ЕЛЕКТРОННО-ЦИФРОВИЙ ПІДПИС ТА ОСОБЛИВОСТІ ЙОГО ВИКОРИСТАННЯ

Коваленко Ю.Б. [1], **Орлик О. В.** [2]

1 –студент, кафедра Інформаційних систем в економіці,
2 – канд. екон. наук, доцент, кафедра Інформаційних систем в економіці
Одеський національний економічний університет, м. Одеса

АНОТАЦІЇ

Коваленко Ю. Б., Орлик О. В. ***Електронно-цифровий підпис та особливості його використання.*** *Визначено, що електронно-цифровий підпис є одним із видів забезпечення цілісності та захисту електронних документів. Розглянуто процес підписання електронного документа та наведено переваги використання електронного цифрового підпису.*
Ключові слова: *електронний підпис, ідентифікація підписувача, підпис, захист електронних даних.*

Коваленко Ю. Б., Орлик О. В. ***Электронно-цифровая подпись и особенности ее использования.*** *Определено, что электронно-цифровая подпись является одним из видов обеспечения целостности и защиты электронных документов. Рассмотрен процесс подписания электронного документа и приведены преимущества использования электронной цифровой подписи.*
Ключевые слова: *электронная подпись, идентификация подписанта, подпись, защита электронных данных.*

Kovalenko Y. B., Orlyk O. V. ***Digital signature and distinctive features of its usage.*** *It is determined that the digital signature is one of types of providing integrity and protection of electronic documents. In addition, it reviews the process of signing an electronic document and highlights advantages in its usage.*
Keywords: *electronic signature, signer authentication, signature, electronic data protection.*

Коваленко, Ю. Б. *Електронно-цифровий підпис та особливості його використання* [Текст] / Ю. Б. Коваленко, О. В. Орлик // Інформатика та інформаційні технології : студ. наук. конф., 20 квітня 2015 р. : матер. конф. — Одеса, ОНЕУ. — С. 16-19.

Розвиток глобальних комунікацій в діловому і повсякденному житті привів до появи нової області взаємовідносин, предметом яких є електронний обмін даними. Проблема збереження електронних документів від копіювання, модифікації і підробки вимагає для свого вирішення специфі-

чних засобів і методів захисту. Одним з поширених в світі засобів такого захисту є електронний цифровий підпис, який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документу, його реквізитів і факту підписання конкретною особою.

Електронний цифровий підпис (ЕЦП) – 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.

Оригіналом електронного документа вважається електронний примірник з електронним цифровим підписом автора.

Електронний цифровий підпис призначений для використання фізичними та юридичними особами – суб'єктами електронного документообігу:

— *для ідентифікації підписувача;*

— *для підтвердження цілісності даних в електронній формі;*

Електронний цифровий підпис, як засіб контролю походження і цілісності інформації, є ефективним інструментом забезпечення інформаційної безпеки на всіх рівнях інфраструктури суспільства: від персональної інформаційної безпеки людини до інформаційної безпеки держави. Тому ЕЦП, зокрема, і інфраструктура відкритих ключів, у цілому, є стратегічною оборонною технологією, від якості й надійності реалізації якої залежить інформаційна безпека України.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. За правовим статусом він прирівнюється до власноручного підпису (печатки). Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа. За умови правильного зберігання власником секретного (особистого) ключа його підробка неможлива. Електронний документ також не можливо підробити: будь-які зміни, не санкціоновано внесені в текст документу, будуть миттєво виявлені.

Підписання електронного документу ЕЦП

При підписанні електронного документу 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» (messagedigest).

Цей відбиток має такі особливості:

— *фіксовану довжину, незалежно від довжини повідомлення;*

— *унікальність відбитку для кожного повідомлення;*

— *неможливість відновлення повідомлення по його відбитку.*

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

Розшифрувати ЕЦП і одержати початковий відбиток, який відповідатиме документу, можна тільки використовуючи Сертифікат відкритого ключа автора. Таким чином, обчислення відбитку документу захищає його від модифікації сторонніми особами після підписання, а шифрування особистим ключем автора підтверджує авторство документу.

Переваги використання електронного цифрового підпису:

— *Всебічна економія ресурсів та удосконалення бізнес-процесів на підприємстві. Ведення електронного документообігу на підприємстві істотно зменшує обсяги паперової бухгалтерської документації, економить час співробітників і витрати підприємства, пов'язані з укладанням договорів, оформленням платіжних документів, та їх пересиланням.*

— *Простота і зручність використання. Використання ЕЦП напрочуд просте і доступне будь-якій людині незалежно від рівня володіння персональним комп'ютером, освіти та роду занять.*

— *Конфіденційність інформації. Неможливість доступу до неї будь-якої особи, що не володіє секретним кодом) забезпечується завдяки надійним криптографічним перетворенням.*

— *Безпека інформації. Безпека використання ЕЦП гарантується тим, що надійні засоби, які використовуються для роботи з ЕЦП, проходять експертизу в Державній службі спеціального зв'язку та захисту інформації України.*

— *Можливість ведення електронного документообігу з державними структурами. Зручність використання одних і тих ж засобів ЕЦП при обміні даними з усіма міністерствами, відомствами, при подачі звітності в будь-які контролюючі органи, що приймають звіти в електронній формі на території Україні.*

— *Ведення ділових відносин на сучасному рівні. Використання ЕЦП істотно прискорює проведення будь-яких комерційних операцій і виключає необхідність додаткових зустрічей і багатогодинних переговорів.*

Розвиток, а також використання електронно-цифрового підпису (ЕЦП) як засобу для захисту електронних документів забезпечує конфіденційність та безпечність її збереження; захищає від підробки, а також від зміни або спотворення інформації, що міститься в документі. Застосування ЕЦП несе багато переваг його використання в діяльності фізичних та юридичних осіб.

ЛІТЕРАТУРА

1. Електронний цифровий підпис [Електронний ресурс] // Портал : uakey.com.ua. — Режим доступу \www/ URL: http://www.uakey.com.ua/. — Заголовок з екрана, доступ вільний, 24.03.2015.
2. Електронний цифровий підпис [Електронний ресурс] // Портал : softline.kiev.ua. — Режим доступу \www/ URL: http://www.softline.kiev.ua/ua/elektronnij-dokumentoobig/51-produkti-ta-servisi/za-vidami-diyalnosti/proektnij-biznes/avtomatizatsiya-biznesu/560-elektronnij-tsifrovij-pidpis.html. — Заголовок з екрана, доступ вільний, 24.03.2015.
3. Закон України «Про електронний цифровий підпис» [Електронний ресурс] // Портал : zakon4.rada.gov.ua. — Режим доступу \www/ URL: http://zakon4.rada.gov.ua/laws/show/852-15. — Заголовок з екрана, доступ вільний, 24.03.2015.
4. Yesina, O. G. The information security software in business [Електронний ресурс] / O. G. Yesina, L. N. Lingur // Економіка: реалії часу. Науковий журнал. — 2013. — № 5 (10). — С. 175-180. — Режим доступу \www/ URL: www.economics.opu.ua/files/archive/2013/No5/175-180.pdf. — Заголовок з екрана, доступ вільний, 24.03.2015.
5. Орлик, О. В. Економічна безпека підприємства: властивості, стратегія та методи забезпечення [Текст] / О. В. Орлик // Економічна безпека в умовах глобалізації світової економіки : [колективна монографія у 2 т.]. — Дніпропетровськ : «ФОП Дробязко С.І.», 2014. — Т. 2. — С. 176-182.
6. Йона, О. О. Світові тенденції боротьби з кіберзлочинністю [Текст] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2013. — № 15(204). — Ч. 1. — С. 59-62.
7. Орлик, О. В. Факторы обеспечения и основные свойства экономической безопасности [Текст] / О. В. Орлик // Modern problems of regional development : Collection of scientific articles. — 2014. — Vol. 2. — P. 190-194.
8. Корольов, М. В. Проблематика дослідження питань інформаційної безпеки у державному управлінні [Текст] // М. В. Корольов, О. О. Скопа / Вісник Східноукраїнського національного університету імені Володимира Даля. — Луганськ : СНУ ім. В. Даля. — 2013. — №15(204). — Ч. 1. — С. 88-93.
9. Орлик, О. В. Фінансово-економічна безпека підприємства та підходи до її забезпечення [Електронний ресурс] / О. В. Орлик // Інформаційна та економічна безпека : міжнар. наук.-практ. конф., 2014 р. : матер. конф. — Х. : ХІБС УБС НБУ. — 1 електрон. опт. диск (CD-ROM). — Систем. вимоги: Pentium ; 512 Mb RAM ; Windows XP, 7, 8 ; Adobe Acrobat Reader 5.0-10.0. — Назва з екрану.
10. Рыбальский, О. В. Защита информации на промышленном предприятии / О. В. Рыбальский, Л. Н. Скачек, В. А. Хорошко // Сучасна спеціальна техніка. — 2010. — № 3 (22). — С. 24-32.
11. Орлик, О. В. Методи управління фінансово-економічною безпекою [Текст] / О. В. Орлик // Сборник научных трудов SWorld. — 2014. — Т. 28. — №. 1. — С. 37-41.