ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ І ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ПРОМИСЛОВИМИ ПІДПРИЄМСТВАМИ У ЗБУТОВІЙ І ЗАКУПІВЕЛЬНІЙ ДІЯЛЬНОСТІ: ПЕРЕВАГИ І НЕДОЛІКИ

THE USE OF ELECTRONIC DOCUMENT AND ELECTRONIC DIGITAL SIGNATURE BY INDUSTRY IN THE PROCUREMENT AND SALE: ADVANTAGES AND SHORTCOMINGS

УДК 330.567.6-047.37.669

Хижняк О.С.
аспірант
Класичний приватний університет

У статті проаналізовано основні завдання електронного документообігу, виділені властивості і методи побудови схем електронного цифрового підпису. Розглянуто найбільш поширені програмні засоби роботи з ЕЦП, а також законодавчі і нормативні акти, які визначають принципи використання електронного документообігу та ЕЦП промисловими підприємствами в Україні.
Ключові слова: *електронний документообіг, електронний цифровий підпис, корпоративні інформаційні системи, кодування електронного підпису, транскордонні угоди.*

В статье проанализированы основные задачи электронного документооборота, выделены свойства и методы построения схем электронной цифровой подписи. Рассмотрены наиболее распространенные программные средства работы с ЭЦП, а также законодательные и нормативные акты, которые определяют принципы использования ЭЦП промышленными предприятиями в Украине.
Ключевые слова: *электронный документооборот, электронная цифровая подпись, корпоративные информационные системы, кодирование электронной подписи, трансграничные сделки.*

The article analyzes the main objectives of electronic document highlighted the properties and methods of construction of digital signature schemes. Considered the most common software work with EDS as well as legislative and regulatory acts that define the principles of using electronic documents and EDS by industry in Ukraine.
Key words: *electronic document management, electronic digital signature, corporate information systems, coding of EDS, cross-border transactions.*

Постановка проблеми. Жорстка конкуренція у ринковій економіці та стрімке зростання науково-технічного прогресу в світі зумовили розвиток нових форм торговельно-економічних відносин. На жаль, практика таких форм, які з'являються за прикладами розвинутих країн, упереджує законодавчі засади державного регулювання цього господарського сегмента і створює умови для нерегламентованого функціонування електронних торгів, що дає негативний результат.

Аналіз останніх досліджень і публікацій. Електронній комерції загалом і регулюванню електронних торгів зокрема присвячені дослідження таких вчених, як С. Кехель, П. Сінг, П. Дінс, Н. Джерк, Г. Дункан, К. Пейтель, А.Саммер.

Постановка завдання. Метою статті є аналіз основних схем, розгляд переваг практичного використання електронного документообігу та електронного цифрового підпису (ЕЦП), а також законодавчих та нормативних актів, які визначають організаційні принципи використання ЕЦП в Україні.

Виклад основного матеріалу дослідження. Український ринок електронного бізнесу розвивається на фоні загального розвитку бізнесу в нашій країні. Впровадження електронних методів в сучасний бізнес визначається виробничою необхідністю, де вирішальною є економічна вигода від застосування нових технологій. Більшість великих і середніх українських підприємств вже зрозуміли зручності, що досягаються ними під час використання Інтернету в бізнесі.

Водночас багато великих українських компаній впроваджують або вже впровадили у себе корпоративні інформаційні системи. Основною функцією таких систем (майданчиків) є проведення електронних торгів.

Важливим моментом у регулюванні відносин «продавець-покупець» є те, що договір купівлі-продажу на електронному торговому майданчику укладається не в електронній, а в усній формі.

Відповідно до змісту статті 207 Цивільного кодексу України письмовою формою вважатиметься таке оформлення правочину, яке забезпечує фіксацію змісту правочину у документах або листах, телеграмах, якими обмінялися сторони. Воля сторін на укладення правочину може бути виражена також за допомогою електронного засобу зв'язку, але за умови наявності достатніх ознак їх приналежності стороні цього правочину.

Основні правові засади електронного документообігу, зокрема у сфері договірних відносин, визначаються Законом України «Про електронні документи та електронний документообіг».

Вказаний Закон встановлює вимоги до оригіналу електронного документа: обов'язкові реквізити, електронний підпис автора або підпис, прирівняний до власноручного підпису відповідно до Закону України «Про електронний цифровий підпис» [1].

Цифровий підпис дає змогу вирішити такі завдання:

– здійснити аутентифікацію джерела повідомлення;

– встановити цілісність повідомлення;

– забезпечити неможливість відмови від факту підпису конкретного повідомлення.

У практичній діяльності важливо не тільки захищати дані від незаконного користувача, але й мати можливість перевірити авторство конкретного повідомлення, а також перевірити те, щоб воно не було змінено сторонньою особою. Саме для вирішення цих проблем було розроблено ряд алгоритмів ЕЦП. В основі більшості з них лежить ідея використання деякої односторонньої функції з секретним ключем F_K для створення пари бінарних рядків (M, Q), де M – електронний документ, а Q – рішення рівняння $F_K(Q) = M$ [9].

Назвемо такі властивості ЕЦП:

1) при будь-якому K існує поліноміальний алгоритм обчислення значення $F_K(Q)$;

2) при невідомому K не існує поліноміального алгоритму для рішення рівняння $F_K(Q) = M$ відносно Q;

3) при відомому K існує поліноміальний алгоритм для рішення рівняння $F_K(Q) = M$ відносно Q.

Завдяки першій властивості завжди легко перевірити, чи відповідає підпис до повідомлення, а завдяки другій властивості підробити підпис при досить великому ключі практично неможливо. Доказ цієї властивості дав би змогу надати підписаним повідомлення юридичну силу.

Секретний та відкритий ключі знаходяться у взаємнооднозначній відповідності, а завдяки третій вимозі не існує поліноміального алгоритму обчислення секретної компоненти по відкритій компоненті.

Під час підписання електронного документа його початковий зміст не змінюється, а додається блок даних – так званий Електронний цифровий підпис.

Отримання цього блоку можна розділити на два етапи.

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

Цей відбиток має такі особливості:

– фіксована довжина, незалежно від довжини повідомлення;

– унікальність відбитку для кожного повідомлення;

– неможливість відновлення повідомлення за його відбитком.

Таким чином, якщо документ був модифікований, то зміниться і його відбиток, що відобразиться під час перевірки Електронного цифрового підпису.

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

Механізм підписання та кодування підпису показано нижче (рис. 1).

Розшифрувати ЕЦП і одержати початковий відбиток, який відповідатиме документу, можна,

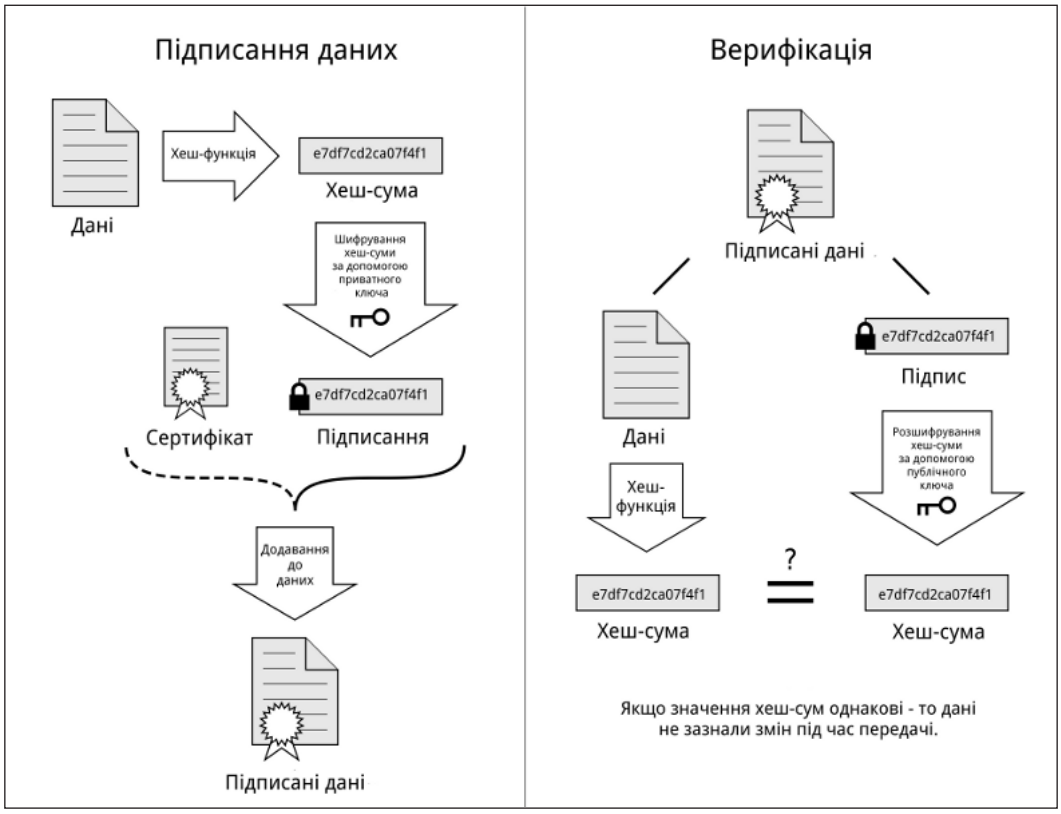

Рис. 1. Механізм дії електронного цифрового підпису

тільки використовуючи Сертифікат відкритого ключа автора.

Таким чином, обчислення відбитку документа захищає його від модифікації сторонніми особами після підписання, а шифрування особистим ключем автора підтверджує авторство документа [2].

Існує кілька методів побудови схем ЕЦП.

Шифрування електронного документа на основі симетричних алгоритмів. Ця схема передбачає наявність у системі третьої особи (арбітра), що користується довірою учасників обміну підписаними подібним чином електронними документами; взаємодія користувачів за цією системою проводиться за такою схемою:

– учасник А зашифровує повідомлення на своєму секретному ключі КА, значення якого розділене з арбітром, потім шифроване повідомлення передається арбітру із зазначенням адресата даного повідомлення (інформація, що ідентифікує адресата, передається також у зашифрованому вигляді);

– арбітр розшифровує отримане повідомлення на ключі КА, проводить необхідні перевірки, а потім зашифровує на секретному ключі учасника В (КВ); далі зашифроване повідомлення посилається учаснику В разом з інформацією, що воно прийшло від учасника А;

– учасник В розшифровує дане повідомлення і переконується в тому, що відправником є учасник А.

Використання асиметричних алгоритмів шифрування. Фактом підписання документа в цій схемі є зашифрування документа на секретному ключі його відправника. Ця схема теж використовується досить рідко внаслідок того, що довжина електронного документа може виявитися критичною. У цьому випадку не потрібна наявність третьої сторони, хоча вона може виступати в ролі сертифікаційного органу відкритих ключів користувачів.

З розвитком попередньої ідеї стала найбільш поширена така схема ЕЦП: зашифрування остаточного результату обробки електронного документа хеш-функцією за допомогою асиметричного алгоритму. Хеш-функцією називається математична або інша функція, яка для рядка довільної довжини обчислює деяке ціле значення або деякий інший рядок фіксованої довжини [7, с. 264]. Математично це можна записати так: h = H (M), де M – вихідне повідомлення, зване іноді прообразом, а h – результат, званий значенням хеш-функції (хеш-кодом або дайджестом).

Генерація підпису відбувається таким чином:

– учасник А обчислює хеш-код від електронного документа; отриманий хеш-код проходить процедуру перетворення з використанням свого секретного ключа; псля чого отримане значення (яке і є ЕЦП) разом з електронним документом відправляється учаснику В;

– учасник В повинен отримати електронний документ з ЕЦП та сертифікований відкритий ключ учасника А, а потім провести дешифрування на ньому ЕЦП, сам ЕД піддається операції хешування, після чого результати порівнюються, і якщо вони співпадають, то ЕЦП визнається істинною, в іншому випадку – помилковою.

Криптографічна хеш-функція повинна забезпечувати стійкість до колізій (два різні набори даних повинні мати різні результати перетворення) та необоротність (неможливість обчислити вхідні дані за результатом перетворення).

У більшості ранніх систем ЕЦП використовувалися функції з секретом, які за своїм призначенням близькі до односторонніх функцій. Такі системи уразливі до атак з використанням відкритого ключа, оскільки, вибравши довільний цифровий підпис і застосувавши до нього алгоритм верифікації, можна отримати вихідний текст. Щоб уникнути цього, разом з цифровим підписом використовується хеш-функція, тобто обчислення підпису здійснюється не щодо самого документа, а щодо його хешу. У цьому випадку в результаті верифікації можна отримати тільки хеш вихідного тексту, отже, якщо використовується хеш-функція, яка криптографічно стійка, то отримати вихідний текст буде обчислювально складно, тобто атака такого типу стає неможливою.

Крім цього, існують інші різновиди цифрових підписів (груповий підпис, незаперечний підпис, довірений підпис), які є модифікаціями описаних вище схем. Їх поява обумовлена різноманітністю завдань, що вирішуються за допомогою ЕЦП.

Під час укладення договору на електронному торговому майданчику відсутній єдиний документ, який би містив реквізити сторін, істотні умови договору і передбачений законодавством засіб посвідчення електронного документа сторонами, оскільки електронна форма правочину є видом письмової форми і відповідає всім її ознакам з урахуванням специфіки всесвітньої інформаційної мережі.

Таким чином, реальне волевиявлення покупця виражається у конклюдентних діях з оплати товару у визначений спосіб, що вже є початком виконання угоди [3]. В базі даних торгового майданчика зберігається інформація про оплату товару продавця, а також його логін (ім'я), але це не буде вважатися письмовою формою правової дії.

Іноземні експерти пропонують в Україні будувати електронні торгові майданчики для здійснення закупівель паралельно з впровадженням технології електронного транскордонного підпису. Це необхідно, щоб електронні угоди із зарубіжними учасниками ринку здобули юридичну значимість без застосування складних посередницьких схем. Залучення до закупівель іноземних постачальників дасть змогу оптимізувати витрати промисловця за рахунок збільшення числа конкурентних пропозицій.

Справа в тому, що при транскордонних угодах на електронних торгових майданчиках український учасник торгів не буде мати можливості перевірити зарубіжний електронний підпис та й загалом може зіткнутися з низкою тонкощів у відмінності місцевих законодавств про його (підпис) допустимість. Без застосування механізму перевірки іноземного електронного підпису варіантів угод з закордонними постачальниками може бути два: або проведення електронних торгів через посередників, або вкрай ризиковані угоди, не підкріплені ЕЦП. Без електронного підпису при недотриманні умов договору однією зі сторін надзвичайно складно довести свою правоту в судовому порядку. Для вирішення подібних проблем у багатьох країнах створюються спеціалізовані організації, які виконують функцію Довіреної Третьої Сторони (ДТЗ), а також реалізується механізм взаємодії електронних торгових майданчиків і ДТЗ з перевірки іноземних ЕЦП. Проте не всі електронні торгові майданчики мають відповідну базу для проведення транскордонних електронних торгів за міжнародними правилами.

Висновки з проведеного дослідження. Підсумовуючи, слід відзначити, що на зарубіжних електронних майданчиках показник шахрайства складає приблизно 0,01% [4]. Що стосується українських торгових майданчиків, то офіційна статистика відсутня, але неофіційні інтернет-опитування користувачів вказують на значний рівень порушень, що пов'язано з неефективним саморегулюванням процедури електронної торгівлі, а також з відсутністю на багатьох майданчиках можливості отримувати електронний цифровий підпис через складності його отримання та підтвердження. Фактично такі майданчики є інформаційною базою, що надають дані про наявних покупців чи продавців певних товарів, але не виконують головну свою функцію – проведення електронних торгів.

Отже, відносини з купівлі-продажу товарів за допомогою електронного майданчику передбачають низку важливих особливостей, які необхідно враховувати під час локального врегулювання таких правовідносин.

На електронних торгових майданчиках України вже незабаром також зможуть здійснюватися угоди з іноземними учасниками ринку. Для цього необхідно створити інфраструктуру відповідно до загальновизнаних міжнародних стандартів.

Завдання створення прозорого середовища процедури закупівель в Україні активно реалізується урядом вже зараз. Справедливе бажання скоротити витрати на закупівлях та продажу товарів чи устаткування обов'язково переросте у реальну можливість. І реальний інструмент досягнення цього доступний вже зараз – реалізація схеми транскордонного підпису на електронних торгових майданчиках країни. Бо саме вихід на євроринок та залучення іноземних партнерів дадуть можливість вітчизняним промисловим підприємцям підвищити технічний рівень бізнес-процесів, отримати найнижчу ринкову вартість на придбаний товар чи сировину, а вітчизняним продавцям – вийти на міжнародний ринок.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. ДСТУ 4145-2002 «Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння» / Державний комітет України з питань технічного регулювання та споживчої політики. – 28.12.2002. – № 31. – [Електронний ресурс]. – Режим доступу : http://www.dssu.gov.ua.

2. Чередниченко В.Б. Електронний цифровий підпис у правовому полі України / В.Б. Чередниченко [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/portal/natural/soi/2009_7/Chered.pdf.

3. Дианова Т.В. Некоторые особенности электронной торговли: от «мифов» к «эффекту скольжения» / Т.В. Дианова // Вопросы экономики. – 2012. – № 5. – С. 139–146.

4. Законодавство / Сайт Верховної Ради України [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

5. Tanaka W. Competition, fraud may harm eBay / W. Tanaka [Електронний ресурс]. – Режим доступу : http://www.crime-research.org/news.

6. Основы криптографии : [учебное пособие] / [А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин]. – 2-е изд., испр. и доп. – М. : Гелиос АРВ, 2002. – 480 с.

7. Гринович А.А. Електронний цифровий підпис: особливості застосування, переваги та проблеми / А.А. Гринович, Г.В. Пухальська [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/portal.