЦП лежать засоби криптографічного захисту інформації. Згадуваний вище Указ Президента України від 22 травня 1998 року №505/98, яким було затверджено Положення "Про порядок здійснення криптографічного захисту інформації в Україні", передбачає, що всі засоби криптографічного захисту інформації

проходять сертифікацію чи державну експертизу. Таким чином, для того, щоб засоби криптографічного захисту інформації використовувалися відповідно до чинного законодавства, вони повинні пройти сертифікацію на предмет відповідності державним нормам та стандартам або одержати позитивний висновок державної експертизи у сфері криптографічного захисту інформації. Причому підзаконні нормативні акти Департаменту не передбачають виділення засобів криптографічного захисту інформації та посилених засобів криптографічного захисту інформації, вони єдині.

Звідси Закон України "Про електронний цифровий підпис", з нашої точки зору штучно та недоцільно виділяє засоби ЕЦП та надійні засоби ЕЦП. Отже, існують єдині засоби криптографічного захисту інформації з обов'язковою процедурою сертифікації або одержанням позитивного висновку державної експертизи. А тому відокремлення двох видів засобів ЕЦП, які з технічної точки зору однаково надійні, уявляється зайвим та безпідставним.

Далі, законодавець протирічить сам собі та вказує, що існує один вид ЕЦП. Складається ситуація, коли, з точки зору законодавця, ЕЦП, що ґрунтується на засобах ЕЦП, та ЕЦП, що ґрунтується на надійних засобах ЕЦП, є одним й тим самим електронним цифровим підписом, визначення якого наведено в ст. 1 вказаного закону України. Більш логічно та послідовно було б виділяти тоді й два види ЕЦП, але більшість держав світу та міжнародних актів цього не передбачають.

І на завершення, законодавець знов, вочевидь, поспішно, виділяє два види сертифікатів ключів підписів на один вид ЕЦП. Таким чином, складається ситуація, коли фактично один й той самий засіб криптографічного захисту інформації з сертифікатом відповідності чи позитивним висновком державної експертизи лежить в основі і засобів ЕЦП, і надійних засобів ЕЦП, з яких генерується один єдиний вид ЕЦП, який може існувати із звичайним сертифікатом відкритого ключа або із посиленим сертифікатом відкритого ключа. Причому за правовим статусом до власноручного підпису прирівнюється лише ЕЦП з посиленим сертифікатом відкритого ключа (ч. 1 ст. 3 вказаного Закону України).

Більш правильною буде така модель (рис. 3.2).

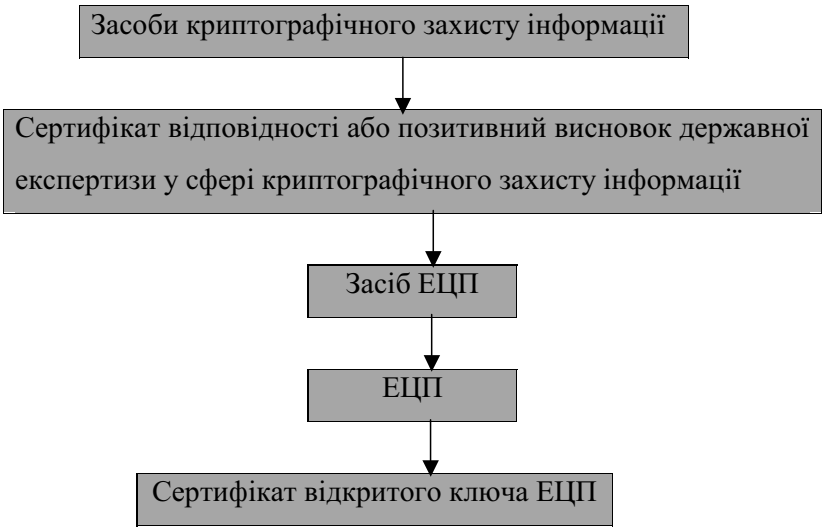

Рис. 3.2. Модель функціонування ЕЦП, що пропонується

Відповідно до даної запропонованої моделі засоби криптографічного захисту інформації згідно з чинним законодавством України проходять обов'язкову сертифікацію або одержують позитивний висновок державної експертизи у сфері криптографічного захисту інформації. З таких засобів КЗІ створюється єдиний вид засобів ЕЦП, з яких, у свою чергу, генерується ЕЦП. ЕЦП має єдиний вид сертифіката, тому використання ЕЦП з сертифікатом в порядку, встановленому законодавством України, дає підстави прирівняти його за правовим статусом до власноручного підпису. Такий підхід запроваджений рядом країн світу та міжнародними актами.

Таким чином, доцільно внести зміни до Закону України "Про електронний цифровий підпис" в частині запровадження вище викладеної моделі, яка передбачає існування одного виду засобів ЕЦП, одного виду ЕЦП та одного виду сертифіката відкритого ключа ЕЦП.

Одна з умов визнання ЕЦП за правовим режимом рівнозначним підпису фізичної особи чи уповноваженого представника юридичної особи – це наявність сертифіката відкритого ключа ЕЦП, чинного на момент підписання електронного документа (стаття 3 Закону України "Про електронний цифровий підпис"). Отже, правове регулювання відносини у сфері використання ЕЦП відбувається через видачу компетентною організацією чи органом сертифіката відкритого ключа ЕЦП.

Сертифікат відкритого ключа ЕЦП – це електронний документ[4] з електронним цифровим підписом уповноваженої особи провайдера сертифікаційних послуг, який включає в себе відкритий ключ ЕЦП, та видається провайдером сертифікаційних послуг особам, які здійснюють електронну комерцію, для підтвердження дійсності ЕЦП та ідентифікації володільця сертифіката відкритого ключа підпису.

Закон України "Про електронний цифровий підпис" передбачає можливість видачі документів, що свідчать про юридичне визнання ЕЦП (сертифікатів), двох видів: звичайних та посилених. Стаття 1 вказаного Закону України визначає сертифікат відкритого ключа як документ, виданий центром сертифікації, який засвідчує чинність і належність відкритого ключа підписувачу; посилений сертифікат відкритого ключа – як сертифікат ключа, виданий акредитованим центром сертифікації, засвідчувальним центром, центральним засвідчувальним органом.

Поділ сертифікатів на звичайні та посилені вказаний закон проводить в залежності від того, на якому правовому титулі перебуває майно у особи, яка звертається за одержанням сертифіката ключа ЕЦП. Зокрема передбачається, щоб підприємства, установи та організації державної форми власності, а також органи державної влади та місцевого самоврядування використовували для засвідчення чинності відкритого ключа ЕЦП лише посилений сертифікат відкритого ключа. Інші юри-

[4] Відповідно до ст. 1 Закону України ввід 22 травня 2003 р. "Про електронний цифровий підпис" сертифікати відкритих ключів ЕЦП можуть розповсюджуватися на електронних носіях або у вигляді документа на папері.

дичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа звичайним, а не посиленим сертифікатом, тобто заборони використовувати ними посилені сертифікати нема.

Виходячи із визначень звичайного та посиленого сертифікатів ключів ЕЦП, що містяться в ст. 1 вказаного закону, різниця між ними полягає в тому, що посилені сертифікати видаються такими провайдерами сертифікаційних послуг, як акредитований центр сертифікації, засвідчувальний центр та центральний засвідчувальний орган, а звичайний сертифікат видається центром сертифікації.

Єдина різниця між центром сертифікації та акредитованим центром сертифікації полягає у необхідності останнього здійснити акредитацію, тобто здійснити процедуру документального засвідчення компетентності здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів, що випливає зі змісту ст. 9 вказаного закону.

Засвідчувальний центр відповідно до ст. 10 вказаного закону відповідає вимогам, встановленим законодавством для акредитованого центру сертифікації. Його особливість полягає у тому, що він засвідчує чинність відкритих ключів ЕЦП та акредитації групи центрів сертифікації ключів, що надають послуги ЕЦП органам державної влади і місцевого самоврядування та підпорядкованим ним підприємствам, установам, організаціям. Таким чином, засвідчувальний центр має право сам надавати послуги ЕЦП або може в своєму підпорядкуванні мати акредитовані центри сертифікації, які будуть надавати такі послуги даному органу та підпорядкованим йому юридичним особам. З цією метою засвідчувальний центр уповноважений сам проводити акредитацію та видавати посилені сертифікати, якими акредитовані центри посвідчують сертифікати, що видаються ними зацікавленим особам.

Центральний засвідчувальний орган відповідно до ст. 11 вказаного закону формує та видає посилені сертифікати ключів засвідчувальним центрам та центрам сертифікації ключів, якими останні посвідчують сертифікати ключів, що видаються

ними зацікавленим особам. Але не вказано, що даний орган проводить акредитацію та видає посилені сертифікати, якими акредитовані центри сертифікації можуть засвідчувати чинність сертифікатів зацікавлених осіб. Таким чином, закон не забороняє юридичним особам недержавної форми власності та фізичним особам використовувати посилені сертифікати ключів, але існування акредитованого центру сертифікації, уповноваженого видавати такі сертифікати, не передбачено, оскільки акредитовані центри сертифікації, названі у ст. 10, позбавлені права обслуговувати недержавних юридичних осіб та фізичних осіб.

Статті 1 та 3 вказаного закону передбачають, що посилений сертифікат видається на ЕЦП, який ґрунтується на надійних засобах, тобто такі засоби повинні мати сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації. Тобто, в силу самого поняття ЕЦП, він може генеруватися лише з тих засобів, які відповідають державним стандартам у сфері криптографічного захисту інформації.

Отже можна стверджувати, що передбачуваний вказаним законом ЕЦП, незалежно від того, який сертифікат він має, генерується з однакових засобів ЕЦП, що повинні відповідати державним стандартам, тобто з технічної точки зору вони є однаково надійними. Виділення сертифікатів двох видів є штучним, таким що не гарантує підвищеної надійності та безпеки посилених сертифікатів. Система органів, що здійснює сертифікацію ключів ЕЦП, в зв'язку з цим стає недоцільно розгалуженою та ускладненою, призводить до існування численних реєстрів виданих сертифікатів ключів підписів замість існування єдиного державного реєстру всіх сертифікатів відкритих ключів підписів, що використовуються в Україні.

Більш того, це дозволяє зробити висновок про те, що суб'єкти господарювання, засновані на державній формі власності, змушені у сфері електронної комерції використовувати лише один вид електронного підпису – електронний цифровий підпис.

Більш логічною та доцільною уявляється така система електронних підписів (рис. 3.3.).

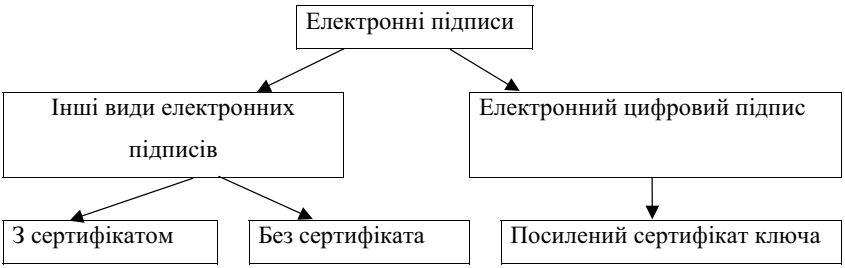

Рис. 3.3. Система електронних підписів, яка пропонується

Існує родове поняття електронного підпису, яке включає в себе певні види, зокрема ЕЦП (це вбачається з визначення понять електронного підпису та ЕЦП, що міститься в ст. 1 Закону України "Про електронний цифровий підпис") чи інші види електронного підпису. Інші види електронного підпису, окрім ЕЦП, можуть використовуватися особами, які здійснюють електронну комерцію як з сертифікатом (ст. 5 Директиви ЄС "Про електронні підписи"), так й без нього (ст. 6 Типового закону ЮНСІТРАЛ "Про електронні підписи"). ЕЦП може застосовуватися лише з сертифікатом.

Отже саме для того, щоб підкреслити особливий рівень безпеки ЕЦП та відокремити його сертифікат від сертифікатів інших видів електронного підпису, законодавство багатьох держав світу й запропонувало називати сертифікати ЕЦП посиленими (кваліфікованими або вдосконаленими). Це, наприклад, згадувана вище Директива ЄС, закон Австрії "Про електронні підписи", закон Ірландії "Про електронну комерцію", Цивільний кодекс Франції (ст. ст. 1316 – 1316-4) [213] тощо.

Окремо слід вказати на протиріччя норм ст. 3 (ч. 1) та ст. 5 (ч. 2). Перша норма передбачає, що ЕЦП за правовим статусом прирівнюється до власноручного підпису при дотриманні умови його підтвердження з використанням посиленого сертифіката. Друга норма передбачає, що юридичні особи недержавної форми власності та фізичні особи можуть використовувати

ЕЦП без сертифіката відкритого ключа. Таким чином, особа, яка здійснює електронну комерцію, легально використовуючи ЕЦП без сертифіката, не може розраховувати на визнання такого ЕЦП рівнозначним власноручному підпису, а отже, не може підтвердити волевиявлення на укладання правочину через мережу електрозв'язку через відсутність підпису уповноваженої особи.

Частина 2 ст. 3 даного закону передбачає, що електронний підпис не може бути визнаний недійсним лише через те, що не ґрунтується на посиленому сертифікаті. Вважаємо, що таке положення закону є некоректним, оскільки дана норма протирічить закону в цілому та принципам електронної комерції. Так, ЕЦП без сертифіката відкритого ключа, який також є видом електронного підпису, та будь-які інші види електронного підпису, сертифікація яких є недоцільною, дійсно не можуть бути визнані недійсним з підстав відсутності сертифікату. Але закон й не передбачає, що такі електронні підписи визнаються рівнозначними власноручному підпису. Отже, дане положення протирічить не тільки принципам електронної комерції (принципу відкритості, або технологічного нейтралітету), а і положенням Типових законів ЮНСІТРАЛ "Про електронну комерцію" (ст. 7 ч. 1) та "Про електронні підписи" (ст. 6 ч. 1).

На підставі викладеного вважаємо, що доцільно існування одного виду засобів ЕЦП з обов'язковою процедурою сертифікації на предмет відповідності державним стандартам у сфері криптографічного захисту інформації; відповідного одного виду ЕЦП; відповідно одного виду сертифікатів відкритих ключів ЕЦП незалежно від виду заявника.

Зазначений підхід відповідає законодавчій практиці ряду держав світу, зокрема Російської Федерації, яка у законі від 10 січня 2002 р. "Про електронний цифровий підпис" передбачає видачу лише одного виду сертифікату (статті 3, 6), Директиві Європейського парламенту та Ради 1999/93/ЄС від 13 грудня 1999 року "Про правові підстави Співдружності для використання електронних підписів" (ст. ст. 2, 5) і передбачає видачу кваліфікованого сертифіката для засвідчення дійсності ЕЦП; в

той же час не виключає можливості одержання сертифікатів іншими видами електронного підпису.

Запровадження в Україні процедури сертифікації інших ніж ЕЦП видів електронного підпису вищевказаним законом України не передбачено, що уявляється справедливим, оскільки право повинно втручатися у ті суспільні відносини, які дійсно потребують правового регулювання. Вважаємо, що якщо сторони, керуючись вільним волевиявленням, прийшли до згоди про використання такого виду електронного підпису як, наприклад, код, порядок застосування якого законодавчо не регламентований, вважають його надійним та достатнім для відносин між собою, то сторони повинні узгодити між собою порядок використання такого виду електронного підпису, підтвердження його дійсності, порядок використання електронних документів, підписаних таким видом електронного підпису в якості судових доказів, тощо. Тобто, держава не повинна запроваджувати обмежень щодо використання таких видів електронного підпису, зокрема необхідність одержання сертифіката.

Держава в інтересах всього суспільства запропонувала суб'єктам господарювання можливість використовувати надійний спосіб ідентифікації відправника електронного документа та аутентифікації його змісту – використання ЕЦП, встановила технічні вимоги, на яких ЕЦП ґрунтується, закріпила правові вимоги до сертифікату ЕЦП тощо. І вже лише від суб'єкта господарювання повинно залежати, який вид електронного підпису він обере для своїх відносин – ЕЦП чи інший. Лише за таких умов правове регулювання відносин у сфері використання електронних підписів в Україні буде достатнім та оптимальним.

Відсутність обов'язку проходження сертифікації інших видів електронного підпису, ніж ЕЦП пов'язано з таким принципом регулювання відносин у сфері електронної комерції, як відкритість, або технологічний нейтралітет. Тобто надання особам, які здійснюють електронну комерцію, можливості вибору між різними технологічними рішеннями з

різною надійністю і тому різними законними наслідками використання таких рішень.

Аналіз деяких прийнятих у світі нормативних актів, які регулюють відносини у сфері використання ЕЦП, дозволяє прийти до висновку, що обсяг відомостей, які фіксуються у сертифікаті відкритого ключа ЕЦП, співпадає. Так, сертифікат повинен містити такі відомості:

1) прізвище, ім'я, по батькові фізичної особи або найменування юридичної особи та прізвище, ім'я, по батькові її уповноваженого представника – володільця закритого ключа ЕЦП;
2) номер цього документа, час початку та завершення його дії;
3) відкритий ключ ЕЦП;
4) найменування засобів ЕЦП, з якими використовується такий відкритий ключ ЕЦП;
5) найменування та юридична адреса провайдера сертифікаційних послуг, який видав даний сертифікат;
6) відомості про відносини, при здійсненні яких електронний документ з ЕЦП буде мати юридичне значення;
7) дані, які дозволяють ідентифікувати загальнодоступний реєстр володільців таких сертифікатів, в який внесено такий документ, та місце його опублікування.

За бажанням особи, яка звертається за одержанням ЕЦП та відповідного сертифіката до провайдера сертифікаційних послуг, особа-заявник у письмовій формі може просити про включення до сертифіката, крім вищезазначених, додаткових відомостей, які підтверджуються пред'явленням відповідних документів.

Призначенням сертифіката ЕЦП є однозначне встановлення того факту, що він одержаний у компетентній організації чи органі для підтвердження дійсності ЕЦП та ідентифікації володільця сертифіката відкритого ключа підпису.

Сертифікат ЕЦП видається у вигляді електронного документа або у вигляді паперового документа встановленого зразка. У першому випадку він підписується електронним цифровим підписом уповноваженої особи провайдера сертифікаційних послуг, у

другому оформляється на бланку цієї установи чи органу і підписується власноручним підписом уповноваженої особи.

Для забезпечення можливості обліку сертифікатів ключів ЕЦП, виданих провайдерами сертифікаційних послуг, можливості доступу до них третіх осіб для підтвердження чинності сертифікатів ключів ЕЦП, провайдер сертифікаційних послуг веде реєстр сертифікатів відкритих ключів ЕЦП, що ним були видані. Провайдер сертифікаційних послуг повинен внести виданий ним сертифікат до такого реєстру не пізніше дати початку дії виданого ним сертифіката відкритого ключа ЕЦП.

Термін зберігання сертифіката ключа підпису у формі електронного документа у провайдера сертифікаційних послуг визначається договором між ним та власником сертифіката ключа підпису. Законодавство ряду держав [37, ст. 7 ч. 2] пішло шляхом встановлення вимоги щодо необхідності зберігання в архівах органу, що легалізує, сертифіката відкритого ключа ЕЦП у вигляді електронного документа протягом строку, який є не меншим, ніж строк позовної давності для відносин, вказаних у сертифікаті як сфера використання ЕЦП. По закінченні цього терміну сертифікат ЕЦП повинен виключатися з реєстру сертифікатів ключів підписів та переводитися в режим архівного зберігання. Тобто у випадку, наприклад, пропущення строку позовної давності для захисту прав та законних інтересів в суді з поважних причин і поновлення вказаного строку, за вказівкою суду сертифікат відкритого ключа ЕЦП може бути вилучений з архівного зберігання провайдера сертифікаційних послуг та наданий суду для підтвердження або спростування відповідних обставин.

Дія сертифікату відкритого ключа ЕЦП може бути блокована провайдером сертифікаційних послуг на підставі вказівки компетентного органу (наприклад, на підставі рішення суду) чи особи, які мають таке право в силу закону чи договору. Така вказівка повинна містити строк, що вираховується у днях, на який дія сертифікату блокується. По закінченні цього строку провайдер при одержанні відповідної вказівки компетентного

органу чи особи, які мають таке право в силу закону чи договору, поновлює дію сертифіката ключа підпису.

Сертифікат відкритого ключа ЕЦП може бути блокований також у випадку, коли володільцю сертифіката відкритого ключа ЕЦП стало відомо про будь-яку подію та/або дію, що призвела або може призвести до несанкціонованого використання закритого ключа. При встановленні недостовірності даних про можливе несанкціоноване використання закритого ключа ЕЦП, дія такого блокованого сертифіката поновлюється (ст. 13 Закону України "Про електронний цифровий підпис").

Відповідно до вказівки компетентного органу чи особи, які мають таке право в силу закону чи договору, про блокування дії сертифіката ключа ЕЦП провайдер сертифікаційних послуг повідомляє про це користувачів сертифікатів ключів ЕЦП, що здійснюється шляхом внесення до реєстру сертифікатів ключів ЕЦП відповідної інформації з зазначенням дати та строку призупинення дії сертифіката ключа ЕЦП. Провайдер сертифікаційних послуг окремо повідомляє про це власника сертифікату ключа підпису та компетентний орган чи особу, від яких була одержана вказівка про блокування дії сертифіката.

Скасування, тобто припинення дії, сертифіката ключа ЕЦП може мати місце з таких підстав:

1) закінчення строку дії сертифіката;
2) за заявою в письмовій формі власника ЕЦП, на чиє ім'я виданий сертифікат ключа підпису, або його уповноваженого представника;
3) припинення діяльності юридичної особи, смерть фізичної особи – власника ключа ЕЦП або визнання її недієздатною за рішенням суду;
4) надання власником ключа ЕЦП недостовірних даних;
5) якщо відбулася будь-яка подія та/або дія, що призвели чи можуть призвести до несанкціонованого використання закритого ключа ЕЦП.

Провайдер сертифікаційних послуг здійснює скасування сертифіката ключа підпису шляхом внесення відомостей про скасування такого сертифіката до реєстру сертифікатів ключів

підписів з вказівкою на дату скасування, а також повідомляє про це власника сертифіката ключа підпису та компетентний орган чи особу, від яких була одержана вказівка про скасування даного сертифіката.

На підставі викладеного можна зробити висновок про те, що Закон України вимагає внесення ряду істотних змін, зокрема необхідно передбачити, що:

1) електронний підпис за правовим статусом прирівнюється до власноручного підпису особи, якщо він використовується на підставі узгодженого волевиявлення сторін, є надійним та таким, що відповідає меті, для якої електронний документ створюється і використовується;
2) ЕЦП має лише один вид сертифіката і не може застосовуватися особами, що здійснюють електронну комерцію, без сертифіката;
3) всі суб'єкти господарювання, а також органи державної влади та місцевого самоврядування повинні мати можливість обрати для застосування той вид електронного підпису, який є надійним та таким, що відповідає меті, для якої електронний документ створюється і використовується.

Змістом господарських правовідносин у сфері створення та використання ЕЦП є взаємозв'язок юридичних прав та обов'язків користувачів відкритого ключа ЕЦП, власників сертифікату ключа ЕЦП, провайдера сертифікаційних послуг та уповноваженого органу державної виконавчої влади (контролюючого органу). Юридичні права та обов'язки останніх двох суб'єктів будуть розглянуті у наступних підрозділах цього розділу.

Права та обов'язки суб'єктів правовідносин у сфері створення та використання ЕЦП взаємопов'язані, кореспондують один одному. Так, наприклад, обов'язок власника сертифіката ЕЦП не використовувати для ЕЦП відкриті і закриті ключі електронного цифрового підпису, якщо йому відомо, що ці ключі використовуються або використовувалися раніше, взаємопов'язаний та кореспондується з обов'язком провайдера сертифікаційних послуг вносити сертифікат ключа підпису до

власного реєстру сертифікатів ключів підписів. Зазначені обов'язки суб'єктів правовідносин у сфері використання ЕЦП пов'язані з таким обов'язком уповноваженого органу державної виконавчої влади, як обов'язок ведення єдиного загального державного реєстру сертифікатів ключів підписів, якими провайдери засвідчують сертифікати відкритих ключів підписів, що видаються ними зацікавленим особам.

Особливість взаємозв'язку прав та обов'язків суб'єктів правовідносин у сфері створення та використання ЕЦП проявляється також в тому, що будь-який суб'єкт господарювання у сфері даних правовідносин при взаємодії з іншими суб'єктами виконує певні обов'язки публічно-правового характеру. Наприклад, у господарських правовідносинах за договором про створення ЕЦП правам замовника (одержати передбачений договором електронний цифровий підпис, певної якості, у певний термін) відповідають права підрядника (створити такий ЕЦП), а правам підрядника (на оплату роботи зі створення передбаченого договором ЕЦП) – обов'язок замовника (здійснити своєчасну оплату робот підрядника). Зазначені права та обов'язки не є повними. Виходячи з вимог чинного законодавства України, обидві сторони під час розробки договірних умов у багатьох випадках повинні враховувати технічні вимоги до якості створюваного товару, передбачені у відповідних стандартах та технічних умовах. Виробник продукції (підрядник) повинен негайно зупинити виробництво (реалізацію) продукції, якщо відповідний орган державного нагляду встановить, що використання або зберігання такої продукції завдає або може завдавати шкоду життю, здоров'ю або майну особи (ст. 8 Закону України "Про електронний цифровий підпис").

У чинних нормативних актах окремих держав світу, які регулюють відносини у сфері використання ЕЦП, обсяг прав та обов'язків користувачів відкритого ключа ЕЦП та володільця сертифіката відкритого ключа ЕЦП не відрізняється. Узагальнюючи обов'язки володільця сертифіката ключа підпису, до них можна віднести:

1) обов'язок не використовувати для електронного цифрового підпису відкриті і закриті ключі електронного циф-

рового підпису, якщо йому відомо, що ці ключі використовуються або використовувалися раніше. Закріплення даного обов'язку володільця сертифіката ключа підпису має виключно важливе значення, саме тому даний обов'язок повинен кореспондуватися з імперативною нормою про обов'язок уповноваженого органу державної виконавчої влади вести єдиний реєстр сертифікатів ключів підписів, що видаються провайдерами сертифікаційних послуг в Україні. Взаємодія зазначених двох норм створить умови, за яких два заявники не зможуть, використовуючи один і той самий закритий ключ ЕЦП одержати у різних провайдерів сертифікаційних послуг однакові відкрити ключі, хоча й з різними сертифікатами;

2) обов'язок зберігати в таємниці закритий ключ ЕЦП. Даний обов'язок володільця сертифіката ключа підпису ґрунтується на положеннях статті 30 "Інформація з обмеженим доступом" Закону України від 2 січня 1992 р. "Про інформацію". Частина 2 ст. 30 даного закону визначає конфіденційну інформацію як "відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов". Фізичні та юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту. Таким чином, закритий ключ ЕЦП являє собою конфіденційну інформацію володільця сертифіката ключа підпису, яку він повинен зберігати в таємниці. Це правило лежить в основі використання ЕЦП – відкритий ключ ЕЦП відомий всім і кожному, закритий ключ ЕЦП – лише власнику сертифіката ключа підпису;

3) обов'язок негайно вимагати блокування дії сертифіката ключа підпису або його скасування при наявності підстав вважати, що таємниця закритого ключа ЕЦП порушена [214]. Дане правило означає, що, якщо власник сертифіката ключа підпису дізнався або повинен був дізнатися про можливість порушення режиму обмеженого доступу до закритого ключа підпису (тобто про порушення конфіденційності інформації про закритий ключ підпису), провайдер сертифікаційних послуг зобов'язаний на вимогу власника відповідного сертифіката ключа підпису блокувати або скасувати дію сертифіката ключа підпису.

При недотриманні зазначених вимог відшкодування заподіяних внаслідок цього збитків покладається на власника сертифіката ключа підпису.

Власник сертифіката ключа підпису перед користувачами відповідного відкритого ключа несе відповідальність у межах, зазначених у сертифікаті, за збитки та інші несприятливі наслідки, що виникли в зв'язку з несанкціонованим використанням закритого ключа ЕЦП.

Користувач відкритого ключа ЕЦП має право звернутися до провайдера сертифікаційних послуг, який видав сертифікат ключа підпису, за підтвердженням сертифіката ключа підпису та відомостей, що в ньому зазначені.

Таким чином можна стверджувати, що обсяг прав та обов'язків користувачів відкритого ключа ЕЦП та володільця сертифіката відкритого ключа ЕЦП, передбачений ст. ст. 7 та 8 Закону України "Про електронний цифровий підпис", є необхідним та достатнім.

3.2. Правовий статус провайдерів сертифікаційних послуг

Провайдери сертифікаційних послуг – це юридичні особи, які мають повноваження засвідчувати відповідність відкритого ключа ЕЦП закритому ключу особам, про що видається відповідний сертифікат ключа ЕЦП.

Система провайдерів сертифікаційних послуг за законом України "Про електронний цифровий підпис" представлена центрами сертифікації, акредитованими центрами сертифікації, засвідчувальними центрами та центральним засвідчувальним органом. Вказані провайдери перебувають у певній ієрархії один відносно одного (рис. 3.4).

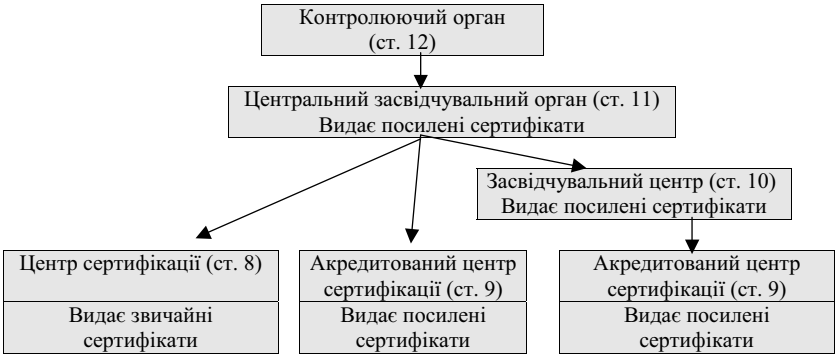

Рис. 3.4. Система провайдерів сертифікаційних послуг в Україні

Низовий рівень системи провайдерів сертифікаційних послуг займають центри сертифікації та акредитовані центри сертифікації.

Центром сертифікації ключів може бути юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги ЕЦП та засвідчила свій відкритий ключ у центральному засвідчувальному органі або засвідчувальному центрі.

До компетенції центру сертифікації ключів відносяться такі права та обов'язки:

1) надавати послуги ЕЦП та обслуговувати сертифікати ключів;
2) отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування сертифіката ключа без-

посередньо у юридичної або фізичної особи чи у її уповноваженого представника;

3) забезпечувати захист інформації в автоматизованих системах відповідно до законодавства;
4) забезпечувати захист персональних даних, отриманих від підписувача, згідно з законодавством;
5) встановлювати під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу;
6) своєчасно скасовувати, блокувати та поновлювати сертифікати ключів у випадках, передбачених законом;
7) своєчасно попереджувати підписувача та додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання ЕЦП, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку центру сертифікації ключів;
8) перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;
9) цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;
10) вести електронний перелік чинних, скасованих і блокованих сертифікатів ключів;
11) забезпечувати цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали;
12) забезпечувати зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;
13) надавати консультації з питань, пов'язаних з ЕЦП.

Акредитованим центром сертифікації ключів є центр сертифікації ключів, акредитований в установленому порядку. Акредитований центр сертифікації ключів має право: а) надавати послуги ЕЦП та обслуговувати виключно посилені сертифікати ключів; б) отримувати та перевіряти інформацію, необхідну

для реєстрації підписувача і формування посиленого сертифіката ключа, безпосередньо у юридичної або фізичної особи чи її представника.

Акредитований центр сертифікації ключів має виконувати усі зобов'язання та вимоги, встановлені законодавством для центру сертифікації ключів, та додатково зобов'язаний використовувати для надання послуг ЕЦП надійні засоби ЕЦП.

З метою забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи центрів сертифікації ключів, які надають послуги електронного цифрового підпису цьому органу і підпорядкованим йому підприємствам, установам та організаціям, Кабінет Міністрів України може визначити засвідчувальний центр центрального органу виконавчої влади. Інші державні органи також можуть за погодженням з Кабінетом Міністрів України визначити свої засвідчувальні центри, призначені для виконання вищевказаних функцій.

Засвідчувальний центр по відношенню до групи центрів сертифікації ключів має ті самі функції і повноваження, що й центральний засвідчувальний орган стосовно центрів сертифікації ключів, та відповідає вимогам, встановленим законодавством для акредитованого центру сертифікації ключів.

Засвідчувальний центр реєструється, засвідчує свій відкритий ключ і акредитується у центральному засвідчувальному органі.

Центральний засвідчувальний орган визначається Кабінетом Міністрів України. До компетенції центрального засвідчувального органу відноситься:

1) формування і видача посилених сертифікатів ключів засвідчувальним центрам та центрам сертифікації ключів;
2) блокування, скасування та поновлення посилених сертифікатів ключів засвідчувальних центрів та центрів сертифікації ключів;
3) ведення електронних реєстрів чинних, блокованих та скасованих посилених сертифікатів ключів засвідчувальних центрів та центрів сертифікації ключів;
4) ведення акредитації центрів сертифікації ключів, отримання та перевірка інформації, необхідної для їх акредитації;

5) забезпечення цілодобового доступу засвідчувальних центрів та центрів сертифікації ключів до посилених сертифікатів ключів та відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали;
6) зберігання посилених сертифікатів ключів засвідчувальних центрів та центрів сертифікації ключів;
7) надання засвідчувальним центрам та центрам сертифікації ключів консультацій з питань, пов'язаних з використанням ЕЦП.

Центральний засвідчувальний орган відповідає вимогам, встановленим законодавством для акредитованого центру сертифікації ключів.

Функції контролюючого органу здійснює спеціально уповноважений центральний орган виконавчої влади у сфері криптографічного захисту інформації, який перевіряє дотримання вимог законодавства центральним засвідчувальним органом, засвідчувальними центрами та центрами сертифікації ключів.

У разі невиконання або неналежного виконання обов'язків та виявлення порушень вимог, встановлених законодавством для центру сертифікації ключів, засвідчувального центру, контролюючий орган дає розпорядження центральному засвідчувальному органу про негайне вжиття заходів по усунення правопорушення.

Аналіз законодавства ряду держав світу дозволяє стверджувати, що поширеною в світі є практика ліцензування діяльності провайдерів сертифікаційних послуг [34, 37]. Господарська діяльність даного суб'єкту в частині створення ключів ЕЦП та видачі відповідних сертифікатів має виключно важливе значення як для осіб, що здійснюють електронну комерцію, так і для суспільства й держави в цілому, які зацікавлені у впорядкуванні правовідносин у сфері використання ЕЦП, формуванні умов забезпечення стійкості економічних стосунків суб'єктів господарювання в Україні. Вказані обставини вимагають державного втручання у зазначені відносини, що детальніше буде розглянуто у підрозділі 3 цього розділу.

Один з основних видів діяльності, який здійснюють провайдери сертифікаційних послуг, це видача зацікавленим особам

сертифікатів ключів підписів. Сертифікат видається у вигляді електронного документа з ЕЦП уповноваженої особи провайдера сертифікаційних послуг або паперового документа з власноручним підписом уповноваженої особи провайдера сертифікаційних послуг.

Провайдери сертифікаційних послуг до початку використання ЕЦП уповноваженої особи провайдера сертифікаційних послуг для посвідчення від імені провайдера сертифікатів ключів ЕЦП зобов'язані одержати у центральному засвідчувальному органі сертифікат ключа підпису уповноваженої особи провайдера сертифікаційних послуг у вигляді електронного документа (ст. 11 Закону України "Про електронний цифровий підпис").

Центральний засвідчувальний орган влади веде єдиний державний реєстр сертифікатів ключів підписів, якими провайдери сертифікаційних послуг посвідчують сертифікати ключів підписів, що видаються ними, забезпечує можливість вільного доступу до цього реєстру, здійснює за зверненнями фізичних осіб, організацій, органів державної влади, органів місцевого самоврядування підтвердження істинності ЕЦП уповноважених осіб провайдерів сертифікаційних послуг у виданих ними сертифікатах ключів підписів.

ЕЦП уповноважених осіб провайдерів сертифікаційних послуг можуть використовуватися тільки після включення їх до єдиного державного реєстру сертифікатів ключів підписів. Використання цих ЕЦП пов'язано виключно з метою посвідчення сертифікатів ключів підписів і відомостей про їх дію.

Правове регулювання відносин у сфері сертифікаційних послуг, що існує у багатьох державах світу, не передбачає обов'язку провайдеру сертифікаційних послуг бути створеним в певній організаційно-правовій формі.

Як правило, провайдер сертифікаційних послуг повинен бути юридичною особою або фізичною особою – суб'єктом підприємницької діяльності, мати необхідні матеріальні і фінансові можливості, що дозволяють йому нести цивільну відповідальність перед користувачами сертифікатів ключів ЕЦП за збитки, що можуть бути понесені ними внаслідок недостовір-

ності відомостей, що містяться в сертифікатах ключів підписів. Провайдери сертифікаційних послуг можуть поєднувати діяльність у сфері створення, сертифікації та наданні інших послуг ЕЦП з іншими видами господарської діяльності з дотриманням умов їх здійснення, передбачених чинним законодавством України.

Поняття припинення діяльності суб'єкта господарського права охоплює юридичні підстави, акти та відповідні процесуальні дії [173, с. 58]. Діяльність провайдерів сертифікаційних послуг, що видають сертифікати ключів підписів для використання в мережах електрозв'язку, припиняється в порядку, встановленому для суб'єктів господарювання чинним законодавством України (ч. 1 ст. 14 Закону України від 22 травня 2003 р. "Про електронний цифровий підпис"). Вказаний закон цілком справедливо розглядає лише певні особливості припинення діяльності провайдерів сертифікаційних послуг, пов'язані із характером здійснюваної діяльності та необхідністю збереження сертифікатів відкритих ключів підписів провайдерів, що припиняють свою діяльність.

Про припинення діяльності провайдер сертифікаційних послуг повідомляє власників сертифікатів відкритих ключів ЕЦП за три місяці (ч. 2 ст. 14 вказаного закону). Після повідомлення провайдери позбавляються права видавати сертифікати ключів підписів. Про припинення діяльності провайдери також повідомляють центральний засвідчувальний орган. Якщо акредитовані центри сертифікації створювалися для обслуговування ЕЦП центральних органів державної влади та місцевого самоврядуванні й підпорядкованих їм підприємств, установ і організацій – про припинення діяльності вони повідомляють відповідний засвідчувальний орган.

При припиненні діяльності провайдерів сертифікаційних послуг сертифікати ключів підписів, видані цими провайдерами, скасовуються і реєстр таких сертифікатів передається центральному засвідчувальному органу. Акредитовані центри сертифікації, що створювалися для обслуговування ЕЦП центральних органів державної влади та місцевого самовряду-

вання та підпорядкованих їм підприємств, установ і організацій, передають свої реєстри скасованих сертифікатів відкритих ключів ЕЦП відповідному засвідчувальному органу.

Частина 6 ст. 14 вказаного закону передбачає, що порядок передачі акредитованими центрами сертифікації сертифікатів ключів ЕЦП, відповідних реєстрів сертифікатів та документованої інформації встановлюється Кабінетом Міністрів України. Але такий порядок ще не встановлений.

Необхідність зберігання сертифікатів ключів підписів, які припинили дію, викликана тим, що тим чи іншим суб'єктам господарювання для захисту їх прав та законних інтересів може виникнути необхідність одержати відомості про належність того чи іншого електронного цифрового підпису конкретній особі в певний момент часу.

Аналіз прийнятих у світі нормативних актів, які регулюють відносини у сфері використання ЕЦП, дозволяє прийти до висновку, що перелік послуг, які надає провайдер сертифікаційних послуг, в цілому співпадає і, зокрема, включає:

1) створення ключів ЕЦП за зверненням зацікавлених осіб з гарантією зберігання в таємниці закритого ключа ЕЦП;
2) блокування і поновлення дії сертифікатів ключів підписів, а також їх скасування;
3) ведення реєстру сертифікатів ключів підписів, забезпечення його актуальності і можливості вільного доступу до нього;
4) перевірка наявності відкритих ключів ЕЦП у реєстрі сертифікатів ключів підписів і архіві провайдера сертифікаційних послуг;
5) видача сертифікатів ключів підписів у формі документів на паперових носіях та (або) у формі електронних документів з інформацією про їх дію;
6) здійснення за зверненням користувачів сертифікатів ключів підписів підтвердження істинності ЕЦП в електронному документі щодо виданих їм сертифікатів ключів підписів;
7) може надавати інші пов'язані з використанням електронних цифрових підписів послуги.

Виготовлення сертифікатів ключів підписів здійснюється на підставі заяви зацікавленої особи. Відомості, що містяться в заяві, підтверджуються пред'явленням відповідних документів.

При виготовленні провайдером сертифікаційних послуг сертифікатів ключів підписів у вигляді документів на паперових носіях такі сертифікати повинні виготовлюватися у двох примірниках, завірятися власноручними підписами власника сертифіката ключа підпису й уповноваженої особи провайдера сертифікаційних послуг, а також його печаткою. Один примірник сертифіката ключа підпису повинен видаватися власнику сертифіката ключа підпису, другий – залишатися у провайдера.

Таким чином, провайдери сертифікаційних послуг являють собою сукупність суб'єктів господарювання, створених відповідно до чинного законодавства України, які надають послуги у сфері використання ЕЦП. Вказані особи одержують свій сертифікат відкритого ключа у центральному засвідчувальному органі, яким засвідчують сертифікати відкритих ключів ЕЦП зацікавлених осіб. Здійснення господарської діяльності щодо надання послуг у сфері використання ЕЦП повинно ґрунтуватися на одержанні ліцензії.

Система провайдерів сертифікаційних послуг та центральний засвідчувальний орган тісно взаємодіють один з одним. З одного боку, провайдери сертифікаційних послуг одержують сертифікат ключа підпису, яким посвідчують сертифікати ключів підписів, що ними видаються, з іншого боку, центральний засвідчувальний орган веде єдиний державний реєстр сертифікатів ключів підписів таких провайдерів.

Необхідно підкреслити, що мова йде саме про систему провайдерів сертифікаційних послуг, тобто про явище, яке складається з певних елементів, що тісно пов'язані та взаємодіють один з одним.

Провайдери сертифікаційних послуг повинні бути пов'язані між собою в єдину систему, а саме необхідно створити єдину базу даних сертифікатів ключів підписів, які видаються провайдерами сертифікаційних послуг України, ведення якої доцільно покласти на центральний засвідчувальний орган. Видача нового сертифіката ключа підпису повинна автоматично відоб-

ражатися у такій базі даних, що дозволить виключити можливість шахрайства з використанням ЕЦП.

Встановлена Законом України від 22 травня 2003 р. "Про електронний цифровий підпис" система провайдерів сертифікаційних послуг є занадто громіздкою, ускладненою та недоцільною. Найбільш авторитетні нормативні акти різних країн світу, які регулюють відносин у сфері використання електронних підписів, не передбачають створення різних видів провайдерів сертифікаційних послуг в залежності від форми власності суб'єктів господарювання, що звертаються за одержанням послуг ЕЦП. Вочевидь, доцільне функціонування одного виду провайдерів, які надають послуги ЕЦП всім зацікавленим особам, та підпорядковуються центральному засвідчувальному органу, який здійснює державне управління та контроль за їх діяльністю.

Досліджуючи правовий статус провайдерів сертифікаційних послуг в Україні, особливої уваги заслуговують обов'язки цього суб'єкта у правовідносинах з володільцем сертифіката відкритого ключа ЕЦП та проблема відповідальності провайдерів сертифікаційних послуг.

Обов'язки провайдерів сертифікаційних послуг (центрів сертифікації, акредитованих центрів сертифікації, засвідчувальних центрів та центрального засвідчувального органу) передбачені законом України від 22 травня 2003 р. "Про електронний цифровий підпис" (ст. ст. 8–11).

Аналіз прийнятих у світі нормативних актів, які регулюють відносин у сфері використання ЕЦП, та норм вказаного закону України дозволяє прийти до висновку, що перелік обов'язків провайдерів сертифікаційних послуг у відносинах з власником сертифікату відкритого ключа ЕЦП в цілому співпадає і, зокрема, включає:

1. Забезпечення видачі сертифіката ключа підпису всім зацікавленим особам, які звернулися до нього у встановленому законом порядку. Право використовувати ЕЦП для підтвердження волевиявлення суб'єкта господарювання на укладання того чи іншого господарського договору через мережу електрозв'язку не пов'язується і не повинно пов'язуватися з одержанням попере-

нього дозволу компетентного органу державної влади. Будь-яка фізична або юридична особа має право звернутися до провайдера сертифікаційних послуг за створенням ЕЦП та одержанням відповідного сертифіката ключа підпису. Такі правовідносини ґрунтуються на договорі, що укладається між провайдером сертифікаційних послуг та відповідною зацікавленою особою.

2. Внесення сертифіката ключа підпису до власного реєстру сертифікатів ключів підписів, а також подання відомостей про це центральному засвідчувальному органу, до компетенції якого повинно відноситися ведення єдиного загального державного реєстру сертифікатів ключів підписів. Закріплення даного обов'язку спрямоване на створення чіткої ієрархічної структури реєстрів сертифікатів ключів підписів. Даний обов'язок повинен складатися з двох частин: обов'язку ведення власного реєстру сертифікатів ключів підпису та обов'язку подавати відомості про видачу сертифіката ключа підпису певній особі на певних умовах центральному засвідчувальному органу. Розглянемо ці дві частини окремо. При поєднанні обов'язку провайдера сертифікаційних послуг вести власний реєстр сертифікатів ключів підписів, що ним видаються, з обов'язком центрального засвідчувального органу вести реєстр сертифікатів ключів підписів, що видаються ним провайдерам сертифікаційних послуг, утворюється механізм, що забезпечує існування реєстрів сертифікатів ключів підписів двох рівнів.

Перший рівень являє собою реєстр сертифікатів ключів підписів, що видаються центральним засвідчувальним органом провайдерам сертифікаційних послуг, за допомогою яких останні посвідчують сертифікати ключів підписів, що ним видаються. Ведення даного реєстру першого рівня дозволяє будь-якій зацікавленій особі звернутися і одержати достовірну інформацію про правомірність або неправомірність видачі певним провайдером сертифікаційних послуг сертифікатів ключів підписів.

Другий рівень являє собою реєстр сертифікатів ключів підписів кожного окремого провайдера сертифікаційних послуг, що видаються ним всім зацікавленим особам, які звернулися до нього у встановленому законом порядку. Ведення даного реєстру пов'язано з необ-

хідністю впорядкування діяльності кожного окремого суб'єкта господарювання в цій сфері, а також з необхідністю забезпечити всім зацікавленим особам можливість встановити, що той чи інший сертифікат ключа підпису видавався або не видавався певній особі в певний момент часу на тих чи інших умовах. Існування реєстру сертифікатів другого рівня є необхідним елементом процедури підтвердження дійсності ЕЦП в електронному документі. Тобто позитивний результат перевірки дійсності ЕЦП відбувається за допомогою сертифіката ключа підпису підписувача, але цьому передує встановлення факту про те, що дійсно даний сертифікат був виданий відповідним провайдером сертифікаційних послуг, є чинним на момент підписання електронного документа та використовується відповідно до відомостей, що в ньому зазначені.

Друга частина обов'язку провайдера сертифікаційних послуг, а саме обов'язок подавати відомості центральному засвідчувальному органу про видачу сертифіката ключа підпису певній особі на певних умовах, кореспондується з обов'язком власника сертифіката ключа підпису не використовувати для ЕЦП відкриті і закриті ключі електронного цифрового підпису, якщо йому відомо, що ці ключі використовуються або використовувалися раніше, а також з обов'язком центрального засвідчувального органу вести єдиний загально державний реєстр сертифікатів ключів підписів. Взаємодія цих норм сприяє створенню правового механізму, який буде виключати можливість вчинення протиправних дій, особливо в частині електронних розрахунків за укладеними господарськими договорами.

3. Блокування або скасування дії сертифіката ключа підпису за зверненням його власника. Даний обов'язок тісно пов'язаний з першим обов'язком провайдера сертифікаційних послуг – забезпечення видачі сертифіката ключа підпису всім зацікавленим особам, які звернулися до нього у встановленому законом порядку.

Оскільки право використовувати ЕЦП для підтвердження волевиявлення суб'єкта господарювання не пов'язується з одержанням попереднього дозволу компетентного органу державної влади і ґрунтується виключно на волі суб'єкта, то логічним продовженням є право даного суб'єкта в будь-який момент з будь-яких підстав

ставити перед провайдером сертифікаційних послуг питання про блокування чи скасування відповідного сертифікату ключа підпису. Підставою такого волевиявлення власника сертифіката ключа підпису можуть бути, наприклад, відомості про порушення режиму конфіденційності інформації про закритий ключ ЕЦП.

4. Повідомлення власника сертифіката ключа підпису про факти, що стали відомі провайдеру сертифікаційних послуг і які істотно можуть позначитися на можливості подальшого використання сертифіката ключа підпису. Цей обов'язок провайдера сертифікаційних послуг спрямований на доведення до власника сертифіката ключа підпису відомостей, які можуть призвести до зміни існуючого правового режиму ЕЦП. До відомостей, що можуть істотно позначитися на можливості подальшого використання ЕЦП, можна віднести, наприклад, скасування технічних вимог та стандартів або запровадження нових, на яких ґрунтуються засоби ЕЦП, з яких безпосередньо виробляється ЕЦП.

5. Інші встановлені нормативними правовими актами або домовленістю сторін обов'язки, оскільки цей перелік не може бути вичерпним.

Таким чином, наведений невичерпний перелік обов'язків провайдерів сертифікаційних послуг (центрів сертифікації, акредитованих центрів сертифікації, засвідчувальних центрів та центрального засвідчувального органу) є необхідним і достатнім для правового регулювання використання ЕЦП особами, які здійснюють електронну комерцію в Україні.

Провайдер сертифікаційних послуг – один з центральних суб'єктів правовідносин у сфері електронної комерції, належне функціонування якого забезпечує об'єктивну можливість вчинення господарських договорів через мережі електрозв'язку, зокрема через мережу Інтернет[5]. Закон України "Про електронний цифровий підпис" (ст. 8) покладає на даного суб'єкта надання послуг

[5] Розглядається лише відповідальність такого суб'єкта правовідносин у сфері електронної комерції, як провайдер сертифікаційних послуг. Відповідальність інших суб'єктів правовідносин у сфері електронної комерції може бути предметом інших самостійних досліджень.

ЕЦП, що включає надання у користування засобів ЕЦП, допомогу при генерації відкритих ключів та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги.

В юридичній літературі справедливо зазначається, що в галузі права "обов'язок без відповідальності – юридичне ніщо, лише благе побажання" [215, с. 6–11], а тому законодавче закріплення обов'язків провайдерів сертифікаційних послуг у сфері здійснення такого важливого для суспільства та держави виду господарської діяльності, як створення та надання послуг ЕЦП, без належного забезпечення їх заходами юридичної відповідальності перетворює такі обов'язки на декларацію.

Як свідчить аналіз законодавчих актів "Про електронні підписи", в таких державах, як Туніс, Філіппіни, Люксембург, Австрія тощо передбачена кримінальна, адміністративна та цивільно-правова відповідальність провайдерів сертифікаційних послуг за невиконання чи неналежне виконання взятих на себе зобов'язань та порушення законодавства про електронні підписи.

Можливість притягнення провайдерів сертифікаційних послуг за вчинення окремих суспільно небезпечних правопорушень[6] до кримінальної відповідальності[7] підкреслює важливість цього виду господарської діяльності для всього суспільства та

[6] Зокрема, примушення будь-якої особи шляхом обману чи насильства до укладання правочинів у сфері електронної комерції, розголошення провайдером сертифікаційних послуг довіреної йому інформації (ст. ст. 50, 52 закону Тунісу "Про електронне переведення коштів та електронну комерцію"); незаконне копіювання, відтворення, поширення, імпортування, використання, зміна, зберігання... електронного підпису... шляхом використання телекомунікаційної мережі, такої як Інтернет, і не тільки (ст. 33 закону Філіппін "Про використання в комерційних та некомерційних цілях засобів електронного зв'язку та електронних документів"); підробка та зміна електронних ключів підписів (ст. 38 закону Люксембургу "Про електронну комерцію") тощо.

[7] Дослідження проблеми кримінальної відповідальності провайдерів сертифікаційних послуг за скоєні злочини може бути предметом самостійного дослідження фахівців науки кримінального права.

пов'язана з тим, що суворе дотримання провайдерами сертифікаційних послуг відповідного законодавства безпосередньо пов'язано із підвищенням ефективності ринкової системи, підвищенням довіри до запроваджуваних у сферу господарювання сучасних інформаційних технологій, та, накінець, із забезпеченням державної безпеки.

Законі України "Про електронний цифровий підпис" в частині відповідальності провайдерів сертифікаційних послуг за порушення законодавства про ЕЦП передбачена загальна норма, згідно з якою особи, винні у порушенні законодавства про ЕЦП, несуть відповідальність згідно з законом (ст. 15). При цьому як види правопорушень, так і види юридичної відповідальності взагалі і господарсько-правової зокрема, законом не встановлені. В той же час ці питання мають важливе значення, на що справедливо звертається увага в юридичній літературі [216, с. 11].

Для забезпечення належного виконання провайдерами сертифікаційних послуг своїх зобов'язань у сфері надання послуг ЕЦП необхідно з'ясувати форми господарсько-правової відповідальності цього суб'єкта, її межі та виділити види правопорушень, за вчинення яких винні особи можуть бути притягнуті до такої відповідальності.

Господарсько-правова відповідальність як вид юридичної відповідальності характеризується сукупністю особливих ознак[8] [173, с. 144], які дозволяють визначити господарсько-правову відповідальність як комплексний інститут господарського права, який має свій особливий предмет – господарські правопорушення, тобто протиправні дії або бездіяльність суб'єкта господарських відносин, які не відповідають вимогам норм господарсько-

[8] З точки зору форми ця відповідальність є юридичною. Юридична природа такої відповідальності полягає у негативній оцінці поведінки правопорушника з боку держави і в прямій вимозі або санкції закону застосувати до нього заходи матеріального впливу у вигляді відшкодування збитків, сплати неустойки, штрафу, пені тощо. Щодо змісту господарсько-правова відповідальність загалом є матеріальною і застосовується у формі певної системи майнових (економічних) санкцій. У функціональному відношенні ця відповідальність покликана стимулювати належне виконання господарських та інших зобов'язань.

го права, не узгоджуються з юридичними обов'язками зазначеного суб'єкта, порушують суб'єктивні права іншого учасника відносин або третіх осіб [173, с. 143]. Провайдер сертифікаційних послуг, як суб'єкт господарювання, у випадках невиконання чи неналежного виконання покладених на нього обов'язків повинен нести господарсько-правову відповідальність, передбачену законом або договором.

Відповідальністю є застосування до правопорушника встановлених законом або договором санкцій, внаслідок чого він зазнає майнових втрат. В.С. Щербина визначає господарсько-правові санкції як визначену безпосередньо законом або договором міру відповідальності правопорушника [173, с. 147].

Частина 2 ст. 217 ГКУ передбачає, що у сфері господарювання застосовуються такі види господарських санкцій: відшкодування збитків; штрафні санкції; оперативно-господарські санкції. Частина 3 вказаної статті зазначає, що крім зазначених у ч. 2 цієї статті господарських санкцій, до суб'єктів господарювання за порушення ними правил здійснення господарської діяльності застосовуються адміністративно-господарські санкції.

На нашу думку, провайдер сертифікаційних послуг у випадках невиконання чи неналежного виконання покладених на нього обов'язків повинен нести господарсько-правову відповідальність у таких формах, як: відшкодування збитків, штрафні санкції, оперативно-господарські санкції та адміністративно-господарські санкції.

Застосування таких господарських санкцій як відшкодування збитків, штрафних санкцій та оперативно-господарських санкцій відбувається у горизонтальних відносинах, тобто між рівноправними суб'єктами господарювання, які уклали договір про надання послуг ЕЦП (ч. 2 ст. 8 Закону України "Про електронний цифровий підпис"). Адміністративно-господарські санкції застосовуються у вертикальних відносинах, тобто між компетентним державним органом та провайдером сертифікаційних послуг.

Отже спочатку розглянемо відповідальність провайдера сертифікаційних послуг за невиконання чи неналежне виконання покладених на нього обов'язків у горизонтальних відносинах.

Питання про межі відповідальності провайдерів сертифікаційних послуг в частині відшкодування збитків за порушення законодавства про електронні підписи однозначно не вирішено ані в законодавстві, ані на доктринальному рівні.

Поширеним у законодавстві окремих держав світу є запровадження повного відшкодування збитків провайдером сертифікаційних послуг за порушення ним законодавства про електронні підписи, що включає відшкодування вартості втраченого, пошкодженого або знищеного майна, додаткових витрат, понесених стороною, яка зазнала збитків внаслідок порушення зобов'язання другою стороною, неодержаного прибутку та матеріальної компенсації моральної шкоди. Типовий закон ЮНСІТРАЛ "Про електронні підписи" (ст. 9) містить загальну норму, яка встановлює, що провайдер сертифікаційних послуг несе відповідальність за юридичні наслідки невиконання покладених на нього обов'язків.

У Директиві Європейського парламенту та Ради 1999/93/ЄС від 13 грудня 1999 р. "Про правові підстави Співдружності для використання електронних підписів" в ст. 6 "Відповідальність" передбачена відповідальність провайдера сертифікаційних послуг за збитки, завдані будь-якій організації, фізичній або юридичній особі. Норма аналогічного змісту закріплена і у ст. 22 закону Тунісу "Про електронне переведення коштів та електронну комерцію": провайдер сертифікаційних послуг відповідальний за всі збитки, що мають наслідки для кожної особи, яка довірилася належному виконанню провайдером своїх обов'язків.

Такий підхід виважений, він узгоджується із положеннями ч. 1 ст. 224 ГКУ, яка передбачає, що учасник господарських відносин, який порушив господарське зобов'язання або установлені вимоги щодо здійснення господарської діяльності, повинен відшкодувати завдані цим збитки суб'єкту, права або законні інтереси якого порушено.

В той же час інший підхід, який знайшов відображення як у доктрині, так і в законодавстві, полягає в тому, що запроваджене відшкодування провайдером сертифікаційних послуг лише реальних збитків (вартість втраченого, пошкодженого або зни-

щеного майна), завданих невиконанням чи неналежним виконанням покладених на нього обов'язків (так звану обмежена відповідальність).

Так, Модельний закон СНД від 9 грудня 2000 р. "Про електронний цифровий підпис" закріпив у ст. 16 норму, згідно з якою провайдер сертифікаційних послуг "...несе відповідальність в обсязі реальних збитків, завданих особі в результаті довіри до представлених у сертифікаті відомостей, які провайдер зобов'язаний перевірити та підтвердити. Відповідальність провайдера сертифікаційних послуг не включає штрафні санкції, відшкодування втраченої вигоди, відшкодування моральної шкоди".

Така точка зору обстоюється і рядом науковців в юридичній літературі [217]. Так, М.М. Дутов зазначає, що повна відповідальність центрів сертифікації уявляється невиправданою, оскільки, перш за все, вона не відповідає ступеню можливої вини. Автор наводить приклад: центр сертифікації видав свідоцтво, не перевіривши належним чином дані володільця закритого ключа ЕЦП, а потім підтвердив цей підпис за запитом зацікавленої особи; в результаті цього зацікавленій особі були завдані певні збитки. Але центр сертифікації може відповідати тільки за належне виконання своїх функцій, а не за всі збитки, розмір яких залежить від численних інших додаткових факторів [218, с. 169].

Слід зауважити, що цієї аргументації недостатньо, а сам підхід потребує подальшого дослідження. Окремо необхідно звернути увагу на застереження, які містяться у ч. 3 ст. 6 Директиви Європейського парламенту та Ради 1999/93/ЄС від 13 грудня 1999 р. "Про правові підстави Співдружності для використання електронних підписів": "Провайдер сертифікаційних послуг може передбачити у сертифікаті відкритого ключа ЕЦП обмеження на використання даного сертифіката, за умови, що такі обмеження визнаються третіми особами. В цьому випадку, провайдер не несе відповідальності за збитки, що виникли внаслідок використання сертифіката відкритого ключа ЕЦП, яке виходить за межі, зазначені в такому

сертифікаті". Норми, аналогічні за змістом, закріплені і у законах інших держав світу[9].

Доцільність запровадження такого застереження до Закону України "Про електронний цифровий підпис", на нашу думку, пов'язана з рядом обставин: а) обмеження на використання сертифіката відкритого ключа ЕЦП (наприклад, максимальна межа щодо ціни угоди, яка може вчинятися з використанням такого сертифіката) буде сприяти швидкому формуванню стабільної практики використання ЕЦП у сфері вчинення господарських договорів через мережі електрозв'язку; б) провайдери сертифікаційних послуг, передбачаючи обмеження на використання сертифіката відкритого ключа ЕЦП, зможуть заздалегідь планувати свою фінансово-господарську діяльність в частині формування, наприклад, певних резервних фондів; в) можливість диференційованого підходу дозволить провайдерам сертифікаційних послуг залучати широке коло суб'єктів господарювання, зацікавлених у наданні послуг ЕЦП.

Отже, закріплення в Законі України "Про електронний цифровий підпис" норми про те, що "в разі невиконання або неналежного виконання зобов'язання провайдером сертифікаційних послуг він зобов'язаний відшкодувати завдані цим збитки суб'єкту, права або законні інтереси якого порушено", та зазначеного вище "обмеження на використання сертифіката" буде, з одного боку, відповідати європейському підходу про повне відшкодування провайдерами сертифікаційних послуг завданих збитків у сфері надання послуг ЕЦП, а з іншого боку, зважаючи на новизну цих відносин для нашої держави та необхідність державного сприяння розвитку цих відносин, буде сприяти швидкому становленню та розвитку надання послуг ЕЦП.

Іншою формою господарсько-правової відповідальності провайдерів сертифікаційних послуг у горизонтальних відносинах повинна бути сплата штрафних санкцій (штрафу) за невиконання чи неналежне виконання покладених на них обов'язків.

Доцільність притягнення провайдера сертифікаційних послуг до цієї форми відповідальності пов'язана з тим, що цей

[9] Таке застереження передбачене, наприклад, у параграфі 26 ч. 4 закону Австрії "Про електронні підписи", ч. 3 ст. 16 Модельного закону СНД "Про електронний цифровий підпис".

суб'єкт господарювання надає виключно важливі для держави і суспільства послуги, тобто ступінь суспільної небезпеки правопорушень провайдерів сертифікаційних послуг у цій сфері значною. А тому каральна (дисциплінуюча) функція штрафу буде сприяти належному виконанню провайдерами сертифікаційних послуг взятих на себе зобов'язань.

Закон України "Про електронний цифровий підпис" не містить прямої вказівки про можливість застосування до провайдера сертифікаційних послуг штрафу, а також не містить переліку правопорушень, вчинення яких цим суб'єктом повинно розглядатися як підстава притягнення його до цієї форми відповідальності.

Аналізуючи обов'язки провайдерів сертифікаційних послуг, передбачені ч. 3 ст. 8 зазначеного вище Закону України, можна виділити групу обов'язків провайдерів, які спрямовані на обслуговування сертифікатів ключів підписів, і належне виконання яких безпосередньо впливає на договірні відносини між провайдером сертифікаційних послуг та підписувачем, а саме обов'язки:

- своєчасно скасовувати, блокувати та поновлювати сертифікати ключів;
- додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання ЕЦП;
- перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;
- цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;
- забезпечувати цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали.

Не підлягає сумніву те, що належне виконання провайдерами сертифікаційних послуг зазначених вище обов'язків має істотне значення для забезпечення прав та законних інтересів підписувачів.

Оскільки особливістю штрафу є те, що він застосовується лише там, де він передбачений законом або договором, доцільно в Законі України "Про електронний цифровий підпис" передбачити, що

виконання зобов'язання між провайдером сертифікаційних послуг та підписувачем може забезпечуватися штрафом. При цьому виникає питання про спосіб обчислення розміру такого штрафу.

Відповідно до ч. 4 ст. 231 ГКУ "у разі, якщо розмір штрафних санкцій законом не визначено, санкції застосовуються в розмірі, передбаченому договором. При цьому розмір санкцій може бути встановлено договором у відсотковому відношенні до суми невиконаної частини зобов'язання або у певній, визначеній грошовій сумі, або у відсотковому відношенні до суми зобов'язання незалежно від ступеня його виконання, або у кратному розмірі до вартості товарів (робіт, послуг)".

Очевидно, що розмір штрафу, яким забезпечується належне виконання провайдером сертифікаційних послуг взятих на себе зобов'язань, повинен бути визначений у певній грошовій сумі.

Крім того, в законодавстві доцільно передбачити можливість використання такої форми господарсько-правової відповідальності провайдерів сертифікаційних послуг у горизонтальних відносинах, як оперативно-господарські санкції, тобто заходи оперативного впливу підписувача на провайдера сертифікаційних послуг, спрямовані на припинення або попередження порушень зобов'язання, а саме відмова від оплати за зобов'язанням, яке виконане неналежним чином. Оскільки до суб'єкта, який порушив господарське зобов'язання, можуть бути застосовані лише ті оперативно-господарські санкції, застосування яких передбачено договором (ч. 2 ст. 235 ГКУ), то підписувачу, укладаючи з провайдером договір про надання відповідних послуг, доцільно передбачити, що до нього може бути застосована така санкція, як відмова від оплати за зобов'язанням.

Зазначеною формою господарсько-правової відповідальності повинно бути забезпечене виконання провайдером сертифікаційних послуг обов'язку забезпечення цілодобового доступу до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали, передбаченого ч. 4 ст. 8 Закону України "Про електронний цифровий підпис".

Крім того, було б доцільним передбачати у договорах про надання послуг ЕЦП з провайдером сертифікаційних послуг

право підписувача на дострокове розірвання договору у випадках несвоєчасного скасування, блокування та поновлення провайдером сертифікатів ключів.

Що стосується вертикальних відносин, тобто відносин між компетентним державним органом та провайдером сертифікаційних послуг, то останній за правопорушення у сфері надання послуг ЕЦП, повинен бути притягнутий до такої форми господарсько-правової відповідальності, як адміністративно-господарські санкції у вигляді: адміністративно-господарського штрафу, зупинення чи анулювання дії ліцензії на здійснення провайдером сертифікаційних послуг відповідного виду господарської діяльності.

Адміністративно-господарські санкції – це заходи організаційно-правового або майнового характеру, спрямовані на припинення правопорушення суб'єкта господарювання та ліквідацію його наслідків (ч. 1 ст. 238 ГКУ).

Оскільки підставою господарсько-правової відповідальності є вчинення суб'єктом господарювання відповідного правопорушення, то важливого значення набуває питання про перелік правопорушень, які повинні розглядатися як підстава для притягнення провайдерів сертифікаційних послуг до цієї форми відповідальності за порушення законодавства у сфері ЕЦП.

Оскільки законодавство України не містить переліку таких правопорушень, то доцільно з даного питання звернутися до аналізу законодавства інших держав світу.

Законодавчі акти ряду держав окремо виділяють правопорушення провайдерів сертифікаційних послуг у відносинах з уповноваженим державним органом у сфері надання послуг ЕЦП.

Так, у законі Тунісу "Про електронне переведення коштів та електронну комерцію" (ст. 46) [30] серед видів правопорушень, які можуть бути вчинені провайдером сертифікаційних послуг, названі: здійснення провайдером сертифікаційних послуг діяльності без отримання ліцензії або з порушенням вимог законодавства. За вчинення цих правопорушень зазначений закон передбачає адміністративне ув'язнення та сплату штрафу у розмірі від 1000 до 10000 динарів.

Закон Австрії "Про електронні підписи" (§ 26) [35] містить перелік можливих правопорушень провайдерів сертифікаційних послуг: порушення обов'язків з належного утримання реєстраційних матеріалів; відмова надати для перевірки журнали, реєстраційну та іншу документацію; неповідомлення контролюючого органу про якінебудь факти, які не дозволяють належним чином здійснювати діяльність відповідно до вимог безпеки. Вчинення цих правопорушень зазначений закон розглядає як адміністративне правопорушення та зобов'язує винну особу сплатити штраф.

Аналогічні норми, які закріплюють перелік видів правопорушень провайдерів сертифікаційних послуг та адміністративну відповідальність за їх вчинення, передбачені й у законі Гонконгу "Про електронні правочини" (ст. ст. 46–48) [27].

Аналізуючи вказані вище правопорушення, можна дійти висновку про те, що всі вони стосуються правил здійснення господарської діяльності. За вчинення вказаних правопорушень до винних осіб застосовуються заходи організаційно-правового або майнового характеру, спрямовані на припинення правопорушення суб'єкта господарювання та ліквідацію його наслідків (адміністративно-господарські санкції). В Законі України "Про електронний цифровий підпис" доцільно закріпити вказані вище правопорушення як юридичну підставу господарсько-правової відповідальності, яка проявляється у застосуванні до правопорушника адміністративно-господарських санкцій.

Розглядаючи обов'язки провайдерів сертифікаційних послуг, передбачені ч. 3 ст. 8 зазначеного вище Закону України, можна виділити групу обов'язків провайдерів, які випливають з вертикальних відносин останніх з уповноваженими державними органами, а саме обов'язки:

- забезпечувати захист інформації в автоматизованих системах відповідно до законодавства;
- забезпечувати захист персональних даних, отриманих від підписувача, згідно з законодавством;
- вести електронний перелік чинних, скасованих і блокованих сертифікатів ключів;

- забезпечувати зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері.

На нашу думку, належне виконання провайдером сертифікаційних послуг зазначених вище обов'язків є необхідною умовою здійснення останнім господарської діяльності у сфері надання послуг ЕЦП відповідно до чинного законодавства України та предметом контролю відповідних уповноважених державних органів.

Зокрема Закон України "Про захист інформації в автоматизованих системах" [1] (ст. 14) передбачає, що управління захистом інформації здійснюється уповноваженим Кабінетом Міністрів України органом. А тому в частині забезпечення провайдером сертифікаційних послуг захисту інформації в автоматизованих системах цей орган повинен за наявності правопорушення притягати винних осіб до господарсько-правової відповідальності з накладенням на них адміністративно-господарського штрафу.

Щодо решти зазначених вище обов'язків центральний засвідчувальний орган, уповноважений здійснювати державне регулювання у сфері надання послуг ЕЦП (ст. ст. 11–12 Закону України "Про електронний цифровий підпис"), повинен за наявності правопорушення притягати винних осіб до господарсько-правової відповідальності з накладенням на них адміністративно-господарського штрафу.

Крім того здійснення провайдером сертифікаційних послуг господарської діяльності у сфері надання ЕЦП без одержання відповідної ліцензії також повинно розглядатися як правопорушення, за вчинення якого винна особа повинна притягатися до господарсько-правової відповідальності у формі адміністративно-господарської санкції (зупинення чи анулювання дії ліцензії на здійснення провайдером сертифікаційних послуг відповідного виду господарської діяльності).

Окрім вище означених питань в законі України "Про електронний цифровий підпис" доцільно також передбачити застереження про те, що провайдер сертифікаційних послуг не несе відповідальності за будь-які збитки, спричинені використанням фальшивих чи підроблених електронних підписів, підтвердже-

них сертифікатом цього провайдера, якщо такий провайдер сертифікаційних послуг виконував вимоги даного закону відносно цього сертифіката[10].

На нашу думку, встановлення такої норми є необхідним, оскільки її закріплення дозволить захистити добросовісних провайдерів сертифікаційних послуг, особливо в умовах численних правових невизначеностей, викликаних недосконалістю закону України "Про електронний цифровий підпис", відсутності судової практики у сфері використання ЕЦП та відсутності достатньої практики діяльності провайдерів сертифікаційних послуг.

На підставі викладеного можна запропонувати такі доповнення до ст. 15 Закону України "Про електронний цифровий підпис":

"В разі невиконання або неналежного виконання провайдером сертифікаційних послуг зобов'язання він зобов'язаний відшкодувати підписувачу всі завдані цим збитки.

Виконання зобов'язання між провайдером сертифікаційних послуг та підписувачем може забезпечуватися згідно з законом або договором штрафом у певній визначеній грошовій сумі.

Провайдер сертифікаційних послуг не несе відповідальності за будь-які збитки, спричинені використанням фальшивих чи підроблених електронних цифрових підписів, підтверджених сертифікатом цього провайдера, якщо такий провайдер виконував вимоги даного закону відносно цього сертифіката.

Провайдер сертифікаційних послуг може передбачити у сертифікаті відкритого ключа ЕЦП обмеження на використання цього сертифіката, за умови, що такі обмеження визнаються третіми особами, в зв'язку з чим провайдер не несе відповідальності за збитки, що виникли внаслідок використання сертифіката відкритого ключа ЕЦП, яке виходить за межі, зазначені в такому сертифікаті".

Вважаємо за доцільне передбачати в договорах такі правопорушення, вчинення яких провайдером сертифікаційних послуг є підставою застосування до нього штрафу:

[10] Така норма міститься, наприклад, в законі Гонконгу "Про електронні правочини" (ст. 42).

1) несвоєчасне скасування, блокування та поновлення сертифікатів ключів;
2) недодавання до сертифіката відкритого ключа підписувача інформації про обмеження використання електронного цифрового підпису;
3) не перевірка законності звернень про скасування, блокування та поновлення сертифікатів ключів та не зберігання документів, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;
4) порушення обов'язку цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;
5) незабезпечення цілодобового доступу користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали.

Вчинення провайдером сертифікаційних послуг правопорушень "1, 5" може бути підставою застосування до останнього таких оперативно-господарських санкцій як відмова від оплати за зобов'язанням, яке виконане неналежним чином ("5"), та дострокове розірвання договору ("1").

Доцільним, також, є закріплення в законодавстві України положення про те, що підставою застосування до провайдера сертифікаційних послуг адміністративно-господарських санкцій повинно розглядатися вчинення останнім таких видів правопорушень:

1)здійснення господарської діяльності без отримання ліцензії або з порушенням вимог законодавства, зокрема:

а) порушення обов'язків по належному утриманню реєстраційних матеріалів;
б) невиконання або неналежне виконання обов'язків з забезпечення захисту інформації в автоматизованих системах відповідно до законодавства;
в) порушення обов'язку ведення електронного переліку чинних, скасованих і блокованих сертифікатів ключів;
г) порушення обов'язку зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством, для зберігання відповідних документів на папері.

2) відмова надати для перевірки журнали, реєстраційну та іншу документацію;

3) неповідомлення центрального засвідчувального органу про які-небудь факти, які не дозволяють належним чином здійснювати діяльність у відповідності з ліцензійними умовами;

4) невиконання або неналежне виконання обов'язків з забезпечення захисту персональних даних, отриманих від підписувача, згідно з законодавством.

Центральний засвідчувальний орган за вчинення провайдером сертифікаційних послуг правопорушень "1(a)" – "1(d)" повинен притягувати останнього до господарсько-правової відповідальності із застосуванням зупинення або анулювання дії ліцензії на здійснення провайдером сертифікаційних послуг господарської діяльності.

Центральний засвідчувальний орган за здійснення провайдером сертифікаційних послуг господарської діяльності без отримання ліцензії та вчинення ним правопорушень "2"–"3" повинен притягувати останнього до господарсько-правової відповідальності із застосуванням адміністративно-господарського штрафу.

Орган, уповноважений Кабінетом Міністрів України здійснювати управління захистом інформації, за вчинення провайдером сертифікаційних послуг правопорушення "4" повинен притягувати останнього до господарсько-правової відповідальності із застосуванням адміністративно-господарського штрафу.

Визначення в законодавстві України видів правопорушень, за вчинення яких наступає господарсько-правова відповідальність, визначення форм та меж такої відповідальності є доцільним та необхідним, оскільки це призведе до утвердження довіри до провайдерів сертифікаційних послуг, а у кінцевому результаті до швидкого запровадження в нашій державі електронної комерції світового рівня.

3.3. Проблеми державного регулювання діяльності провайдерів сертифікаційних послуг в Україні

Розвиток сучасних інформаційно-комунікаційних технологій, використання їх фізичними та юридичними особами для вдосконалення здійснюваної ними господарської діяльності, викликали таке явище, як електронна комерція. Відсутність правового регулювання у цій сфері може, перш за все, становити значну перепону для розвитку електронної комерції, а отже, і на шляху загального розвитку України, оскільки електронна комерція пропонує нашій державі можливості швидшого економічного розвитку та рівноправної конкуренції з державами, які набагато економічно більше розвинуті.

Однією з основних груп правовідносин, які складають електронну комерцію, є правовідносини у сфері створення та використання електронних цифрових підписів (ЕЦП). Врегулювати вказані відносини покликаний Закон України "Про електронний цифровий підпис". Основним суб'єктом цих правовідносин виступає провайдер сертифікаційних послуг.

Виключне значення інституту провайдерів сертифікаційних послуг в електронній комерції пов'язано з послугами, що надаються ним, а саме: надання у користування засобів ЕЦП; допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення); надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів; надання послуг фіксації часу; тощо.

Надання провайдерами вказаних послуг спрямоване на введення до господарського обігу ЕЦП, забезпечення високого рівня довіри до нього, що є основною умовою функціонування системи електронної комерції. Саме тому держава передбачає створення системи взаємодіючих провайдерів сертифікаційних послуг, покладає на них ряд обов'язків та вимог, яких вони повинні дотримуватися в процесі здійснюваної ними діяльності, а також передбачає створення та функціонування органів, на які

покладено обов'язок контролювати дотримання вимог чинного законодавства провайдерами сертифікаційних послуг.

Повноваження контролювати діяльність вказаних провайдерів поділені між двома органами – центральним засвідчувальним органом та контролюючим органом (ст. ст. 11–12 вказаного закону України "Про електронний цифровий підпис").

З метою засвідчення компетентності провайдера сертифікаційних послуг здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів, вищевказаним законом України, встановлена процедура акредитації, яку повинні пройти акредитовані центри сертифікації ключів ЕЦП та засвідчувальні центри (ст.ст. 9–10 Закону).

Відповідно до ст. 1 Закону акредитація розуміється як процедура документального засвідчення компетентності центра сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів. Вказане розуміння акредитації певною мірою відрізняється від традиційного розуміння акредитації, яке вживається у нормативних актах України [219–222], як офіційного визнання можливості певної особи чи органу здійснювати у визначений або невизначений строк певний виді діяльності, Частина 4 ст. 9 вказаного вище закону передбачає, що порядок акредитації та вимоги, яким повинен відповідати акредитований центр сертифікації ключів, встановлюються Кабінетом Міністрів України. Порядок проведення акредитації регламентований Порядком акредитації центру сертифікації ключів, затвердженим Постановою Кабінету Міністрів України № 903 від 13.07.2004 р.[11].

Використання самого терміна "акредитація" спирається на Директиву Європейського парламенту та Ради 1999/93/ЄС від 13 грудня 1999 р. "Про правові підстави Співдружності для використання електронних підписів", де у ст. 3 зазначено, що держави можуть вводити або дотримуватися системи добро-

[11] Дослідження змісту поняття «акредитація», який вживане вказаним нормативно-правовим актом, його співвідношення із поняттям «ліцензування» є дуже важливою, актуальною проблемою, та буде предметом окремої наукової праці.

вільної акредитації, спрямованої на підвищення рівня сертифікаційних послуг. При цьому під акредитацією в Директиві розуміється будь-який дозвіл, встановлення прав та обов'язків стосовно надання сертифікаційних послуг державним або приватним органом, відповідальним за надання таких прав та обов'язків, і здійснення нагляду на предмет відповідності їм в тому випадку, коли провайдер сертифікаційних послуг не уповноважений користуватися правами, що виникають з дозволу, до того, як він одержить рішення органу.

Вказане положення ст. 3 Директиви необхідно розглядати в зв'язку з положеннями, передбаченими ч. 3 цієї статті, якими на держави покладено обов'язок забезпечити створення достатньої системи, яка дозволяє здійснювати нагляд за діяльністю провайдерів сертифікаційних послуг, які засновані на їх території та видають кваліфіковані сертифікати[12]. Таким чином, Директива закріплює, що держави не повинні передбачати умовою надання провайдерами сертифікаційних послуг їх попередній дозвіл, але відносно створення ЕЦП Директива зобов'язує створювати наглядову систему, в контексті якої і розглядається поняття акредитації, зміст якої, зокрема, дуже близький до поняття ліцензування, яке використовується у законодавстві України.

Так, за Директивою, до початку здійснення діяльності провайдер сертифікаційних послуг повинен звернутися до уповноваженого органу за одержанням дозволу на здійснення діяльності з надання послуг сертифікації. Зважаючи на те, що Директива є типовим нормативним актом, який пропонує кожній окремій державі прийняти за основу її положення, вона не містить детальної регламентації процедури акредитації, її строків, тощо. До компетенції уповноваженого органу віднесе-

[12] Необхідно зазначити, що вказаною Директивою передбачено (ст. ст. 1, 5), що на вдосконалений електронний підпис (ЕЦП) видається кваліфікований сертифікат ключа підпису, на решту видів електронного підпису видається звичайний сертифікат ключа підпису. Таким чином, Директива у ст.3 ч. 3 запроваджує нагляд за діяльністю провайдерів сертифікаційних послуг, які видають кваліфіковані сертифікати на ЕЦП.

но здійснення нагляду щодо відповідності здійснюваної провайдером діяльності тим правам та обов'язкам, що випливають з одержаного дозволу. Отже, за Директивою акредитація, за змістом являє собою ліцензування, оскільки йдеться не тільки про одержання дозволу на здійснення певного виду діяльності на чітко визначених умовах, а й про постійний систематичний контроль з боку держави за дотриманням умов здійснення такого виду діяльності.

Однією з країн, яка прямо передбачила ліцензування діяльності провайдерів сертифікаційних послуг, пов'язаної з видачею та обслуговуванням сертифікатів відкритих ключів ЕЦП, є Німеччина. Так, закон Німеччини від 22 липня 1997 р. "Про цифровий підпис", який є складовою частиною закону Німеччини "Про регулювання основних умов надання інформаційних та комунікаційних послуг", у параграфі 2 встановлює, що провайдер сертифікаційних послуг (сертифікуючий центр) – це фізична або юридична особа, яка засвідчує зв'язок відкритих ключів з певною фізичною особою та має ліцензію. Здійснення ліцензування за даним законом покладено на Відомство телекомунікацій та пошти. Умовою одержання ліцензії є доведення здатності виконувати всі передбачені законом норми безпеки. Після одержання ліцензії орган, що ліцензує, зобов'язаний регулярно проводити перевірки дотримання провайдером вимог безпеки. Якщо буде встановлено, що провайдер не відповідає вимогам безпеки, та недоліки не будуть повністю усунені протягом встановленого строку, ліцензія може бути відкликана.

Ліцензування діяльності провайдерів сертифікаційних послуг передбачено і в інших країнах світу, зокрема законом Тунісу "Про електронне переведення коштів та електронну комерцію" (ст. 9), законом РФ "Про електронний цифровий підпис" (ст. 8) і законом РФ від 13.07.2001 р. "Про ліцензування окремих видів діяльності" (ч. 1 ст. 17) [223], тощо.

Послуги ЕЦП, які надають провайдери сертифікаційних послуг, а саме: надання у користування засобів цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів, надання інформації щодо

чинних, скасованих та блокованих сертифікатів ключів, послуги фіксування часу, консультації, тощо – є досить складними не тільки з технічної, але і з організаційної точки зору.

Таким чином, необхідно визначити ряд кваліфікаційних, організаційних та технологічних вимог, дотримання яких повинно бути необхідною умовою можливості здійснення діяльності провайдером сертифікаційних послуг. Так, провайдер сертифікаційних послуг для здійснення сертифікації відкритих ключів ЕЦП повинен бути укомплектований штатними спеціалістами, які відповідають за фахом даному виду діяльності та обсягу робіт; спеціалісти провайдера повинні мати відповідну професійну освіту та володіти необхідними для здійснення даного виду діяльності знаннями. Для провадження господарської діяльності в галузі сертифікації відкритих ключів ЕЦП провайдер повинен мати внутрішнє положення, де були б визначені підрозділ (підрозділи), які безпосередньо надаватимуть послуги ЕЦП, конкретні інструкції щодо порядку та правил надання таких послуг, функціональні обов'язки та кваліфікаційні вимоги до спеціалістів, їх відповідальність, тощо. Крім того, для здійснення провайдером сертифікації відкритих ключів ЕЦП він повинен мати певне приміщення та виробничі потужності (інформаційно-обчислювальні комплекси, ліцензійне програмне забезпечення, тощо); відповідні матеріальні та фінансові можливості, що дозволять йому нести відповідальність перед власниками сертифікатів ключів підписів за збитки, що можуть бути ним завдані через недостовірність відомостей, що містяться у сертифікатах ключів підписів.

Законодавство окремих країн світу вже закріпило організаційні та технічні вимоги до провайдерів сертифікаційних послуг. Так, Директива ЄС "Про електронні підписи" в додатку 2 містить вимоги, що висуваються законодавцем до провайдера сертифікаційних послуг, який обслуговує сертифікати ЕЦП, зокрема провайдери повинні:

1) демонструвати надійність, необхідну для того, щоб забезпечити послуги сертифікації;
2) гарантувати швидку дію та забезпечити безпечне та негайне обслуговування та скасування;

3) гарантувати, що дата та час, коли сертифікат було видано або скасовано, можуть бути визначені точно;
4) найняти персонал, який має експертні знання, досвід та кваліфікацію, необхідні для надання послуг сертифікації, та дотримуватися організаційних і адміністративних процедур, які є адекватними та відповідають визнаним стандартам;
5) використовувати надійні системи та програмне забезпечення, які захищені від модифікації та гарантують технічну та криптографічну безпеку процесів, пов'язаних з наданням сертифікаційних послуг;
6) мати достатні фінансові ресурси для забезпечення виконання обов'язків, покладених на них законодавством;
7) тощо.

Аналогічні за змістом вимоги до провайдерів сертифікаційних послуг закріплені й у ст. 7 закону Австрії "Про електронні підписи", в додатку 2 закону Ірландії від 10 липня 2000 р. "Про електронну комерцію" тощо.

Вищевикладене дозволяє дійти висновку щодо необхідності розроблення вичерпного переліку організаційних, кваліфікаційних та інших спеціальних вимог (ліцензійних умов), обов'язкових для надання провайдерами сертифікаційних послуг ЕЦП, тобто до необхідності запровадження режиму ліцензування діяльності провайдерів сертифікаційних послуг [224] (замість акредитації, як це передбачено законом), в порядку, передбаченому законом України "Про ліцензування певних видів господарської діяльності".

Законом України "Про електронний цифровий підпис" передбачено також здійснення контролю за дотриманням центральним засвідчувальним органом, засвідчувальними центрами та центрами сертифікації ключів вимог законодавства про ЕЦП, який покладено на контролюючий орган (ст. 12 вказаного закону) (функції якого покладені на спеціально уповноважений центральний орган виконавчої влади у сфері криптографічного захисту інформації, яким являється Департамент спеціальних телекомунікаційних систем та захисту інформації Служби Без-

пеки України), та центральний засвідчувальний орган (ст. 11 вказаного закону). Тобто функції контролю розподілені між двома органами – центральним засвідчувальним органом та контролюючим органом.

Так, ст. 11 вказаного закону передбачає, що Кабінет Міністрів України визначає центральний засвідчувальний орган. Вказаний орган безпосередньо не надає послуг ЕЦП, а покликаний забезпечувати діяльність системи провайдерів сертифікаційних послуг. До його компетенції відноситься формування та видача посилених сертифікатів провайдерам сертифікаційних послуг, їх блокування, скасування та поновлення, ведення електронних реєстрів чинних, блокованих та скасованих посилених сертифікатів ключів ЕЦП провайдерів сертифікаційних послуг, проведення акредитації відповідних провайдерів сертифікаційних послуг тощо[13].

Функціонування центрального засвідчувального органу тісно пов'язане з діяльністю контролюючого органу, до компетенції якого віднесене єдине повноваження – перевірка дотримання законодавства про електронний цифровий підпис провайдерами сертифікаційних послуг (ч. 2 ст. 12 вказаного закону). Дана стаття закону не роз'яснює, в чому полягає перевірка дотримання законодавства, яким чином це відбувається і які правові наслідки порушення законодавства у цій сфері.

Відповідно до ч. 3 ст. 12 вказаного закону у разі невиконання чи неналежного виконання обов'язків та виявлення порушень вимог, встановлених законодавством для центру сертифікації ключів, засвідчувального центру, контролюючий орган лише дає розпорядження центральному засвідчувальному органу про негайне вжиття заходів, передбачених законом. Необхідно зазначити, що вказаний закон не містить переліку таких заходів до осіб, що порушують законодавство про ЕЦП, не передбачає навіть підстав позбавлення акредитації провайдерів сертифікаційних послуг.

---

[13] Див.: Положення про центральний засвідчувальний орган, затверджене Постановою Кабінету Міністрів України № 1451 від 28.10.2004 р.

Можна стверджувати, що значення контролюючого органу зведено нанівець невизначеністю компетенції цього органу, відсутністю права вживати певних конкретних заходів до осіб, що порушують законодавство про ЕЦП, невизначеністю відповідальності таких осіб.

Розпорошеність функцій між контролюючим органом та центральним засвідчувальним органом, призведе до того, що жоден з них не зможе застосовувати конкретних заходів у випадку виявлення порушення законодавства у сфері використання ЕЦП. Крім того, виходячи з аналізу зазначеного закону, центральний засвідчувальний орган взагалі не підпорядкований контролюючому органу, і останній не може на нього впливати ніяким чином.

Дуже вдало, компетенція контролюючого органу (в даному випадку це Міністерство економіки) визначена у законі Словенії "Про електронну комерцію та електронні підписи" [225], який встановлює (ст. 40), що міністерство, проводячи контроль, має повноваження перевіряти: а) чи відображені відповідним чином положення даного закону у правилах внутрішнього розпорядку провайдера сертифікаційних послуг; б) чи дотримується провайдер протягом усього часу своєї діяльності вимог даного закону та правил свого внутрішнього розпорядку; в) контролювати законність видачі, зберігання і анулювання сертифікатів; г) контролювати законність надання інших послуг провайдером сертифікаційних послуг. Вказане міністерство веде державний електронний реєстр усіх провайдерів сертифікаційних послуг Словенії.

Зазначений закон Словенії (ст. 41) уповноважує інспектора Міністерства економіки проводити перевірку документації та файлів, які відносяться до сфери діяльності провайдера сертифікаційних послуг; проводити інспекцію приміщень, в яких надаються послуги з сертифікації, інформаційних технологій, інфраструктури та іншого технічного обладнання і документації провайдерів; контролювати порядок роботи і заходи провайдерів сертифікаційних послуг. Інспектор має право на конфіскацію документації терміном до 15 днів, якщо це необхідно для

забезпечення доказів або для точного встановлення невідповідності. На підставі здійсненої перевірки інспектор може (ч. 4 ст. 41): заборонити використання незаконного порядку роботи і інфраструктур; призупинити діяльність провайдера частково або повністю; заборонити діяльність провайдера сертифікаційних послуг, якщо він не дотримується вимог закону, і, якщо попереджувальні заходи не мали потрібного результату або не могли його мати, вимагати анулювання сертифіката, коли є причини вважати, що сертифікат був підроблений.

Таким чином, здійснення ефективного контролю за діяльністю провайдерів сертифікаційних послуг у сфері здійснення сертифікації відкритих ключів ЕЦП повинно ґрунтуватися на функціонуванні єдиного державного органу, який буде об'єднувати в своїй компетенції повноваження, передбачені законом для центрального засвідчувального органу та контролюючого органу, а також містити реальні заходи впливу на провайдерів сертифікаційних послуг, що порушують законодавство про ЕЦП, встановлювати порядок притягнення таких осіб до відповідальності.

Отже, доцільним є створення та функціонування єдиного, підпорядкованого центральному органу виконавчої влади, державного органу з чітко окресленою компетенцією, яка охоплювала б повноваження по регулюванню та контролю за діяльністю провайдерів сертифікаційних послуг, по застосуванню реальних заходів впливу на осіб, що порушують законодавство про ЕЦП, а саме: по формуванню та видачі сертифікатів провайдерам сертифікаційних послуг; їх блокуванню, скасуванню та поновленню; по веденню державного електронного реєстру чинних, блокованих та скасованих посилених сертифікатів ключів ЕЦП провайдерів сертифікаційних послуг та забезпеченню доступу до них; по проведенню ліцензування провайдерів сертифікаційних послуг; контролю за дотриманням ними ліцензійних умов; призупиненню, поновленню та анулюванню ліцензії; по видачі підзаконних нормативних актів, що встановлюють стандарти та методику надання провайдерами послуг ЕЦП, та контролю за їх виконанням; по наданню консультацій та розробці методичної літератури щодо порядку надання послуг ЕЦП, тощо.

На підставі викладеного можна зробити ряд висновків: так, доцільним є створення одного виду провайдерів сертифікаційних послуг, уповноваженого надавати послуги ЕЦП всім зацікавленим особам; до Закону України "Про електронний цифровий підпис" (відповідно і до закону України "Про ліцензування певних видів господарської діяльності") було б доцільним внести зміни, передбачивши процедуру ліцензування діяльності провайдерів сертифікаційних послуг, розробити ліцензійні умови здійснюваної ними діяльності та передбачити єдиний державний орган, який би здійснював державне регулювання та контроль за діяльністю провайдерів сертифікаційних послуг, компетенція якого повинна передбачати застосування реальних заходів по усуненню правопорушень законодавства в цій сфері.

Запровадження даної моделі державного регулювання відносин у сфері використання ЕЦП в Україні дозволить здійснити захист інформаційної безпеки держави, забезпечити здійснення єдиної державної політики у сфері відносин, пов'язаних з використанням ЕЦП, координувати діяльність провайдерів сертифікаційних послуг, розвивати підприємництво та конкуренцію, дозволить забезпечити високий рівень якості послуг ЕЦП.

Резюмуючи викладене, зробимо висновки. Так, один з блоків правовідносин, що складаються у сфері електронної комерції, являє собою правовідносини щодо використання ЕЦП. Регулювання даних правовідносин доцільно здійснювати на підставі загального закону України "Про електронну комерцію", прийняти який необхідно, та спеціального закону України від 22 травня 2003 р. "Про електронний цифровий підпис".

Загальний закон "Про електронну комерцію" повинен закріплювати ряд загальних положень, пов'язаних із використанням ЕЦП для здійснення правочинів через мережі електрозв'язку. Зокрема, в електронній комерції повинно допускатися використання всіх передбачених законодавством України видів електронного підпису; електронний підпис не повинен визнаватися недійсним та таким, що не відповідає власноручному

підпису, лише з тих підстав, що він представлений електронним документом та не ґрунтується на сертифікаті.

Частину 1 ст. 3 Закону України від 22 травня 2003 р. "Про електронний цифровий підпис" "правовий статус електронного цифрового підпису" доцільно доповнити ще однією умовою, дотримання якої є необхідним для визнання ЕЦП рівнозначним власноручному підпису: правомірне володіння закритим ключем ЕЦП особою, яка підписала електронний документ ЕЦП.

При створенні ЕЦП повинні використовуватися лише такі засоби ЕЦП, які мають сертифікат відповідності або позитивний висновок державної експертизи в галузі криптографічного захисту інформації. До Порядку проведення сертифікації засобів криптографічного захисту інформації від 15 грудня 1999 р., затвердженого Комітетом України з питань стандартизації, метрології та сертифікації, доцільно внести зміни та чітко визначити обсяг повноважень органу із сертифікації засобів КЗІ.

Положення вказаного закону України, що встановлюють вимоги до сертифікатів відкритих ключів ЕЦП, права та обов'язки їх володільців та користувачів відкритих ключів ЕЦП, обов'язки провайдерів сертифікаційних послуг відносно володільців сертифікатів відкритих ключів ЕЦП, є необхідні та достатні для правового регулювання використання ЕЦП в цій частині.

Провайдери сертифікаційних послуг (центри сертифікації, акредитовані центри сертифікації, засвідчувальні органи, центральний засвідчувальний орган) є юридичними особами, створеними в порядку, передбаченому чинним законодавством України, мають необхідні матеріальні і фінансові можливості, що дозволяють їм нести відповідальність перед володільцями та користувачами сертифікатів ключів підписів за збитки, що можуть бути понесені ними внаслідок недостовірності відомостей, що містяться в сертифікатах ключів підписів.

У вказаному законі України доцільно виключити положення про акредитацію та передбачити ліцензування діяльності провайдерів сертифікаційних послуг. В цій частині відповідні зміни повинні бути внесені і в закон України "Про ліцензуван-

ня певних видів господарської діяльності". Крім того, доцільно розробити ліцензійні умови надання провайдерами послуг сертифікації відкритих ключів ЕЦП, які б містили кваліфікаційні, організаційні та технологічні вимоги до провайдерів, що надають такі послуги.

Провайдер сертифікаційних послуг до початку використання ЕЦП уповноваженої особи провайдера сертифікаційних послуг для засвідчення сертифікатів ключів підписів повинен одержати у центральному засвідчувальному органі сертифікат ключа підпису уповноваженої особи провайдера сертифікаційних послуг у вигляді електронного документа.

Частину 2 ст. 11 вказаного Закону України "центральний засвідчувальний орган" доцільно доповнити, включивши до компетенції центрального засвідчувального органу обов'язок ведення єдиного загальнодержавного реєстру сертифікатів, що видані в Україні, таким чином, щоб одержання сертифіката відкритого ключа ЕЦП у будь-якого з провайдерів на території України автоматично відбивалося у такому реєстрі.

Електронні цифрові підписи уповноважених осіб провайдерів сертифікаційних послуг повинні використовуватися тільки після включення їх до єдиного державного реєстру сертифікатів ключів підписів. Використання таких ЕЦП повинно пов'язуватися виключно з метою посвідчення сертифікатів ключів підписів і відомостей про їх дію.

Передбачувана Законом України від 22 травня 2003 р. "Про електронний цифровий підпис" система провайдерів сертифікаційних послуг є недоцільно ускладненою та розгалуженою. Тому, необхідно передбачити існування одного виду провайдерів сертифікаційних послуг, уповноважених видавати сертифікати відкритих ключів підписів всім зацікавленим особам. Захист державних інтересів у сфері використання ЕЦП може бути забезпечений шляхом передбачення обов'язку центральних органів державної влади та місцевого самоврядування, підприємств, установ та організацій, їм підпорядкованих, використовувати тільки такий вид електронного підпису, як ЕЦП.

Повноваження з державного регулювання відносин у сфері використання ЕЦП в Україні недоцільно розподіляти між двома органами – контролюючим органом та центральним засвідчувальним органом. В Законі України "Про електронний цифровий підпис" необхідно передбачити єдиний орган (центральний засвідчувальний орган), який би здійснював державне регулювання діяльності провайдерів сертифікаційних послуг.

Провайдер сертифікаційних послуг та інші суб'єкти правових відносин у сфері створення та використання ЕЦП несуть відповідальність за дії, що призвели чи завдали шкоди юридичним або фізичним особам, згідно із законодавством.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Відомості* Верховної Ради України. – 1994. – № 31. – Ст. 286.
2. Концепція створення організованого ринку обігу цінних паперів високотехнологічних підприємств України, затверджена Рішенням Державної комісії з цінних паперів та фондового ринку від 3 січня 2002 року № 2 // Офіційний вісник України. – № 4. – С. 476. – Ст. 154 від 07.02.2003.
3. *Положення* «Про ввезення на митну територію України окремих видів товарів», затверджене Постановою Кабінету Міністрів України від 29.03.2002 № 390 // Урядовий кур'єр № 63 від 03.04.2002.
4. *Указ Президента* України від 31 липня 2000 р. № 928 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» // Урядовий кур'єр від 8.08.2000.
5. *Див.*: http://dogovor.adgrafics.net/dodatok_2.php?adgrafics=pp
6. Інструкція "Про порядок та умови одержання інформації з інформаційного фонду Єдиного державного реєстру нормативно-правових актів", затверджена Наказом Міністерства юстиції України від 26 червня 2002 року N 57/5 // Офіційний вісник України. – № 27. – С. 271. – Ст. 1306 від 19.07.2002.
7. Бенеско Г. С электронным бизнесом – в третье тысячелетие //http://www.osp.ru/ecom/2001/01/044.htm
8. *UNCITRAL* Draft Model Law on Electronic Commerce // http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm
9. *Климович Л.* Электронная коммерция в интернационализации предпринимательской деятельности. – Белорусский журнал международного права и международных отношений. – 2003. – № 1. – С. 12–16.
10. *Кулешов М.* Развитие электронной торговли в России и правовое обеспечение // http://www.ice.ru/exp/20362
11. *Царев В.В., Кантарович А.А.* Инфраструктура системы электронной коммерции // http://www.rsoft.ru/koi-8/most/reviews/ob11_01.htm
12. *Гозалан М.* Е-метаморфозы деловой среды // http://www.bizon.ru/viewarticle.phtml?id=53
13. *Сериков С.* Автогиганты на виртуальных шасси // http://www.bizon.ru/viewarticle.phtml?id=135
14. *Баско Ф.* B2B в России: проблемы и перспективы. – eCommerce World. – 2001. – № 3.
15. *Семенов А.* Электронная коммерция в Европе жива и здорова // http://www.bizon.ru/viewarticle.phtml?id=479
16. *Семенов А.* Иного пути у нас просто нет // http://www.bizon.ru/viewarticle.phtml?id=20
17. *Форт П.* Конкурентная борьба за европейский рынок электронной коммерции обостряется // http://www.bizon.ru/viewarticle.phtml?id=58
18. *UNCITRAL* Model Law on Electronic Signatures // http://www.uncitral.org/english/sessions/unc/unc-34/acn-493e.pdf
19. *Directive* 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic

commerce, in the Internal Market (Directive on electronic commerce) // Official Journal of the European Communities. – 2000. – L 178.
20. *Directive* 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures (Electronic Signatures Directive) // Official Journal of the European Communities. – 1999. – L13.
21. *Electronic* Communications Act of UK, of May 15, 2000 // http://www.uk-legislation.hmso.gov.uk/acts/acts2000/20000007.htm
22. *The Electronic* Signatures Regulations Act of UK, of February 13, 2002 // http://www.legislation.hmso.gov.uk/si/si2002/20020318.htm
23. *Закон* штату Юта США від 1.05.1995 р. "Про електронний підпис" // http://www.le.state.ut.us/~code/TITLE46/46_03.htm
24. *Uniform* Electronic transactions Act, State of Utah, of July 3, 2000 // http://www.le.state.ut.us/~2000/htmdoc/sbillhtm/SB0125.htm
25. *Electronic* Transaction Act of Singapure, of June 29, 1998 // http://www.cca.gov.sg/eta/framecontent.html
26. *The Electronic* transaction Bill of Australia, 1998-1999 // http://scaleplus.law.gov.au/html/pasteact/3/3328/top.htm
27. *Electronic* Transactions Ordinance of Hon-Kong, of January 7, 2000 // http://www.bmck.com/hongkong-t.htm#eto
28. *An Electronic* Commerce Act of Ireland, of July 10, 2000 // http://www.bmck.com/ireland-t.htm#ecb
29. *An Act* providing for the recognition and use of electronic commercial and non-commercial transactions and documents, penalties for unlawful use thereof and for other purposes of Philippines, of June 14, 2000 // www.bmck.com/Philippine%20E-Com%Law.doc
30. *The Electronic* Exchanges and Electronic Commerce Bill of Tunisia, of August 9, 2000 // http://www.bmck.com/Tunisian%20National%20Certification%20Agency.pdf
31. *Electronic* Commerce Act of Luxembourg, of Augest 14, 2000 // http://www.etat.lu/OLAS/docs/ComelecEN.pdf
32. *Модельний* закон Міжпарламентської асамблеї країн-учасниць СНД від 09.12.2000 року "Про електронний цифровий підпис" // Информационный бюллетень. СПб. – 2001. – № 26. – 310 с.
33. *Закон* Італійської Республіки від 01.03.1997 року "Закон Басаніні" // http://www.bmck.com/italy-t.htm#21
34. *Хозяйственный* кодекс Украины: Комментарий. – Х.: ООО «Одиссей», 2004. – 895 с.
35. Federal Electronic Signature Law of Austria, of August 19, 1999 // http://www.bmck.com/ecommerce/austrianesig.pdf
36. *Федеральний* Закон США від 1.10.2000 року "Про електронні підписи у міжнародних та внутрішньодержавних торгових відносинах" // http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:s761enr.txt.pdf
37. *Закон* Російської Федерації від 10.01.2002 року "Про електронний цифровий підпис"// www.russianlaw.net/law/laws/t18.htm.
38. *Закон* Туркменістану від 19.12.2000 року "Про електронний документ"// http://law/intergroup.ru/infolaw/zakon/phtml?file=turk
39. *Закон* Республіки Бєларусь від 10.01.2000 року "Про електронний документ" // http://law/intergroup.ru/infolaw/zakon/phtml?file=belarus

40. *Господарський* кодекс України. – К.: Атіка, 2003. – 208 с.
41. *Цивільний* кодекс України. – К.: Атіка, 2003. – 416 с.
42. *Закон* України від 05.04.2001 року "Про платіжні системи та переказ грошей в Україні"// Відомості Верховної Ради України. – 2001. – № 29. – Ст.137.
43. *Закон* України від 09.04.1999 року "Про обов"язковий примірник документів" // Відомості Верховної Ради. – 1999. – № 22–23. – Ст. 199.
44. *Закон* України від 02.10.1992 року "Про інформацію" // Відомості Верховної Ради. – 1992. – № 48. – Ст. 650.
45. *Інструкція* "Про безготівкові розрахунки в Україні в національній валюті", затверджена Постановою Правління НБУ № 135 від 29.03.2001 року в редакції 04.12.2001 року // Офіційний вісник України. – № 18. – Т. 2. – С. 848. – Ст. 794 від 18.05.2001.
46. *Інструкція* "Про міжбанківські розрахунки в Україні", затверджена Постановою Правління НБУ України № 621 від 27.12.1999 року в редакції 23.04.2002 року // Офіційний вісник України. – № 5. – С. 134. – Ст. 181 від 18.02.2000.
47. *Правила* організації захисту електронних банківських документів, затверджені Постановою Правління НБУ № 280 від 10.06.1999 року // Офіційний вісник України. – № 35. – С. 92 від 17.09.1999.
48. *Закон* України від 22.05.2003 року "Про електронний цифровий підпис" // Урядовий кур'єр, № 119, від 02.07.2003 року.
49. *Закон* України "Про електронні документи та електронний документообіг"// Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275.
50. *Закон* України "Про телекомунікації" // Голос України N 244 від 23.12.2003.
51. *Закон* України від 16.05.1995 року "Про зв'язок" // Відомості Верховної Ради, 1995. – № 20. – Ст. 143.
52. *Законопроект* України від 17.02.2003 року "Про електронну торгівлю" № 3114 // http://oracle2.rada.gov.ua/pls/zweb/webproc4_1?id=&pf3511=14256http://oracle2.rada.gov.ua/pls/zweb/webproc4_1?id=&pf3511=14256
53. *Стоуньер Т.* Информационное богатство: профиль постиндустриальной экономики // Новая технократическая волна на Западе. – М.: Прогресс, 1986. – 420 с.
54. *Ракитов А.И.* Наш путь к информационному обществу // Теория и практика общественно-научной информации. – М.: ИНИОН, 1989. – С. 12–14.
55. *Чесноков А.Г.* Системная организация информационных технологий и их влияние на развитие и повышение эффективности субъектов экономической деятельности: Автореф. дис. док. экон. наук. – М., 1998. – 35 с.
56. *Бастрикова С.А.* Интернет в системе взаимодействия государства и формирующегося гражданского общества Российской Федерации: Дис. канд. политол. наук. – М., 2000. – 145 с.
57. *Василенко Л.А.* Интернет в информатизации государственного управления. Социолого-методологический анализ: Дис. д-ра социол. наук. – М., 2000. – 323 с.
58. *Копылов В.А.* Информационное право. – М.: Юристъ, 1997. – 512 с.
59. *Степанов Е.Б.* Информация как фактор производства: Автореф. дис. канд. экон. наук. – Кострома, 2000. – 21 с.
60. *Громов Г.Р.* Очерки информационной технологии. – М.: ИнфоАрт, 1993. – 336 с.
61. *Дрыганов В.* Основные аспекты правового регулирования электронной коммерции в Беларуси и за рубежом // www.russianlaw.net/law/doc/a116.htm.

62. *Статистичні* дані Інституту сертифікованих консультантів з електронної комерції про кількісні показники розвитку електронної комерції / текст знаходиться за адресою: www. teleor.net/e-commerce/e-commerce2.html
63. *Семенов А.* Электронная торговля в мире и России // http://www.bizon.ru/viewarticle.phtml?id=78
64. *Мелюхин И.С.* Информационное общество: истоки, проблемы, тенденции развития. – М.: МГУ, 1999. – 208 с.
65. *Петровский С. В.* Правовое регулирование оказания Интернет-услуг. Дис. канд. юрид. наук. М. 2002. – 204 с.
66. *Англо-русский* словарь по сетям и сетевым технологиям / Сост. С.Б. Орлов – М.: Солон, 1997. – 302 с.
67. *Пастухов О.М.* Авторське право у сфері функціонування всесвітньої інформаційної мережі Інтернет: Автореф. дис. канд. юр. наук. – К., 2002. – 18 с.
68. *Острейковский В.А.* Информатика. – М.: Высшая школа, 2000. – 511 с.
69. *Малахов С.В.* Гражданско-правовое регулирование отношений в глобальной компьютерной сети Интернет: Автореф. дис. канд. юр. наук. – М., 2001. – 21 с.
70. *Малахов С.В.* Гражданско-правовое регулирование отношений в глобальной компьютерной сети Интернет: Дис. канд. юр. наук. – М., 2001. – 173 с.
71. *Бабенко В.С.* Две книги о виртуальной реальности // Труды Лаборатории виртуалистики Института проблем человека РАН. – М.: Институт проблем человека РАН, 1997. – № 3. – С. 85.
72. *Талимончик В.П.* Международно-правовое регулирование отношений информационного обмена в Интернет. Дис. канд. юр. наук. – СПб., 1999. – 430 с.
73. *Постанова* Вищого арбітражного суду України від 27.03.2001 року № 04-1/11-7/60 «Про деякі питання застосування електронної форми правочинів» // Вісник господарського судочинства. – 2001. – № 3. – С. 171–174.
74. *Листи* Вищого Арбітражного Суду РФ від 24.04.1992 року К-3/96, від 19.08.1994 р. С1-7/оп-578, від 07.06.1995 року С1/ОЗ-316 // http://www.russianlaw.net/law/cases/case_crypto_lancrypto.htm
75. *Наумов В.* Год прошел // http://www.ibusiness.ru/offline/2002/192/15385/
76. *Серго А.* Правовое регулирование электронной коммерции // http://www.rol.ru/news/it/legal/interview.htm
77. *Указ* Президента України від 22 січня 2000 року "Про запровадження єдиної державної регуляторної політики у сфері підприємництва" № 89/2000 // Урядовий кур'єр від 25.01.2000
78. *Законопроект РФ* від 12.01.2001 року "Про електронну торгівлю" № 47432-3/ / http://www.e-commerce.ru/legasp/projets/e_trading/index.html
79. *Законопроект РФ* від 16.11.2000 року "Про правочини, що вчиняються за допомогою електронних засобів (Про електронні правочини)" № 27813-3// http://www.russianlaw.net/law/acts/z6.htm
80. *Баранов А.* Цифровое законодательство. – К., Зеркало недели. – № 20 (395) от 01.06.2002 г.
81. *Міщенко В.* Правове регулювання розвитку ринку фінансових послуг на основі електронної комерції.- К., Підприємництво, господарство і право. – 2002. – № 11. – С. 70-74.
82. *Громов Д.Е.* Электронная коммерция: развитие в России. Социальные проблемы права: сборник статей. – Выпуск второй. – М., 2001. – С. 140–148.

83. *Соловяненко Н.И., Ларин В.В., Лебедев А.Н.* Правовое регулирование заключения сделок на современном этапе / http://vlarin.chat.ru./larin/diplom.htm;
84. *Шамраев А.* Развитие европейского права электронной коммерции // www.e-management.ru/e-law-euro.htm;
85. *Стах А., Емельянова (Лукашевич) Т.* Правовое регулирование электронной торговли на территории Республики Беларусь // Бюллетень нормативно-правовой информации. – 2002. – № 12. – С. 36-42.
86. *Степаненко Е.* Электронная коммерция в России. Основные вопросы. / Хозяйство и право. – М., 2000. – № 12. – С. 23-37.
87. *Кульченко М.В.* Роль электронной коммерции в современных международных экономических отношениях: Автореф. дис. канд. екон. наук. – М., 1999. – 25 с.
88. *Соловяненко Н.И.* Перспективы российского законодательства об электронной коммерции / http://www.ice.ru/exp/20371
89. *Балабанов І.Т.* Інтерактивний бізнес. – СПб. – 2001. – 342 с.
90. *Operkent A.* Global Economy & Electronic Commerce. – London: Business School Press, 1999.
91. *Новомлинский Л.* «Электронная пара»: бизнес и коммерция // http://www.bizon.ru/viewarticle.phtml?id=222
92. *Комментарий* к гражданскому кодексу Российской Федерации, части первой (постатейный). Руководитель авторского коллектива и ответственный редактор доктор юридических наук, профессор О.Н. Садиков. – М.: Юридическая фирма КОНТРАКТ; ИНФРА-М, 1997. – 790 с.
93. *Дутов М.М.* Правове забезпечення розвитку електронної комерції: Автореф. дис. канд.. юрид. наук. – Донецьк, 2003. – 17 с.
94. *Тедеев А.А.* Правовые проблемы развития электронной коммерции: пробелы в праве и пробелы налогообложения // Юрист, М. – 2002. – № 5.
95. *Наумов В.* Ключевые вопросы государственного регулирования Интернет-коммерции в РФ // http://www.ice.ru/exp/20302
96. *Скородумов Б.* Писать или не писать ... Вот в чем вопрос! // http://www.bizon.ru/viewarticle.phtml?id=369
97. *Положення* "Про порядок емісії платіжних карток і здійснення операцій з їх застосуванням", затверджене Постановою Правління Національного банку України від 24.09.1999 р. № 479 // Офіційний вісник України. – N 47. – С. 84 від 10.12.1999.
98. *Шамраев А.* Введение в право электронной коммерции // Бизнес-онлайн. – 2000. – № 4.
99. *Орлов А., Ананьев А.* Во Всемирной Торговой Организации нет согласия по электронной торговле // iBusiness. – М., 2001. – № 1–2.
100. *Шамраев А.* Апейрон // http://www.bizon.ru/viewarticle.phtml?id=427
101. *Беляневич О.А.* Господарський договір та способи його укладання. Дис. канд. юрид. наук. – Київ, 1999. – 173 с.
102. *Роз'яснення* Вищого Господарського Суду України № 02-5/111 від 12.03.1999 р. "Про деякі питання практики вирішення спорів, пов'язанних з визнанням правочинів недійсними" // Вісник Вищого арбітражного суду України. – 1999. – № 2.
103. *Роз'яснення* ВАСУ від 06.10.1994 р. № 02-5/706 з наступними змінами та доповненнями "Про окремі питання практики вирішення спорів, пов'язаних з

укладанням та виконанням кредитних договорів". Арбітражне судочинство. Збірник нормативних актів ВАСУ. – Харків, 1999. – 558 с.
104. *Роз'яснення* ВАСУ від 28.04.1995 року № 02-5/302 з наступними змінами та доповненнями "Про деякі питання практики вирішення спорів, пов'язаних з укладанням та виконанням договорів про спільну діяльність" // Арбітражне судочинство. Збірник нормативних актів ВАСУ. Харків, 1999. – 558 с.
105. *Брагинский М.И.* Общее учение о хозяйственных договорах. – Минск: Наука и Техника, 1967. – 259 с.
106. *Вершинин А.П.* Электронный документ: правовая форма и доказательство в суде. – М.: Городециздат, 2000. – 242 с.
107. *Дутов М.* Правові проблеми електронного документа// Підприємництво, господарство і право. – 2002. – № 4. – С. 33–35.
108. *Дутов М.* Правові проблеми електронного документообігу// Право України. – 2002. – № 6. – С. 122–124.
109. *Дутов М.* Сравнительный анализ европейского законодательства в области электронного документооборота // Підприємництво, господарство і право. – 2002. – № 8. – С. 25–28.
110. *Марченко А.* Предварительные соображения к построению законодательной основы широкого применения электронных средств связи // http://www.ice.ru/exp/20316
111. *Бірюков В.* Письмові правочини за законодавством Польщі // Підприємництво, господарство і право. – 2003. – № 4. – С. 79–81.
112. *Шамраев А.* Концепція закона об электронном документе // http://www.ice.ru/exp/20318.
113. *Завидов Б.Д.* Электронная цифровая подпись. Правовое значение // Экзамен. Москва. – 2001. – 21 с.
114. *Вихорев С.* Закон об ЕЦП принят. Что дальше ? // http://www.cio-world.ru/bsolutions/analytics/21889/
115. *Информатика* для юристов и экономистов / Под ред. С.В. Симоновича и др. – СПб.: Питер, 2001. – 687 с.
116. *Рабинович П.М.* Основи загальної теорії права та держави. – К., 1994. – 236 с.
117. *Господарське* право. Практикум. Під заг. ред. В.С. Щербини – К.: Юрінком Інтер. – 2001. – 319 с.
118. *Жилинкова И.* Договор о предоставлении услуг доступа в Интернет / Підприємництво, господарство і право. – К. – 2002. – № 11. – С. 3–6.
119. *Хозяйственное* право: Учебник / Под ред. В.В. Лаптева – М.: Юрид. лит., 1983. – 527 с.
120. *Беляневич О.А.* Господарський договір та способи його укладання. Навчальний посібник. – К.: Наукова думка., 2002. – 279 с.
121. *Соловяненко Н.* Разработка проекта Федерального закона РФ «Об электронной торговле» // eCommerce World. – 2000. – № 8.
122. *Соловяненко Н.* Приоритеты законодательства в области электронной коммерции // eCommerce World. – 2000. – № 1.
123. *Руководство* по принятию типового закона Юнситрал «Об електронной коммерции» // http://www.uncitral.org/en-index.htm
124. Законопроект РФ від 27.06.2001 р. "Про електронний документ" № 107599-3 // http://www.ice.ru/exp/112577

125. *Конституція* України // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
126. *Закон* України від 14.05.1992 року "Про відновлення платоспроможності боржника або визнання його банкрутом" (в редакції закону України від 30.06.1999 року) // Урядовий Кур'єр. – 1999. – 19 вересня.
127. *Закон* України від 01.06.2000 року "Про ліцензування певних видів господарської діяльності" // Відомості Верховної Ради України. – 2000. – № 36. – Ст. 299.
128. *Положення* "Про порядок здійснення криптографічного захисту інформації в Україні", затверджене Указом Президента України від 22.05.1998 р. № 505/98 в редакції 27.09.1999 р. // Урядовий кур'єр від 09.07.1998.
129. *Положення* "Про Департамент спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України", затверджене Указом Президента України від 06.10.2000 року № 1120/2000 // Офіційний вісник України. – № 41. – С. 46. – Ст. 1745 від 27.10.2000.
130. *Ліцензійні* умови провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівлі і засобами криптографічного захисту інформації, затверджені Спільним наказом Державного комітету України з питань регуляторної політики та підприємництва і Департаменту Спеціальних телекомунікаційних систем та захисту інформації СБУ від 29.12.2000 року № 88/66 // Офіційний вісник України. – № 4. – С. 289. – Ст. 154 від 09.02.2001.
131. *Порядок* контролю за додержанням ліцензійних умов провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівлі криптосистемами і засобами криптографічного захисту інформації, затверджений наказом Державного комітету України з питань регуляторної політики та підприємництва і Департаменту Спеціальних телекомунікаційних систем та захисту інформації СБУ від 12.12.2001 року № 151/72 // Офіційний вісник України. – № 52. – С. 453. – Ст. 2406 від 11.01.2002.
132. *Положення* "Про державну експертизу у сфері криптографічного захисту інформації", затверджене Наказом Департаменту Спеціальних телекомунікаційних систем та захисту інформації СБУ від 25.12.2000 року № 62 // Офіційний вісник України. – N 3. С. 397. – Ст. 89 від 02.02.2001.
133. *Сафиулин Д.Н.* Хозяйственный договор : Общие положения. – Свердловск: Свердловский юридический институт им. Руденко, 1986. – 72 с.
134. *Брагинский М.И., Витрянский В.В.* Договорное право. Книга первая: Общие положения. – М.: Статут, 2001. – 841 с.
135. *Вердников В.Г.* Хозяйственные договоры. – М.: ВЮЗИ, 1965. – 118 с.
136. *Лаптев В.В.* Предмет и система хозяйственного права. – М.: Юрид. лит., 1969. – 176 с.
137. *Луць В.В.* Господарські договори. – Львів: Вид – во Львівського ун – ту, 1973. – 28 с.
138. *Можейко В.Н.* Хозяйственный договор в СССР. – М.: Госюриздат, 1962. – 240 с.

139. *Овчинников Н.И.* Понятие и классификация хозяйственных договоров. – Владивосток: Изд-во Дальневосточного ун-та, 1970. – 160 с.
140. *Побирченко И.Г.* Хозяйственная юрисдикция (общее учение). – К.: РИО МВД УССР, 1973. – 252 с.
141. *Брагинский М.И.* Хозяйственный договор: каким ему быть? – Москва: Экономика, 1990. – 175 с.
142. *Сафиуллин Д.Н.* Теория и практика правового регулирования хозяйственных связей в СССР. – Свердловск: Изд-во Уральского университета, 1990. – 139 с.
143. *Шелестов В.С.* Хозяйственные договоры: Конспект лекций для студентов Харьковского юридического института. – Харьков, 1965. – 43 с.
144. *Див.:* http://www.kreditprombank.com/kpbrus.nsf/CorpServiceFull/4D106F92772B9406 C225699E002D9450!OpenDocument
145. *Агарков М. М.* Обязательство по советскому гражданскому праву. – М.: Юриздат, 1940. – 192 с.
146. *Венедиктов А.В.* Государственная социалистическая собственность. – М., Изд-во АН СССР, 1948. – 839 с.
147. *Иоффе О.С.* План и договор в социалистическом хозяйстве. – М.: Юрид. лит., 1971. – 216 с.
148. *Калмыков Ю.Х.* Правовое регулирование хозяйственных отношений. – Саратов: Изд – во Саратовского университета, 1982. – 204 с.
149. *Танчук И.А., Ефимочкин В.П., Абова Т.Е.* Хозяйственные обязательства. – М.: Юрид. лит., 1970. – 216 с.
150. *Халфина Р.О.* Значение и сущность договора в советском гражданском праве. – М.: АН СССР, 1954. – 240 с.
151. *Гражданское* право. Том 1. / Под ред. Суханова Е.А. – М.: Изд-во БЕК, 2002. – 785 с.
152. *Иоффе О.С.* Советское гражданское право. Т. 1. – Л., 1958. – 478 с.
153. *Шахматов В.П.* Составы противоправных сделок и обусловленные ими последствия. – Томск, 1967. – 158 с.
154. *Круглова Н.Ю.* Хозяйственное право. – М.: Русская Деловая Литература, 1997. – 604 с.
155. *Леонович Е.* Электронный документ: скромное настоящее, большое будущее // Бюллетень нормативно-правовой информации. – 2001. – № 8. – С. 9–15.
156. *Литовко С.* Оформление договоров: печать, подпись и реквизиты. // Бюллетень нормативно-правовой информации. – 2001. – № 35. – С. 42–27.
157. *Кодекс* торговельного мореплавства від 23 травня 1995 року // Відомості Верховної Ради. – 1995. – № 47–52. – Ст. 349.
158. *Ананько А.* Электронная форма сделки в международной торговле // http://www.russianlaw.net/law/doc/a124.htm
159. *Украинский* советский энциклопедический словарь. В 3 т./ Главная редакция Украинской Советской Энциклопедии им. М.П. Бажана. – К.; 1989. – Т. 3. – 772 с.
160. *Якимов П.П.* Письменные доказательства в практике арбитража. – М., 1959.
161. *Закон* України від 24.02.1994 року “Про міжнародний комерційний арбітраж” // Відомості Верховної Ради України. – 1994. – № 25. – Ст. 198.
162. *Александров Д.К.* Электронно-цифровая форма договора // www.vic.spb.ru/law/doc/a111.htm
163. *Цивільний* кодекс Української РСР // Кодекси України. Книга друга. – К.: Юрінком Інтер., 1997. – 575 с.

164. *Інструкція* з діловодства у міністерствах, інших центральних органах виконавчої влади, Раді Міністрів Автономної Республіки Крим, місцевих органах виконавчої влади, затверджена Постановою Кабінету Міністрів України № 1153 від 17.10.1997 року в редакції 28.07.2003 року // http://www.rada.kiev.ua/cgi-bin/putfile.cgi
165. *Кротов М.* Пояснительная записка проекту модельного закона «Об электронной цифровой подписи» // http://www.ice.ru/exp/30
166. *Архів* Третейського суду при АТ "Міжбанківський фінансовий дім". Рішення від 28.05.1993 року.// http://www.urbicom.ru/Include/OpenMaterial.htm?Id=1173
167. *Соловяненко Н.* Соглашение между коммерческими партнерами об электронном обмене данными // eCommerce World. – 2000. – № 2.
168. *Мальцев Ю.В., Молчанов В.В., Шерстобитов А.Е.* Правовое регулирование электронного документооборота в банковской практике // Гражданско-правовое регулирование банковской деятельности. – М., 1994. – С. 34-41.
169. *Буткевич С.А.* Заключение хозяйственных договоров. – К.: Вища школа, 1978. – 89 с.
170. Скарго В.А. Заключение хозяйственного договора: Автореф. дис... канд. юрид. наук. М. – 1972. – 23 с.
171. *Вердников В.Г., Скарго В.А.* Заключение хозяйственного договора. – Сов. гос. и право, 1971. – № 1. – С. 22–29.
172. *Ананько А.* Заключение договоров путем электронного обмена данными // http://www.russianlaw.net/law/doc/a123.htm
173. *Щербина В.С.* Господарське право: Підручник. – К.: Юрінком Інтер, 2003. – 480 с.
174. *Луць В.В.* Заключение и исполнение хозяйственных договоров. – М.: Юридическая литература, 1978. – 143 с.
175. *Дорохов В.Я.* Понятие документа в советском праве // Правоведение. – 1982. – № 2.
176. *Закон* України від 09.04.1999 року "Про обов'язковий примірник документів" // Відомості Верховної Ради України. – 1999. – № 22-23. – Ст. 199.
177. *Вершинин А.П.* Электронный документ: правовая форма и доказательство в суде. – М.: Городециздат, 2000. – 247 с.
178. *Соловьев Н.* Электронные документы. Какие они? / http://www.depository.ru/news/speech/snn-0900.htm
179. *Косовец А.А.* Правовое регулирование электронного документооборота. Вестник Московского университета. Сер. 11, Право. – 1997. – № 4. – С. 46–50.
180. *Тернер М., Смит Г.* Юридические вопросы электронной коммерции // http://www.rans.ru/lawyer/herbert.html
181. *Семилетов С.И.* Электронный документ как продукт технологического процесса документирования информации и объект правового регулирования. – Государство и право. – 2003. – № 1. – С. 15-21.
182. *Лист* Вищого Арбітражного Суду РФ від 19.08.1994 року С1-7/оп-578 // http://www.russianlaw.net/law/cases/case_crypto_lancrypto.htm
183. *Гадасин В. А., Конявский В. А.* От документа – к электронному документу. Системные основы. – М.: РФК-Имидж Лаб, 2001. – 218 с.
184. *Uniform* Electronic Commerce Act of Canada, of August 30, 1999 // http://www.le.state.ut.us/~2000/htmdoc/sbillhtm/SB0125.htm
185. *Инструктивные* указания Госарбитража СССР от 29.06.1979 года "Об использовании в качестве доказательств по арбитражным делам документов, подготов-

ленных с помощью электронно-вычислительной техники". – Систематизированный сборник инструктивных указаний Государственного арбитража при Совете Министров СССР. – 1989.
186. *Бару М.О.* Советское гражданское право. – К., – 1977. – 428 с.
187. *Новицкий И. Б.* Советское гражданское право. – М.: Госюриздат, 1950. – 368 с.
188. *Шварц Х.И.* Советское гражданское право. – М.: Госюриздат, 1965. – 320 с.
189. *Кабалкин А.Ю.* Советское гражданское право. Т. 1. – М.: Юрид. лит., 1965. – 249 с.
190. *Крылова З.Г.* Советское право. – М.: Юрид. лит., 1978. – 346 с.
191. *Зобов'язальне* право: Теорія і практика. Навчальний посібник / Під ред. О.В. Дзери. – К.: Юрінком Інтер, 1998. – 910 с.
192. *Рабинович Н.В.* Недействительность сделок и ее последствия. – Л.: Изд-во ЛГУ, 1960. – 324 с.
193. *Наумов В.* Проблема ответственности информационных провайдеров // Материалы третьей всероссийской конференции «Право и Интернет: теория и практика» 27–28 ноября 2000 года, Москва. Российская академия государственной службы при президенте Российской Федерации. – С. 320-324.
194. *Предпринимательское* право: Сборник нормативных актов / Сост. И.В. Ершова. – М.: Юриспруденция, 2000. – 591 с.
195. *Указ* Президента від 22 квітня 1998 року "Про деякі заходи захисту інтересів держави в інформаційній сфері" № 346/98 // Урядовий кур'єр від 30.04.1998.
196. *Концепція* розвитку державної системи ліцензування підприємницької діяльності за її видами, затверджена Постановою Кабінету Міністрів України від 23.09.1996 року № 1164 // Інформаційний збірник. – 1996. – № 20.
197. *Концепція* створення Єдиної державної автоматизованої паспортної системи, затверджена Постановою Кабінету Міністрів України від 20.01.1997 року № 40 // Офіційний вісник України. – 1997. – N 4. – Ст. 35.
198. *Гражданское* право // Под ред. Е.А. Суханова – М.: БЕК, 2002. – 785 с.
199. *Соловяненко Н.И.* Разработка законодательства об электронной подписи // Банковское дело в Москве. – 2001. – № 1 (73).
200. *Лебедев А.Н.* Что такое электронные документы в России (техника, технологии и законы) // http://vlarin.chat.ru/lancrypto/2.htm
201. *Предложение* Соединенных Штатов Америки. Проект международной конвенции по электронным сделкам // http://www.algo.ru/internetlaw/analog18.asp
202. *Соловяненко Н.* Электронная подпись в правовом лабиринте. – eCommerce World. – 2001. – № 2. – С. 16–22.
203. *Шамраев А.* Правовое поле электронного бизнеса: наступая на заморские грабли? // http://www.bizon.ru/viewarticle.phtml?id=370
204. *Елисеев И.* О криптографии – не шифруясь. – eCommerce World. – 2001. – № 2. – С. 14-18.
205. *Олейник В.* Цифровая подпись – это очень просто // http://e-commerce.com.ua/secur/sec5.html
206. *Закон* України від 17.05.2001 року "Про підтвердження відповідності" // Відомості Верховної Ради. – 2001. – № 32. – Ст. 169.
207. *Положення* "Про сертифікацію засобів захисту інформації", затверджене постановою Уряду Російської Федерації від 26.06.1995р. № 608 // http://www.libertarium.ru/libertarium/15009.

208. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», прийнятий Держстандартом СРСР та введений в дію 01.07.1990 р.
209. *Волчков А.А.* Кому нужен закон «Об электронной цифровой подписи»? // Защита информации. Конфидент. – 2002. – № 3. – С. 3–7.
210. ГОСТ 34.310-95 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».
211. ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хеширования».
212. *Положення* "Про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації", затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ 30.11.1999 року № 53 // Офіційний вісник України. – № 50. – Ст. 456 від 31.12.1999.
213. *Code Civil* // http://www.legifrance.gouv.fr/WAspad/ListeCodes
214. *Язев А.* Электронный документооборот: основные понятия // Мир электронной коммерции. – 2001. – № 1. – С. 22–27.
215. *Братусь С.Н.* Юридическая ответственность и законность. – М.: Юрид. лит., 1976. – 153 с.
216. *Кожухов А.* Настоящие контракты в виртуальном мире // Юридическая практика. – 2001. – 22 февраля. – С. 4.
217. *Соловяненко Н.И.* О проекте модельного закона СНГ «Об электронной цифровой подписи» // http://kinnet.ru/cterra/342/26.html
218. *Дутов М.М.* Правовое обеспечение развития электронной коммерции.: Дис. канд. юрид. наук. – К., 2003. – 196 с.
219. *Правила* атестації фахівців неруйнівного контролю, затверджені Держнаглядохоронпраці № 118 від 06.05.1997 року // Офіційний вісник України. – № 36. – Ст. 39 від 17.09.1997.
220. *Правила* проведення торгів на Валютній секції Української Міжбанківської Валютної біржі, затверджені Українською міжбанківською валютною біржею № 30 від 16.07.1997 року.
221. *Постанова* Кабінету Міністрів України від 26.06.1996 року "Про акредитацію експертів-гемологів дорогоцінного, напівдорогоцінного та декоративного каміння" № 673.
222. *Закон* України «Про друковані засоби масової інформації (пресу) в Україні» від 16.11.1992 року // Відомості Верховної Ради. – 1993. – № 1. – Ст. 1.
223. *Закон* Російської Федерації від 08.08.2001 року "Про ліцензування окремих видів діяльності" //Російська газета, 10.08.2001 року.
224. *Беззубцев О.А., Мартынов В.Н., Мартынов В.М.* Некоторые вопросы правового обеспечения использования ЭЦП // http://www.ibusiness.ru/egover/19956/
225. *Electronic* commerce and electronic signature Act of Slovenia, of June, 2000 // http://www.sigov.si/ep/ecaes.doc
226. *Жилінкова І.* Правове регулювання Інтернет-відносин // Право України. – 2003. – № 5. – С. 132–136.
227. *Шевченко О.* Електронна комерція в умовах чинного законодавства // Право України. – 2003. – № 10. – С. 82–83.
228. *Макарова М.В.* Електронна комерція: Посібник для студентів вищих навчальних закладів. – К.: ВЦ "Академія", 2002. – 357 с.

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

Анна Вячеславівна ЧУЧКОВСЬКА

ПРАВОВЕ РЕГУЛЮВАННЯ ЕЛЕКТРОННОЇ КОМЕРЦІЇ В УКРАЇНІ

Навчальний посібник

Керівник видавничих проектів – *Б.А.Сладкевич*
Редактор – *Л.І. Єросова*
Комп'ютерний набір і верстка – *І.В. Марченко*
Дизайн обкладинки – *Б.В. Борисов*

Підписано до друку 01.11.2006. Формат 60х84 1/16.
Друк офсетний. Гарнітура PetersburgC.
Умовн. друк. арк. 14.

Видавництво "Центр учбової літератури"
вул. Електриків, 23
м. Київ, 04176
тел./факс 425-01-34, тел. 451-65-95, 425-04-47, 425-20-63
8-800-501-68-00 (безкоштовно в межах України)
e-mail: office@uabook.com
сайт: WWW.CUL.COM.UA

Свідоцтво ДК №2458 від 30.03.2006