УДК: 347.441:004

ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС ЯК РЕКВІЗИТ ДОГОВОРУ КУПІВЛІ-ПРОДАЖУ В МЕРЕЖІ ІНТЕРНЕТ

Т. А. Чернова, І. В. Стаднік

Анотація. У статті досліджені питання електронного цифрового підпису, виявлені актуальні проблеми, зокрема щодо створення, використання та збереження даного виду підпису та окреслено шляхи їх вирішення у вигляді пропозиції щодо прийняття ряду нормативно-правових актів.

Ключові слова: Інтернет, електронний правочин, електронний підпис, сертифікація, банківська діяльність.

Документообіг є важливою складовою частиною процесів управління і прийняття управлінських рішень. Електронний підпис, у свою чергу, є обов'язковим реквізитом, який використовується для ідентифікації автора або особи, що підписувала електронний документ, іншими суб'єктами електронного документообігу. Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Проблеми запровадження в Україні електронного цифрового підпису стають все актуальнішими у зв'язку з розширенням використання інформаційно-комунікаційних технологій у суспільних відносинах, розбудовою систем електронних платежів, електронної торгівлі, управління тощо. Тому виникає необхідність у дослідженні саме цього питання, виявленні актуальних проблем та шляхів їх вирішення.

Законодавство України допускає використання ЕЦП при пересиланні документів для забезпечення електронного документообігу. Для укладення договору купівлі-продажу в мережі Інтернет достатньо обміну документами, підписаними електронним підписом, з яких кожен містить волевиявлення однієї зі сторін. Але, цей вид підпису може використовуватися виключно, якщо усі сторони електронного правочину використовують засіб електронного цифрового підпису. У тому випадку, коли при укладенні даного договору непотрібен електронний підпис, користувач заповнює форму, визначаючи в ній умови, а потім відправляє її, натискаючи, як правило, кнопку-іконку «Згоден». Існують також і способи заміни електронного цифрового підпису, серед яких можливість електронного підпису одноразовим ідентифікатором. Це відома споживачеві так звана алфавітно-цифрова послідовність, що передається засобом зв'язку на електронну пошту або мобільний телефон споживача для введення в інформаційно-телекомунікаційній системі продавця з метою підтвердження укладання правочину. Як вбачається, це більш спрощена система підпису електронного договору купівлі-продажу, що є зручнішою як для покупця, так і для продавця.

Перехід до електронного документообігу з використанням електронного цифрового підпису – це новий крок у розвитку суспільства. Електронний документообіг не можливий без побудови відповідної інфраструктури й законодавчої підтримки. Тому основою даного процесу є Закони України «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг» та інші нормативні акти, стандарти й протоколи.

Так, електронний цифровий підпис – це вид підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача [1].

Як зазначає Є. О. Суханов, «електронний цифровий підпис є результатом роботи програми генерації цифрового підпису» [2, с. 125]. Такий підпис є аналогом власноручного підпису і має дві основні властивості: відтворюється тільки однією особою, а оригінальність його може бути засвідчена багатьма; він нерозривно пов'язаний з конкретним документом і

лише з ним. Електронний цифровий підпис жорстко поєднує в одне ціле зміст документа і секретний ключ того, хто підписує, і робить неможливою зміну документа без порушення оригінальності даного підпису [3]. На думку автора, він є самостійним аналогом власноручного підпису поряд з аналогом, отриманим в результаті факсимільного відтворення підпису з допомогою засобів механічного або іншого копіювання.

Відповідно до ст. 3 ЗУ «Про електронний цифровий підпис», електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

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

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

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

При використанні прямого цифрового підпису взаємодіють тільки самі учасники, тобто відправник та одержувач. Передбачається, що одержувач знає відкритий ключ відправника. Цифровий підпис може бути створений шифруванням усього повідомлення або його хеш-коду (перетворення вхідного масиву даних довільної довжини в вихідний бітовий рядок фіксованої довжини) закритим ключем відправника [4].

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Захист інформації в електронному документі ґрунтується на двох основних методах шифрування: симетричному й асиметричному. Впродовж останніх років набули поширення системи асиметричного кодування даних в електронній формі, які дають змогу не тільки організувати конфіденційну передачу інформації без попереднього обміну секретним ключем, а й такі, що значно розширюють функції криптографії, включаючи технологію електронного цифрового підпису. Метод асиметричного шифрування надає можливість використовувати пари ключів: закритого і відкритого.

Закритий ключ є найбільш вразливим компонентом всієї криптосистеми цифрового підпису. Зловмисник, який вкрав закритий ключ користувача, може створити дійсний цифровий підпис будь-якого електронного документа від імені цього користувача. Тому особливу увагу потрібно приділяти способу зберігання закритого ключа. Користувач може зберігати закритий ключ на своєму персональному комп’ютері, захистивши його за допомогою пароля. Однак такий спосіб зберігання має ряд недоліків, зокрема, захищеність ключа повністю залежить від захищеності комп’ютера, і користувач може підписувати документи лише на цьому комп’ютері. Найбільш захищений спосіб зберігання закритого ключа – зберігання на смарт-картці. Для того, щоб використовувати смарт-карту, користувачеві необхідно не тільки її мати, але й ввести PIN-код, тобто, здійснюється двофакторна аутентифікація. Після цього підписується документ, або його хеш передається в карту, її процесор здійснює підписування хешу і передає підпис назад. У процесі формування підпису таким способом не відбувається копіювання закритого ключа, тому весь час існує тільки єдина копія ключа. Крім того, зробити копіювання інформації зі смарт-карти складніше, ніж з інших пристроїв зберігання [5].

Інсталяція та налаштування спеціальних програмних засобів накладання електронного цифрового підпису максимально автоматизована й у більшості випадків не потребує втручання. Накладання даного підпису під матеріалами заявки та шифрування матеріалів заявки також спрощені й відбуваються в такій послідовності: зчитування ключа, вибір необхідних матеріалів, накладання підпису та шифрування. Сервер системи електронного подання перевіряє підписи й у разі чинності сертифікату та цілісності підписів передає матеріали на подальшу обробку, про що сповіщає заявника [6].

Основними структурними елементами національної системи електронного цифрового підпису є акредитовані центри сертифікації ключів і користувачі. Основними видами послуг акредитованих центрів сертифікації ключів є сертифікація ключів користувачів і підтримка їх чинності. Послуги надаються відповідно до тарифних планів і на певний строк. Під час генерації ключів необхідно вказати пароль доступу до кожного з них. Для зменшення ймовірності розкриття паролю він має відповідати певним вимогам щодо довжини та вжитих літер. Отриманий персональний ключ має зберігатися таким чином, щоб унеможливити доступ до нього стороннім особам. Пошкодження носія з ключем або втрата довіри щодо його конфіденційності є компрометацією ключа. У таких випадках необхідно звернутися до акредитованих центрів сертифікації ключів з відповідною заявою про блокування та скасування скомпрометованого ключа й отримати новий.

Центральний засвідчувальний орган, який функціонує на базі Державного комітету інформатизації України, засвідчує своїм кореневим сертифікатом Центри сертифікації ключів (ЦСК) і засвідчувальні центри (ЗЦ) [7]. На сьогоднішній день зареєстровано 14 ЦСК, і акредитовано 12 ЦСК і ЗЦ [8]. ЗЦ НБУ засвідчує ЦСК, створені в банках. ЦСК засвідчують своїми сертифікатами відкриті ключі користувачів. В Україні також створений засвідчувальний центр НБУ, який бере участь в процедурі сертифікації відкритих ключів банків, що мають центри сертифікації ключів [9]. Цей центр здійснюватиме сертифікацію відкритих ключів банків. Банки, у свою чергу, сертифікуватимуть відкриті ключі своїм клієнтам. Таким чином, для підтвердження ключа клієнтові банку необхідно мати два сертифікати: один – від засвідчувального центру НБУ, інший – від банку (ЦСК).

Отже, поняття електронного цифрового підпису в найбільшій мірі відповідає своєму призначенню, а саме гарантуванню цілісності та незмінності електронного документа. Але це не єдиний вид підписання договору купівлі-продажу в мережі Інтернет, на практиці використовують ще одноразовий ідентифікатор та заповнений бланк з кнопкою-іконкою «Згоден». Це більш зручний та спрощений спосіб, але прогрес не стоїть на місці, застосування саме електронного цифрового підпису при укладанні договорів відбувається все частіше, особливо у випадках конфіденційності підписуваних документів, в тому числі фінансових. Якщо ж мова йде, наприклад, про купівлю-продаж товарів у Інтернет-магазині, використання ЕЦП може ускладнити процес і зробити його більш тривалим. Крім того, більшість осіб, що здійснюють покупки у Інтернет-магазинах, ЕЦП не мають, і навряд чи є сенс зобов'язувати їх до цього. Тому і закріплювати ЕЦП у якості обов'язкового елемента договору купівлі-продажу в мережі Інтернет не представляється доцільним.

Використання ЕЦП передбачається як фізичними, так і юридичними особами для обміну документами з державними органами, а також між клієнтом і банком без безпосереднього їх відвідування. Для накладання даного підпису використовується таємний (особистий) ключ, а для його перевірки – відкритий (загальновідомий). Послуги з надання електронного цифрового підпису в Україні впроваджуються акредитованими центрами сертифікації ключів.

Дослідивши вищевикладене, можна виявити проблемні питання, які потребують вирішення. Одним з питань, що потребують нормативного вирішення у цій сфері, – є організація роботи центрів сертифікації ключів, які мають надавати послуги цифрового підпису. Слід погодитись з тими спеціалістами, які вважають, що кількість бажаючих займатися такою діяльністю є досить незначною, оскільки фінансовий бар'єр виходу на ринок зазначених структур за нинішніх умов є дуже високим з огляду на специфіку їх функцій (надання засобів цифрового підпису, формування, розповсюдження, скасування, блокування та поновлення сертифікації ключів, генерація відкритих та особистих ключів тощо). А враховуючи те, що все повинно починатися практично з нуля, оскільки майже таким на даному етапі є ринок користувачів, «повернення» інвестицій представляється досить тривалим процесом.

Окрім цього, для остаточного масового використання електронного цифрового підпису в Україні необхідно прийняти певну кількість нормативно-правових актів щодо: національних стандартів, вимог до засобів електронного цифрового підпису, форматів даних, які для цього використовуються. Усе це допоможе покращити функціонування інституту електронного цифрового підпису та удосконалити процес електронного документообігу.

Аннотация. В статье исследованы вопросы электронной цифровой подписи, раскрыты актуальные проблемы, в частности, относительно создания, использования и сохранения данного вида подписи, а также очерчены пути их решения в виде предложения по принятию ряда нормативно-правовых актов.

Ключеые слова: Интернет, электронная сделка, электронная подпись, сертификация, банковская деятельность.

Abstract. The article explores the issues of electronic digital signature, discovered the actual problems, in particular concerning the creation, use and preservation of this type of signature, and found ways to address them in the form of proposals for the adoption of a number of regulatory legal acts.

Key words: Internet, electronic deal, electronic signature, certification, banking.

СПИСОК ЛІТЕРАТУРИ

1. Про електронний цифровий підпис: Закон України від 22.05.2003р., № 852-IV // Відомості Верховної Ради. – 2003. – № 36. – Ст. 276.
2. Суханов Е.А. Гражданское право: учебн. / Е. А. Суханов. – М. : БЕК, 2003. – Т. II. – 469 с.
3. Ліга страхових організацій України [Електронний ресурс]. – Режим доступу : www. uainsur.com/massmedia/16059.
4. Ткач Ю. М. Електронний цифровий підпис / Ю. М. Ткач // Доповідь. – Л., 2010. – 83 с.
5. Беляев А. В. Методы и средства защиты информации: курс лекций / А. В. Беляев. – СПб., 2000. – 112 с.
6. Особливості отримання послуг і використання ЕЦП під час складання, подання та експертизи заявок на об'єкти промислової власності / К. Константинов. – К., 2012. – 58 с.
7. Сертифікати акредитованих ЦСК та ЗЦ [Електронний ресурс]. – Режим доступу: www.czo.gov.ua/index.php?page=cca&type=1.
8. Акредитовані ЗЦ та ЦСК [Електронний ресурс]. – Режим доступу: www.czo.gov.ua/index.php?page=reestr.
9. Савченко А. С. Електронна Україна: міф чи реальність? / А. С. Савченко, І. С. Івченко // Вісник НБУ. – 2010. – № 3. – С. 18–23.

УДК: 347.518.2

ВІДШКОДУВАННЯ ШКОДИ, ЗАПОДІЯНОЇ ВНАСЛІДОК ДОРОЖНЬО-ТРАНСПОРТНОЇ ПРИГОДИ: ПРОБЛЕМНІ ПИТАННЯ ВИРІШЕННЯ СПОРІВ

С. О. Чорний, О. І. Антонюк

Анотація. У статті розглядаються питання відшкодування шкоди, завданої внаслідок дорожньо-транспортної пригоди. Проаналізовано окремі проблемні питання та особливості відшкодування майнової і моральної шкоди, завданої внаслідок дорожньо-транспортної пригоди, що виникають на практиці, та запропоновані шляхи їх вирішення.

Ключові слова: джерело підвищеної небезпеки, дорожньо-транспортна пригода, шкода, страховий випадок, страховик.

Запобігання дорожньо-транспортних пригод (далі – ДТП) та усунення їх наслідків є одними із найгостріших проблем кожної держави, і Україна у цьому випадку не є виключенням. Майже кожна ДТП завдає певну шкоду: майнову або моральну. За даними статистики Управління безпеки дорожнього руху Департаменту превентивної діяльності