УДК 004.056.55:651

ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС ЯК ЗАСІБ ЗАХИСТУ ІНФОРМАЦІЇ НА ВІТЧИЗНЯНИХ ПІДПРИЄМСТВАХ

Роїк О. М., д.т.н., професор

Азарова А. О., к.т.н., доцент

Года К. О.

Вінницький національний технічний університет

У статті проаналізовано сутність та структуру електронного цифрового підпису. Досліджено проблеми, з якими стикаються вітчизняні підприємства під час користування ЕЦП. Розроблено рекомендації та пропозиції щодо вирішення проблем, пов’язаних із застосуванням цифрового підпису.

Ключові слова: електронний документообіг, електронний цифровий підпис (ЕЦП), таємний ключ, відкритий ключ, компрометація, сертифікат.

The nature and structure of the digital signature are analyzed in the article. The problems which are faced by domestic companies while using EDS are considered. The recommendations and suggestions for resolving problems associated with the use of the digital signature are designed.

Key words: electronic document management, digital signature (EDS), a secret key, public key compromise, certificate.

Актуальність проблеми. Сьогодні необхідно мати доступ до інформаційних ресурсів і скоротити часові витрати на розв'язання задач, не пов'язаних з обслуговуванням громадян. Відсутність необхідності вручну розмножувати документи, відслідковувати переміщення паперових документів всередині організації, контролювати порядок передавання конфіденційної інформації істотним чином знижує трудовитрати діловодів. Одним із найбільш продуктивних засобів усунення сучасних діловиробничих проблем є електронний документообіг, оскільки він є високотехнологічним і

прогресивним підходом до суттєвого підвищення ефективності роботи фірм, установ та організацій.

Проте впровадження його на підприємстві стикається із проблемою захисту інформації. Тому ключовим моментом створення систем електронного бізнесу та запобігання фінансовим і нефінансовим ризикам стала система організації та запровадження електронного підпису.

Серед найбільш поширених та актуальних прикладних задач, які вирішуються за допомогою цифрового підписування, є такі:

– створення безпеки електронного документообігу;

– убезпечення електронних платіжних систем та електронної комерції;

– забезпечення авторства при електронному голосуванні;

– підписування повідомлень електронної пошти;

– аутентифікація (процедура встановлення належності користувачеві інформації в системі пред’явленого ним ідентифікатора) у бездротових мережах;

– створення безпеки мобільної комерції;

– безпечність стільникового зв'язку;

– підписування цифрових сертифікатів та цифрових паспортів на базі смарт-карток.

Аналіз останніх наукових досліджень. Серед провідних дослідників, які займалися вивченням питань, аналізованих у статті, слід зазначити таких закордонних вчених, як Ю. М. Батуріна, І. Л. Бачило, Г. Г. Абрамкін, Ю. Хаяші [1-2] та вітчизняних: В. А. Лужецький, В. В. Гніліцький, К. Єрохін, М. Р. Макарова, А. В. Чучковська, В. І. Міщенко, Г. В. Юрчук, В. Б. Аверьянов, В. М. Антонов та ін. [2-5].

Отже, за сучасних умов, застосування ЕЦП є досить актуальним.

Метою дослідження статті є підвищення рівня інформаційної безпеки суб’єктів господарювання за допомогою використання електронного підпису.

Виклад основного матеріалу дослідження. Електронний цифровий підпис (ЕЦП) – це блок інформації, який додається до файлу даних автором та захищає файл від несанкціонованої модифікації і вказує на підписувача [3].

Дані щодо створення підпису − унікальні дані, такі, як коди або приватні шифрувальні ключі, які використовує власник підпису для створення електронного підпису.

Пристрій для створення підпису − це програмне забезпечення певної конфігурації або апаратний комплекс, що використовується для застосування даних щодо створення підпису.

Для функціонування ЕЦП використовуються два ключі захисту (які зберігаються в різних файлах) [4]:

– таємний (особистий, закритий) ключ, який зберігається у підписувача;

– відкритий ключ, який, як правило, публікується в зальнодоступному або спеціалізованому довіднику.

Для накладання ЕЦП використовується таємний (особистий) ключ, а для його перевірки – відкритий (загальновідомий) ключ [2].

Накладання електронного цифрового підпису (підписування) – це операція, яка здійснюється відправником документа з використанням його таємного ключа. При виконанні цієї операції на вхід відповідної програми подаються дані, які треба підписати, та таємний ключ підписувача. Програма створює з даних за допомогою таємного ключа унікальний блок даних фіксованого розміру, який може бути справжнім тільки для цього таємного ключа та саме для цих вхідних даних. Тобто ЕЦП – це своєрідний «цифровий відбиток таємного ключа і документа» [2].

Надалі ЕЦП, як правило, додається до вхідного документа (або розміщується в окремому полі документа), і така комбінація даних (документ + ЕЦП) утворює захищений електронний документ

Перевірка електронного цифрового підпису – це операція, яка виконується отримувачем захищеного електронного документа з використанням відкритого ключа підписувача. Для виконання цієї операції необхідно отримати

відкритий ключ відправника та захищеного документа. Відповідний програмний модуль перевіряє, чи дійсно цифровий підпис відповідає документу та відкритому ключу. Якщо в документ або у відкритий ключ внесено будь-які зміни, перевірка закінчується негативним результатом [2].

У зв’язку з такою структурою ЕЦП постає проблема захисту його від фальсифікації. Зловмисник може тим або іншим чином отримати доступ до закритого ключа. В таких випадках застосовують термін компрометація особистого ключа – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа [6]. Це, у свою чергу, спричиняє компрометацію електронного підпису, створеного з допомогою закритого ключа. Таємний ключ може бути сфальсифікований різними способами, які можна умовно класифікувати як традиційні й нетрадиційні. Традиційні способи компрометації, як правило, пов'язані із крадіжкою та іншими протизаконними діями. Але це дозволяє якоюсь мірою розраховувати на те, що захист ключа, хоча і опосередковано, забезпечує законодавство.

На жаль, це не стосується нетрадиційних методів компрометації, заснованих на реконструкції закритого ключа за даними, одержаними цілком реально, зокрема, застосовуючи відкритий ключ. Достатньо просто повідомити потенційному відправнику таємної інформації підроблений ключ і, перехопивши таємне повідомлення, отримати доступ до конфіденційної інформації. Довести незаконність дій з реконструкції чужого закритого ключа практично неможливо.

Ще однією проблемою при веденні електронного документообігу та використання цифрового підпису для вітчизняних підприємств є відсутність чіткої законодавчої бази, яка б врегулювала систему функціонування електронного документообігу і стандартизувала процес накладання та перевірки ЕЦП. Україна нескінченно далека від упровадження систем електронного документообігу та цифрового підпису. Основними перешкодами, які не дозволяють нам перейти від «паперової епохи» – дорогої, неефективної і неконкурентоспроможної до електронної є:

1) безсистемність. Вона полягає у тому, що відсутність єдиної державної політики та координації призвела до повного хаосу в електронних системах управління. В одній податковій адміністрації електронний документообіг забезпечують одразу три центри сертифікації ключів, які між собою не сумісні;

2) незахищена програмна платформа. На українських підприємствах спостерігається повна незахищеність баз даних, оскільки вони будуються на імпортному програмному забезпеченні з різними форматами кодування;

3) нелегітимність нинішньої системи видачі цифрових підписів. Центральний засвідчувальний орган із січня 2009 року формально не має права видавати підписи, оскільки не відповідає вимогам безпеки, а дію постанови Кабінету Міністрів, що регламентує його роботу, частково припинено. А отже, всі підприємці, котрі за останні 3 роки купили ЕЦП, можуть подати до суду і виграти справу в держави.

Глибоко дослідивши та проаналізувавши проблеми, з якими стикаються вітчизняні підприємства під час користування електронним цифровим підписом, автори статті пропонують такі шляхи їх подолання. Проблему захисту особистих ключів від пошкодження, модифікації, замінювання можна вирішити за допомогою сертифікатів. Під сертифікатом розуміють електронне засвідчення, яке встановлює зв'язок між даними щодо сертифікації підпису і власником підпису та підтверджує його особу.

За використання сертифікованих засобів криптографічного захисту інформації гарантом якості виконання основної функції й відсутності побічної дії виступає Департамент спеціальних телекомунікаційних систем захисту інформації Служби безпеки України. А при використанні несертифікованих засобів криптографічного захисту інформації таких гарантій не може дати ніхто.Тобто використання сертифікатів суттєво знижує ризик фальсифікації ключів.

Що стосується другої проблеми, яка пов’язана із відсутністю чіткої законодавчої бази врегулювання системи функціонування електронного документообігу та стандартизації процесу накладання і перевірки ЕЦП, то

авторами розроблені пропозиції та рекомендації для її подолання. На рівні держави слід:

- створити спеціальний орган, який визначатиме ідеологію електронної реформи, і визначити відомство, яке відповідатиме за жорстку і послідовну реалізацію цієї реформи в усіх сферах;
- уніфікувати програмне забезпечення і розробити єдині стандарти зберігання та передавання даних, щоб гарантувати контроль;
- терміново ввести ситуацію із засвідчувальними центрами в законне русло, щоб уникнути потенційних матеріальних збитків.

Висновок. Провівши дане дослідження, автори статті рекомендують використовувати сертифіковані засоби криптографічного захисту, оскільки, вони знижують ризики фальсифікації ЕЦП. Крім того, слід законодавчо врегулювати систему електронного документообігу, а також розробити стандарти, що дозволять спростити процес накладання та перевірки ЕЦП.

Список використаних джерел

1. Новицька Н.Б. Організаційно-правові аспекти інформаційної культури в управлінській діяльності: дис. … канд. юрид. наук.: 12.10.07/ Національна академія держ. податкової служби України. – Ірпінь, 2007. – 210 с.

2. Лужецький В.А. Інформаційна безпека: посібник / В.А. Лужецький, О.П. Войтович, А.В. Дудатьєв. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 240 с.

3. Гніліцький В.В. Захист інформації: навч. посібник для студентів економічних спеціальностей / В.В. Гніліцький, Є.Г. Орєхов. – Житомир: ІМІДЖ, 2009. – 164 с.

4. Макарова М.Р. Електронна комерція: посібник для студентів вищих навчальних закладів / М.Р.Макарова. – К.: Видавничий центр «Академія», 2002. – 272 с.

5. Чучковська А.В. Правове регулювання електронної комерції в Україні: навч. посіб. / А.В. Чучковська. – К.: Центр учбової літератури, 2007. – 224 с.

6. Про електронний цифровий підпис: Закон України від 22.05.2003 // Відомості Верховної Ради України (ВВР). – 2003. – N 36. – ст.276.