УДК 343.9

ВИЯВЛЕННЯ ПІДРОБКИ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ДЛЯ ВСТАНОВЛЕННЯ ЗМІН У ДОКУМЕНТІ

Линник О.В.,
доцент кафедри кримінального права, процесу та криміналістики
Національний університет державної податкової служби України

Стаття присвячена аналізу поняття електронних документів, можливості їх засвідчення шляхом використання електронного цифрового підпису та правового регулювання таких суспільних і правових відносин відповідно до законодавства України. Крім того, у статті зазначено принципи і вимоги, яким мають відповідати електронні цифрові підписи, а також способи фальсифікації даних підписів та їх наслідки.

Ключові слова: електронний документ, електронний підпис, цифровий підпис, підробка підпису, зміни у документі, фальсифікація.

Линник Е.В. / ВЫЯВЛЕНИЕ ПОДДЕЛКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ДЛЯ УСТАНОВЛЕНИЯ ИЗМЕНЕНИЙ В ДОКУМЕНТЕ / Национальный университет государственной налоговой службы Украины, Украина

Статья посвящена анализу понятия электронных документов, возможности их засвидетельствования путем использования электронной цифровой подписи и правового регулирования таких общественных и правовых отношений в соответствии с законодательством Украины. Кроме того, в статье указано принципы и требования, которым должны соответствовать электронные цифровые подписи, а также способы фальсификации данных подписей и их последствия.

Ключевые слова: электронный документ, электронная подпись, цифровая подпись, подделка подписи, изменения в документе, фальсификация.

Linnik O.V. / DETECTION OF COUNTERFEIT ELECTRONIC DIGITAL SIGNATURE FOR ESTABLISHING CHANGES IN THA DOCUMENT / National University of State Tax Service of Ukraine, Ukraine

The article analyses the concept of electronic documents, the possibility of their certification through the use of digital signature and the legal regulation of social and legal relations in accordance with the legislation of Ukraine. In addition, the article states the principles and requirements to be met by digital signatures, as well as methods of data falsification of signatures and their consequences.

The article aims to study the concept of digital signature, conditions and ways to fake the purpose of amending the documents and identify ways to overcome them. Also indicated in this article attempts to falsify the signature or signed document – the so-called «attack».

Also, this paper describes the classification of possible results of such attacks: 1. Full hacking digital signature. Getting private key, which means full evil algorithm. 2. Universal fake digital signature. Definition of a similar signature algorithm allows to forge signatures for any electronic document. 3. Selective forgery of digital signatures. In this case, the attacker fabricate two documents with the same signature, and at the right time substitute one another. 4. Existential forgery of digital signatures. The offender may try to pick up a document to this signature to caption fitted. However, in most cases, this document may be the only one.

Based on the properties of digital signature requirements were formulated to him: 1. Signature must be a binary pattern that depends on the text of the signed document. 2. In the signature should be used a unique subscriber information to prevent forgery. 3. Create a digital signature should be relatively easy. 4. Forgery of signatures should be computationally impossible by creating a new document to an existing digital signature, and by creating a fake digital signature for the present document. 5. The digital signature must be sufficiently compact and not take up a lot of memory.

Key words: electronic document, electronic signature, digital signature, signature forgery, changes in the document, falsification.

На даний час в нашій країні широкого поширення набуло використання електронних документів, які існують не лише наряду з традиційними паперовими документами, але й замість них. Саме застосування систем електронного документообігу дозволяє досягти економічної доцільності та корисності. У зв'язку з цим, одним з найважливіших напрямків розвитку українського законодавства і правозастосовчої практики є правове регулювання відносин у сфері електронного документообігу та надання юридичної сили електронним документам, а також їх захисту. Виконання цих завдань та можливість у подальшому використовувати такі документи як доказ, можливе шляхом внесення до переліку їх обов'язкових реквізитів так званого електронного цифрового підпису.

Метою статті є дослідження поняття електронного цифрового підпису, умов та способів його підробки з метою внесення змін у документи, а також визначення шляхів їх подолання.

Дану проблематику досліджувало багато вчених, серед яких: М. І. Анохін, С. Бернет, Ю. В. Бородакій, Н. П. Варновский, В. М. Глушков, М. В. Денисова, М. М. Дутов, А. В. Кобець, Г. І. Купріянова, А. Матвієнко, В. А. Онегов, І. А. Семан, М. Н. Цивін, В. А. Шахвердов, В. В. Ященко та інші.

В наш час, коли підробка відомостей та підпису у паперовому документі не складає жодної проблеми для правопорушників, все більше людей звертаються до більш захищеного документообігу – електронного. Адже, відомо, що існує безліч спеціалістів-шахраїв, здатних в лічені хвилини відтворити підпис будь-якого ступеня складності [1].

У 1976 році Уітфілдом Діффі та Мартіном Хеллманом було вперше запропоновано поняття «електронний цифровий підпис», хоча вони всього лише припускали, що дані схеми можуть існувати. А вже в 1977 році, Рональд Ривест, Аді Шамір і Леонард Адлеман розробили криптографічний алгоритм RSA (абревіатура з прізвищ розробників), який без додаткових модифікацій можна було використовувати для створення примітивних цифрових підписів. Незабаром після RSA були розроблені інші електронні цифрові підписи, такі як алгоритми цифрового підпису Рабіна, Меркле. У 1984 році Шафі Гольдвассер, Сільвіо Мікалі і Рональд Ривест першими чітко визначили вимоги безпеки до алгоритмів цифрового підпису та моделі атак на них [2, с. 18-19].

С. Бернет і С. Пейн вважають, що електронний підпис – це будь-який знак або процедура, реалізовані електронними засобами, тобто виконані або прийняті стороною, що бере участь, з наміром пов'язати запис із зобов'язанням або засвідчити справжність запису [2, с. 289].

Відповідно до наведеного визначення електронним підписом може бути вихідний сигнал складного біометричного пристрою, такого, наприклад, як система комп'ютерного розпізнавання відбитків пальців або просте введення імені в кінці електронного повідомлення, тобто технологія його створення електронними засобами не має значення.

Н. І. Соловяненко також вказує на те, що пов'язані з електронним документом символи, коди, паролі тощо можуть розглядатися як електронний підпис, якщо вони виконані або прийняті сторонами за взаємною згодою та з явним наміром підтвердити справжність написаного [3, с. 76].

Для подолання протиріч в 2003 році, хоча передумови до цього склалися набагато раніше, Верховною Радою України були прийняті Закони «Про електронні документи та електронний документообіг» та «Про електронний цифровий підпис».

Саме вказані закони визначають поняття та регулюють процес використання зазначених вище категорій. Отже, електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. А для ідентифікації автора електронного документа може використовуватися електронний підпис. І саме накладанням електронного підпису завершується створення електронного документа [4]. В той же час, Закон України «Про електронний цифровий підпис» зазначає, що електронний підпис – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних. А електронний цифровий підпис – це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. В свою чергу, відкритий ключ – це параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису [5].

Існує кілька схем побудови цифрового підпису: на основі алгоритмів симетричного та асиметричного шифрування. Перша схема передбачає наявність у системі третьої особи, що користується довірою обох сторін. Авторизацією документа є сам факт зашифрування його секретним ключем і передача його третій стороні. А що стосується другої схеми, то, на даний момент, вона є найбільш поширена і знаходить широке застосування. 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 електронних підписів.

На думку А. Гарибян, електронний цифровий підпис володіє двома основними властивостями:

1) відтворений він тільки однією особою, а його справжність може бути засвідчена і багатьма;

2) він нерозривно пов'язаний з конкретним документом і тільки з ним [6, с. 12].

На думку Є. Каменєвої, використання електронного підпису дозволяє здійснити:

1) контроль цілісності переданого документа: при будь-якій випадковій або навмисній зміні документа підпис стане недійсним, тому що він обчислений на підставі вихідного стану документа і відповідає лише йому;

2) захист від змін (підроблення) документа: гарантія виявлення підробки при контролі цілісності робить підроблення недоцільним у більшості випадків;

3) неможливість відмови від авторства, так як створити коректний підпис можливо лише знаючи закритий ключ, а він повинен бути відомим тільки власнику, а тому власник не може відмовитися від свого підпису під документом;

4) доказове підтвердження авторства документа: оскільки закритий ключ повинен бути відомим тільки власнику, то власник пари ключів може довести своє авторство підпису під документом. Залежно від деталей визначення документа можуть бути підписані такі поля, як «автор», «внесені зміни», «мітка часу» тощо [7, с. 49-50].

Отже, по суті електронний цифровий підпис – це якась послідовність символів, яка отримана в результаті певного перетворення початкового документа (або будь-якої іншої інформації) за допомогою спеціального програмного забезпечення. Будь-яка зміна вихідного документа робить електронний цифровий підпис недійсним, а на практиці він є унікальним для кожного документа і не може бути перенесений на інший документ; неможливість підробки електронного цифрового підпису забезпечується дуже великим обсягом математичних обчислень, необхідним для його підбору. Таким чином, при отриманні документа, підписаного електронним цифровим підписом, одержувач може бути впевнений в авторстві і незмінності тексту даного документа [8].

Відповідно до Закону України «Про електронний цифровий підпис» електронно-цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів. Він використовується фізичними та юридичними особами-суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі. Крім того, використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, встановлений законом для вчинення правочинів у письмовій формі [5].

С. О. Малофєєв вважає, що електронний цифровий підпис використовується в наступних випадках:

1) для електронних торгів: постачальник може підписати електронним цифровим підписом пропозицію на торгах і це гарантує юридичну значимість його пропозиції;

2) при укладанні договорів: якщо контракт підписано електронним цифровим підписом – він має юридичну силу. При цьому здійснюється підпис електронних документів, тобто можна, наприклад, підписати ним документ Word [9, с. 25].

Аналіз можливостей підробки підписів, в тому числі й електронних цифрових підписів, називається криптоаналіз. Спробу сфальсифікувати підпис або підписаний документ криптоаналітики називають «атака».

У своїй роботі Гольдвассер, Микали і Рівестом описують наступні моделі атак, які актуальні і в даний час:

1. Атака з використанням відкритого ключа. Криптоаналітик має тільки відкритий ключ.

2. Атака на основі відомих повідомлень. Правопорушник володіє допустимими підписами набору електронних документів, які йому відомі, але які він не має змоги обрати сам.

3. Адаптивна атака на основі вибраних повідомлень. Криптоаналітик може отримати підписи електронних документів, які він обирає сам [10].

Також у вказаній роботі описана класифікація можливих результатів таких атак:

1. Повний злом цифрового підпису. Отримання закритого ключа, що означає повний злом алгоритму.

Саме закритий ключ є найбільш вразливим компонентом всієї криптосистеми електронного цифрового підпису. Шахрай, 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.

На думку вчених та практиків, на даний час існують різноманітні засоби та пристрої зберігання закритого ключа, до яких можна віднести дискети, USB-брелок, Таблет-

ки Touch-Memory та смарт-карти. Саме остання вважається найбільш захищеним способом, оскільки для того, щоб використовувати смарт-карту, користувачеві необхідно не тільки її мати, але й ввести PIN-код, тобто, виходить двофакторна аутентифікація.

А, зважаючи на те, що крадіжка або втрата одного з таких пристроїв зберігання може бути легко помічена користувачем, відповідний сертифікат може бути негайно відкликаний.

2. Універсальна підробка цифрового підпису. Визначення аналогічного алгоритму підпису дозволяє підробляти підписи для будь-якого електронного документа.

3. Вибіркова підробка цифрового підпису. У цьому випадку зловмисник фабрикує два документи з однаковим підписом, і в потрібний момент підміняє один іншим.

4. Екзистенціальна підробка цифрового підпису. Правопорушник може спробувати підібрати документ до даного підпису, щоб підпис до нього підходив. Проте в переважній більшості випадків такий документ може бути тільки один.

Вважається, що самою «небезпечною» атакою є адаптивна атака на основі вибраних повідомлень, і при аналізі алгоритмів електронного цифрового підпису на криптостійкості потрібно розглядати саме її (якщо немає яких-небудь особливих умов) [10].

Отже, з огляду на вищевикладене, слід зазначити, що для гарантування інформаційної безпеки та попередження кримінальних правопорушень, вчинених шляхом підробки електронних документів, велику увагу слід приділяти електронному цифровому підпису. Для недопущення його підробки має бути встановлена відповідність певним принципам та вимогам.

Саме тому електронний цифровий підпис має володіти такими властивостями:

1) повинна бути можливість перевірити автора, дату і час створення підпису;

2) повинна бути можливість аутентифікувати зміст під час створення підпису;

3) підпис повинен бути перевірений третьою стороною на випадок необхідності вирішення спорів у майбутньому [10].

На підставі цих властивостей можна сформулювати наступні вимоги до електронного цифрового підпису:

1. Підпис повинен бути двійковим зразком, який залежить від тексту підписаного документа.

2. У підписі має бути використано певну унікальну інформацію підписувача для запобігання підробки.

3. Створювати цифровий підпис має бути відносно легко.

4. Підробка підпису повинна бути обчислювально неможливою як шляхом створення нового документа для існуючого цифрового підпису, так і шляхом створення підробленого цифрового підпису для справжнього документа.

5. Цифровий підпис має бути досить компактним і не займати багато пам'яті.

Щодо завдання захисту ключів від підробки, то дана проблема може бути вирішена за допомогою сертифікатів. Відповідно до Закону України «Про електронний цифровий підпис» сертифікат ключа – це документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача [5]. Сертифікат дозволяє засвідчити укладені в ньому дані про власника і його відкритий ключ підписом будь-якої довіреної особи. Існують системи сертифікатів двох типів: централізовані і децентралізовані. У децентралізованих системах шляхом перехресного підписування сертифікатів знайомих і довірених людей кожним користувачем будується мережа довіри. У централізованих системах сертифікатів використовуються центри сертифікації, підтримувані довіреними організаціями.

Саме центр сертифікації формує закритий ключ і власний сертифікат, а також сертифікати кінцевих користувачів і засвідчує їх автентичність своїм цифровим підписом. Також центр проводить відкликання минулих і скомпрометованих сертифікатів і веде бази виданих та відкликаних сертифікатів. Звернувшись в сертифікаційний центр, можна отримати власний сертифікат відкритого ключа, сертифікат іншого користувача і дізнатися, які ключі відкликані. І це є одним з найважливіших способів захисту електронних цифрових підписів від підробки, а електронних документів – від внесення змін до їх змісту.

ЛІТЕРАТУРА

1. Підробка підпису. Злочин і кара [Електронний ресурс]. – Режим доступу : http://svitohlyad.com.ua/zakon/pidrobka-pidpysu-zlochyn-i-kara/

2. Бернет С. Криптография. Официальное руководство RSA Security / С. Бернет, С. Пейн. – М. : Бином-Пресс, 2002. – 384 с.

3. Соловяненко Н. И. Юридическая роль электронной подписи в электронной коммерции / Н. И. Соловяненко // Предпринимательское право в XXI веке. – М. : МЗ-Пресс, 2002. – С. 67–83.

4. Про електронні документи та електронний документообіг : Закон України від 23 травня 2003 року [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/851-15

5. Про електронний цифровий підпис : Закон України від 22 травня 2003 року [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/852-iv

6. Гарибян А. Электронная цифровая подпись: правовые аспекты / А. Гарибян // Российская юстиция. – 1996. – № 11. – С. 12–13.

7. Каменєва Є. ЕЦП та електронне узгодження проектів документів з використанням СЕД / Є. Каменєва // Діловодство і документообіг на підприємстві. – 2009. – № 9. – С. 48–56.

8. Електронно-цифровий підпис як засіб захисту електронного документа [Електронний ресурс]. – Режим доступу : http://ukrbukva.net/72204-Elektronno-cifrovaya-podpis-kak-sredstvo-zashity-elektronnogo-dokumenta.html

9. Малофєєв С. О Застосуванні електронного цифрового підпису в електронному документообігу / С. О. Малофєєв // Секретарська справа. – 2009. – № 7. – С. 24–28.

10. Ткач Ю. М. Електронний цифровий підпис / Ю. М. Ткач [Електронний ресурс].– Режим доступу : http://uchil.net/?cm=167737