

ПРОБЛЕМИ ЗАСТОСУВАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПISУ

студент: **Борель Н.В.**
(науковий керівник, ст. викл.: **Лисня В.І.**)

Застосування глобальних комунікацій в економічній діяльності та повсякденному житті привело до появи принципово нового виду відносин, пов'язаних з обміном інформацією без використання паперових носіїв - з електронним обміном з використанням електронних документів. Під електронним документом мають на увазі документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, зокрема електронний цифровий підпис - вид електронного підпису, який дає змогу підтвердити його цілісність та ідентифікувати підписувача.

Електронний цифровий підпис визнається реквізитом електронного документа, призначення якого - захищати підписаний документ від усіх можливих дій зловмисників.

Сутність цифрового підпису полягає в тому, що для гарантованого підтвердження достовірності інформації електронного документа, а також для можливості доведення третій стороні, що електронний документ був складений конкретною особою або за його дорученням і саме в такому вигляді, в якому він пред'явлений, автору документу пропонується обрати своє індивідуальне число (зазвичай називається індивідуальним, секретним ключем). Кожного разу для «цифрового підписування» необхідно згорнути цей свій секретний ключ вмістом конкретного електронного документа. Результат такого згортання - інше число - може бути названий цифровим підписом даного автора під даним конкретним документом.

Механізми цифрового підпису ґрунтуються на алгоритмах асиметричного шифрування, коли для шифрування використовується один загальнодоступний ключ, а для дешифровки - інший, що є секретним, при цьому знання загальнодоступного ключа не дозволяє визначити секретний ключ. Вони включають дві процедури: формування підпису відправником та її розпізнавання (верифікацію) одержувачем.

Підробити електронний цифровий підпис, а разом з ним і засвідчений документ, неможливо, адже це потребуватиме величезної

кількості обчислень, які не можуть бути реалізовані за сучасного рівня математики й обчислювальної техніки, поки інформація, що міститься в підписаному документі, є актуальною.

Електронний документообіг є одним з тих інструментів, що в змозі забезпечити потреби сьогодення в швидкому інформаційному обміні. Документи можуть бути засвідчені електронним цифровим підписом і передані до місця призначення протягом декількох секунд, адже електронний документ передається за допомогою швидкісних телекомунікаційних систем, однією з яких є, наприклад, інтернет.

За таких умов усі учасники обміну електронними документами незалежно від відстані мають однакові можливості в електронному інформаційному обміні, тому документообіг з використанням електронного цифрового підпису невдовзі посяде домінуюче місце у системі опрацювання, підготовки, підписання та надсилання документу.

Не викликає сумніву, що впровадження електронного цифрового підпису є загальнодержавним завданням для нашої країни. Проте для достаточного масового використання електронного цифрового підпису в Україні необхідно прийняти низку нормативно-правових актів, зокрема щодо архівного зберігання електронних документів; щодо національних стандартів; щодо вимог до засобів електронного цифрового підпису, форматів даних, які для цього використовуються. Здосконалення та оновлення нормативно-правової бази України, створення спеціальних юридичних норм сприятиме ефективному функціонуванню електронного цифрового підпису та електронного документообігу.

Всебічне використання електронного цифрового підпису дасть можливість не тільки спростити та прискорити документообіг між суб'єктами господарювання та зміцнити конкурентоспроможність вітчизняних підприємств, а й створити умови для розвитку експортно-імпорتنих операцій, електронної торгівлі, електронних банківських послуг, повномасштабного дистанційного навчання та надання медичних послуг із застосуванням новітніх інформаційних технологій. Окрім цього, впровадження електронного цифрового підпису закладе організаційно-технічну основу для надання електронних інформаційних послуг органами державної влади та органами місцевого самоврядування юридичним та фізичним особам при використанні інтернету.