УДК 004.773.3
DOI https://doi.org/10.32838/2663-5941/2021.2-1/14

Василенко М.Д.
Національний університет «Одеська юридична академія»

Золотоверх Д.С.
Національний університет «Одеська юридична академія»

Новіков В.П.
Національний університет «Одеська юридична академія»

Рачук В.О.
Національний університет «Одеська юридична академія»

ТЕХНІКО-КОНФІДЕНЦІЙНІ АСПЕКТИ ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ ЕЛЕКТРОННО-ЦИФРОВОГО ПІДПИСУ

У статті розкрито зміст поняття ЕЦП та визначено, від чого залежить його надійність. Продемонстровано, яким чином ЕЦП здійснює підпис з забезпеченням надійної конфіденційності. Відзначено, що ЕЦП завжди потребує збереження конфіденційності, підтримання якої унеможливлює отримання інформації не уповноваженою особою, представляючи собою сукупність даних, отриманих за результатом певного криптографічного перетворення деякого набору даних. ЕЦП створюється на основі гешу повідомлення, що надає йому можливість бути сталою довжиною достатньою простотою будь-яких повідомлень. Наведено характеристики геш-функції у вигляді комп'ютерного алгоритму, що перетворює масив даних довільної довжини у рядок бітів визначної довжини. Показано на практиці, як це відбувається з використанням відкритого і закритого ключів. Установлено, які загрози можуть виникати в зв'язку з використанням геш-функції. Визначено, які види шифрування використовують алгоритми ЕЦП. Розглянуто окремі алгоритми на практиці, встановлено основні кроки створення ЕЦП. Визначено, що використання відкритого ключа та вдосконалення норм діючого законодавства є ключовими напрямами вдосконалення ЕЦП. Описано види підробок і шляхи їх відтворення. Відображено механізм збереження та посилення конфіденційності під час передачі такого підпису, а також його законодавче закріплення в контексті змін, пов'язаних з розвитком інформаційних технологій. При цьому розвиток останніх завжди випереджає розвиток удосконалення законодавства. Як вагомий позитивний крок відзначено прийняття Закону України «Про електронні довірчі послуги», але зроблено застереження, що наразі потрібні технічні та організаційні доробки питань, пов'язаних саме з ЕЦП. Розкриттям сутності ЕЦП практично доведено, що, відображаючи організацію гарантованого застосування ЕЦП криптографічною системою з відкритим ключем, за якої відкритий ключ передається по відкритому (незахищеному) каналі та використовується як для перевірки ЕЦП, так і для шифрування повідомлення, слід констатувати його підвищену конфіденційність та надійність і те, що його практично неможливо підробити.

Ключові слова: *підпис, електронно-цифровий, конфіденційність, ключ, геш-функція, шифрування.*

Постановка проблеми. В усі часи підписи здійснювалися та й продовжують здійснюватися власноруч підписантами. Так званий «мокрий» підпис, який має бути зроблено ручкою з чорнилом відповідного (чорного, фіолетового) кольору або за допомогою «шарикової» ручки, є підтвердженням візуалізації підписаного документа. Впровадження глобальних комунікацій спонукало розвиток систем електронного обміну даними, користувачами яких виступають як різні установи, так і громадяни. Електронно-цифровий підпис (ЕЦП) почав використовуватися в повсякденній діяльності поряд з рукописним підписом і був покликаний стати аналогом рукописного підпису. Зазвичай рукописний підпис використовується як реквізит, що надає документу юридичну силу, а особа, яка його підписала, несе відповідальність за його зміст. ЕЦП має схожі цілі, але має дещо інший вигляд, на відміну від рукописного, бо він є числом, двійковим кодом, що зберігається в пам'яті комп'ютера. Якщо рукописний підпис є унікальним за рахунок певних письмово-рухових навичок, що характерні для кожної людини, то цифровий підпис відбувається завдяки певній про-

цедурі формування, параметри якої відомі лише особі, що здійснює такий підпис. При цьому саме підпис потребує збереження в комп'ютерній системі таких ознак інформації, як конфіденційність, цілісність, автентичність (справжність). Слід зауважити, що саме конфіденційність полягає у неможливості отримання інформації не уповноваженою особою, а цілісність полягає у неможливості будь-якої трансформації інформації не уповноваженою особою або ж уповноваженою, але без обґрунтованої на те мети. Такою трансформацію є його зміна, спотворення або взагалі знищення. Отже, ЕЦП представляє собою сукупність даних, отриманих за результатом певного криптографічного перетворення деякого набору даних, яка додається до цього набору даних або логічно поєднується з ним та надає можливість підтвердити його цілісність і спроможність, а також перевірити автентичність особи, яка підписалася. При цьому залишається важливим і те, що необхідно враховувати також доступність підпису, як властивість інформації бути отриманою уповноваженою особою за розумну кількість часу, а також підтвердження автентичності. Остання представляє собою властивість, що полягає ідентифікації заявленого ресурсу та ресурсу, який насправді визначається як джерело достовірної інформації. В зв'язку з вищенаведеним слушно зауважити, що конфіденційність, як цілісність та доступність самої інформації, залишається важливим складником теорії інформації та кодування, складаючи принципову характеристику ЕЦП.

Аналіз останніх досліджень і публікацій. У відомих публікаціях, які були узагальнені в монографії [1], охоплені різні сторони теоретичних та практичних питань, пов'язаних з ЕЦП. Так, у цій же монографії [1] в тому числі обговорено стан та сутність деяких проблемних питань теорії та практики аналізу синтезу та застосування ЕЦП в інформаційних та інформаційно-телекомунікаційних системах різноманітного призначення. Наводяться результати класифікації, обґрунтування вимог і порівняльного аналізу механізмів і криптологічних протоколів на основі ЕЦП на час написання згаданої монографії. Попри достатню кількість розробок щодо ЕЦП, існують певні «вузькі місця» в цих дослідженнях (див. також [1]). У роботі [2] зроблено аналіз нових методів для формування ЕЦП, котрі базуються на нових математичних основах. Прийнято вважати, що кодова криптографія виявляється ефективною для побудови схем направленого шифрування та інкапсуляції ключів, тоді як для формування та перевірки цифрового підпису вона не є раціональним рішенням через високу обчислювальну складність [3]. Сьогодні добре відомо, що конфіденційна інформація передається або зберігається таким чином, що неавторизований користувач не може розкрити її зміст. З цією метою первинна (відкрита) інформація підлягає криптологічному перетворенню та подальшому її зберіганні або передачі в перетвореному вигляді [4; 5, с. 129].

У роботах [6–8] розглядається кодова схема ЕЦП щодо її ефективності в порівнянні з поширеною альтернативою схемою CFS [9]. Йдеться про відчутне зниження обчислювальних затрат на формування підпису, що є вагомим практичним кроком для подолання основного недоліку кодових схем ЕЦП. Порівняльний аналіз методів й алгоритмів створення / перевірки ЕЦП показав, що одними з найпоширеніших стали алгоритми DSA (англ. DigitalSignatureAlgorithm) та RSA (RivestShamirAdleman) з використанням відкритого ключа (RSA став першим стандартизованим алгоритмом ЕЦП, який заснований на обчислювальній складності взяття логарифмів в кінцевих полях – авт.). Під час їх використання тільки один суб'єкт реально може створити геш-значення повідомлення, але будь-хто може перевірити його коректність. Таким чином, можна стверджувати, що більш-менш достатньою мірою розроблено застосування ЕЦП, у яких використовується різний математичний апарат за умови досягнення різних кількісних показників якості. При цьому існують обмеження з точки зору вибору параметрів генерування ключів, тобто фактично параметра криптографічного алгоритму ЕЦП, доступного суб'єктам відносин у сфері використання такого підпису. Однак існують також певні прогалини в реалізації конфіденційності в практичній площині самого підпису.

Постановка завдання. Метою статті є демонстрація практичних технічних можливостей на реалізацію ЕЦП за умови дотримання його зростаючої конфіденційності з встановленням її прийнятності.

Виклад основного матеріалу дослідження. Не викликає сумнівів той факт, що всі алгоритми ЕЦП не є ідеальними криптосистемами. Це можна пояснити тим, що усі алгоритми ЕЦП використовують ключі шифрування сталої довжини і, як наслідок, вразливі до атаки грубою силою. При цьому ЕЦП представляє собою вид електронного підпису, отриманого завдяки саме криптографічному перетворенню даних, що до них додаються, або поєднується з ними логічно. Надійність ЕЦП

принципово залежить від автентичності, аутентифікації повідомлення, а також заперечення невизнання участі учасників. І тут, для автентичності, важливим фактором виступає впевненість у тому, що повідомлення не було змінено під час його передачі по каналу. Аутентифікація повідомлення передбачає перевірку його адресанта. ЕЦП в комп'ютерних мережах дає змогу впевнитись у тому, хто насправді надіслав повідомлення. Невизнання участі фактично означає невизнання одного з об'єктів комп'ютерною системою події, яка відбулася. Невизнання характеризується як відмовою від авторства (заперечення причетності до утворення або передачі інформації), так і відмовою на одержання – заперечення причетності до отримання інформації. ЕЦП не дає змогу учасникам (адресанту та адресату) заперечувати причетність до процесу комунікації.

Підпис, завдяки математичним перетворенням, залежить від змісту повідомлення. Зазвичай підпис створюється на основі гешу повідомлення, що надає йому можливість бути сталою довжиною, а також надає обчислювальної простоти у випадках великих повідомлень.

Геш-функція представляє собою комп'ютерний алгоритм, що перетворює масив даних довільної довжини на рядок бітів визначної довжини (геш). У цьому разі ознаки геш-функції можна охарактеризувати наступним чином.

1. Гешування ідентичного повідомлення створює ідентичний геш.

2. Не потребує великої кількості обчислювальних ресурсів.

3. Наявність лавинного ефекту (мала зміна у повідомлені) призводить до значної зміни гешу.

4. Наявність низької вірогідності знаходження однакового гешу для різних повідомлень, коли обчислення такої пари повідомлень неможливо провести за визначений період часу.

Повідомлення, що підписане ЕЦП, складається з двох частин, власне самого повідомлення та підпису, як зображено на рис. 1. Якщо узагальнити моделі ЕЦП (див. [1, с.]), можна дійти висновку, що всі алгоритми мають однакову схему. Загалом одні моделі відрізняються від інших саме математичними перетвореннями, що використовуються.

В той же час усі алгоритми ЕЦП використовують асиметричне шифрування, хоча ЕЦП можна побудувати навколо симетричного шифрування, такий алгоритм не буде надавати інформації, що передається, а тоді проявляються ознаки невизнання участі. Асиметричне шифрування передбачає використання закритого та відкритого ключа. Така назва пов'язана з використанням різних ключів під час шифрування та дешифрування, на відміну від симетричного шифрування, в якому такі ключі є ідентичними. Під час асиметричного шифрування відкритий ключ розповсюджується, а закритий – зберігається та є секретом, який має бути відомим тільки для особи, що здійснює підпис.

Для розповсюдження відкритого ключа в ЕЦП використовують сертифікат. Асиметричне шифрування в ЕЦП передбачає шифрування гешу. Головна мета шифрування в алгоритмі ЕЦП полягає в тому, що можна було б перетворити геш таким чином, щоб здатність зашифровувати належала лише особі, яка здійснює підписання (використовуючи закритий ключ), а здатність до розшифровування може здійснювати будь-хто відкритим ключем. Саме асиметричність надає можливість перевірити, хто здійснив ЕЦП, чи є ця особа такою, якій надано доступ до закритого ключа. У разі процесу створення ЕЦП поділяється на дві частини: створення підпису та його підтвердження (верифікація). При цьому повідомлення, що потрібно підписати, гешується. Повідомлення перетворюється на достатньо невелике число (порівняно з розміром повідомлення). Це пов'язано з тим, що, по-перше, геш у своїй більшості набагато швидше зашифровується, ніж саме повідомлення; по-друге, зашифрована інформація завжди має сталу довжину (залежить від обраної геш-функції).

Рис. 1. Схематичне зображення реалізації ЕЦП в підписаному повідомлені

Сьогодні найпопулярнішою геш-функцією є SHA-1, яка має розмір гешу 160 біт, вона використовується у таких стандартизованих алгоритмах, як DSA та ECDSA (згідно FIPS PUB 186-3 (версія стандарту, куди включено ЕЦП, який ґрунтується на DSA [10].

Необхідно зазначити, що на практиці основним напрямом вдосконалення ЕЦП є використання відкритого ключа, але вимога щодо вдосконалення параметрів підпису передбачає і вдосконалення законодавчих актів (див. [11, 12]) щодо його технічних можливостей, які покликані використовувати функції гешування. Передусім мається на увазі перехід на SHA-2 або SHA-3 (геш-функції), які можуть створювати геші розміром 224, 256, 384 та 512 біт.

На першій стадії генерується пара ключів (відритий-закритий), шифрується геш, зашифрований геш додається до повідомлення, повідомлення розповсюджується. На другій стадії дії дещо повторюються, але у зворотному напрямі. Коли особа, що хоче впевнитися в автентичності повідомлення, відокремлює повідомлення від його ЕЦП. І, нарешті, відбувається розшифровування повідомлення відкритим ключем. Як було зазначено вище, оскільки доступ до відкритого ключа необмежений, будь-хто може розшифрувати підпис та отримати геш. Далі здійснюється перевірка гешу, гешування повідомлення. Якщо повідомлення автентичне – геші збігаються. Схема ЕЦП зображена на представленому рис. 2. У цьому випадку криптоаналіз виступає дуже важливим складником, бо передбачає знаходження вразливостей або обхід схеми ЕЦП. При цьому криптоаналітик може застосовувати різні можливості. В такому разі найслабшою атакою може бути така, за якої криптоаналітик володіє лише загальновідомою інформацією про алгоритм здійснення ЕЦП.

Прикладом може бути використання методу «грубої сили», коли шляхом перебору обирається дійсна пара підпис-повідомлення. Така атака не є загрозою, адже під час розробки будь-якої якісної системи такий фактор враховується. За рахунок великого розміру ключа криптографічної функції, такий підбір не є можливим за обмежену кількість часу. В такому випадку криптоаналітик може відслідковувати підписані повідомлення та створювати таблицю пар повідомлень і дійсних підписів, а в подальшому використовувати їх. Така атака (перевірка) має назву відомих повідомлень (англ. Known Message Attack). Окремим видом є атаки, пов'язані з підробкою підпису (англ. Signature Forgery), тобто атаки, що передбачають створення підпису для повідомлення, яке не створено уповноваженою особою.

Серед таких підробок слід виділити такі:

1. Екзистенційна підробка – така, що передбачає створення хоча б одного дійсного підпису для повідомлення, не створеного у минулому уповноваженою особою. Зазвичай таке повідомлення є довільного змісту (наприклад, довільний набір символів, довільної довжини) і обирається криптоаналітиком, через що зазвичай не несе у собі загрози.

2. Вибіркова підробка – така, що передбачає створення пари дійсного підпису та такого пові-

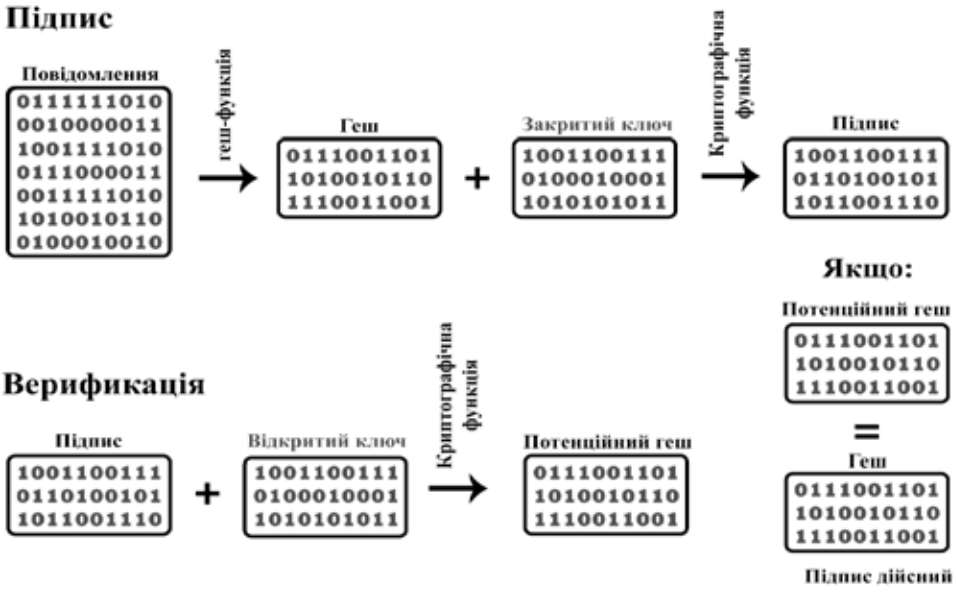

Рис. 2. Схема ЕЦП

домлення, що було обрано криптоаналітиком до здійснення атаки. Вибірковість пов'язана з улаштуванням алгоритму, що надає певним повідомленням такі особливості, що дають змогу криптоаналітику розрахувати пари. Криптоаналітик, знаючи ці особливості, може з певною вірогідністю створити таке повідомлення та розрахувати для нього дійсний підпис. Зазначимо, що універсальна підробка надає криптоаналітику можливість створення повідомлення будь-якого змісту.

Окремо слушно виділити атаку, що передбачає повний злам системи ЕЦП, у тому числі й оволодіння секретом підпису.

Оскільки більшість ЕЦП оперують гешом, існують певні загрози, пов'язані з використанням геш-функції. Найпоширенішою з них вважають атаку, яку пов'язують з такою особливістю гешу, як його стала довжина. Оскільки кількість різних гешів, що можна обчислити, за змістом стає досить великою, тому існує можливість колізії – явища, за якого різні повідомлення матимуть один геш. В такому разі, якщо довжина дорівнює 160 біт, то кількість буде дорівнює 2 160, а якщо 512 біт, то 2 512. Врешті решт існує можливість підробити геш одного повідомлення іншим.

Слід також відзначити, що в разі, коли геш-функція є односторонньою, створення гешу повідомлення залишається простим, а відновлення повідомлення з гешу стає надзвичайно складним для обчислювання. Таке відновлення передбачає використання методу «грубої сили». І хоча для однієї особи згенерувати геш-таблицю пар повідомлення – геш, не є можливим, такі таблиці все ж таки існують у відкритому доступі у мережі Інтернет.

Реалізація ЕЦП набула популярності у наступних алгоритмах: RSA (алгоритм, створений у 1978 році), який став першим стандартизованим алгоритмом ЕЦП. В основі алгоритму лежать математичні операції, пов'язані із задачами факторизації, що являє собою розкладання великих чисел (більше ніж 2 200) на множники – числа, що ділять число націло.

Надалі (1985 р.) була створена схема підпису, яка використовує обчислення дискретного логарифму. І хоча така схема не набула загального використання, згодом була перетворена Агентством національної безпеки США на DSA.

DSA представляє собою алгоритм, стандартизований DSS (англ. Digital Signature Standard) FIPS-186-1, FIPS-186-2, FIPS-186-3, FIPS-186-4. Він використовує асиметричне шифрування, основане на піднесенні до степеня за модулем при дискретному логарифмуванні.

Розглянемо алгоритм DSA на практиці. Для демонстрації була використана мова програмування Python 3.7.3.

Наприклад, припустимо, нам потрібно підписати повідомлення, що має наступний вміст:

Привіт, це повідомлення підписане.

Де «Привіт, це повідомлення підписане».

Для початку генеруємочисла p, q, g, h, a

Алгоритм складається з двох основних частин: з генерації пари відкритого-закритого ключа та здійснення підпису і його підтвердження.

Перша частина складається за наступних кроків:

1) Обирається просте число p, довжина L якого становить від 512 до 1 024 біт: 512 <= L <= 1024, L повинно ділитися націло на 64. Також число (p-1) повинно мати дільник q, котрий 160 біт у довжину: (p-1)mod q = 0

2) Обирається число g, що задовольняє наступним умовам:

– g повинно бути цілим числом
– $1 < g < p$
– $g^{q(\mathrm{mod}\ p)} = 1$
– $g = h^{((p-1)/q)(\mathrm{mod}\ p)}$

3) Обчислюється число h: $h=g^{a(\mathrm{mod}p)}$

4) Обирається число a, яке задовольняє умові $2<a<q-1$

Набір чисел p, q, g, h є відкритим ключем, а набір p, q, g, a – закритим.

p=14231284372943868712274767439176673544286752559169288059811676865558178802536430264831718390836472450265092948017891665647191827088419776157659594240057713199916633247936564 1

q=1090253430700240822105942483552272273919983077513

g=4571682647781247451573724771764474800956133061596781950732878870890019304257686342043362912600989763484308393052159778924770825861992741958631001455973374699117264018588676 1

h=1208040376985201793958262626499512464624718391646939114210669538670731609583925227293900934847203294406855628869992602976316708461420947580202993235393219736730999184726925 69

a=2053256546193605077330067469512861935929179299 14

На другій стадії обирається геш-функція (зазвичай SHA-1). Для створення електронного підпису виконуються наступні кроки:

1) за допомогою геш-функції, повідомлення, що підписується, перетворюється на число-геш H.

H=337852034620107388415398522718939782524511422999

2) Генерується число k, що є більшим 0 та меншим від r (0 <r<q-1)

3) Обчислюється число r за наступною формулою: $C1 = g^{r(modp))(modq).}$ Якщо C1 дорівнює нулю, потрібно брати інше r.

4) Обчислюється C2 за наступною формулою: $C2 = (H + aC1)r^{-1(modq)}$

5) Якщо C2 дорівнює нулю, переобирається число r.

Підписом є пара C1 C2

C1=832043819108692318357721515142593963173462435 27

C2=354423173594352506035878605268929174328149183 58

Для підтвердження повідомлення відбувається процес верифікації, який складається з наступних кроків:

1) Повідомлення знову перетворюється на геш H, використовуючи ідентичний алгоритм гешування, що і під час створення підпису.

2) Обчислюється число $t1 = HC2^{-1(modq)}$

3) Обчислюється число $t2 = C1\ C2^{-1(modq)}$

Підпис визнається як дійсний, якщо виконується рівність $g^{t1}\ h^{t2}(modp)(modq)=C1$

$g^{t1}\ h^{t2}(mod\ p)(mod\ q)=8320438191086923183577215151425939631734624352 7=C1$

Таким чином, саме такий підпис слід вважати дійсним. Обсяги публікації не дозволяють навести коди програми та відповідні суто технічні розрахунки, тим більше, що в цілому сьогодні вони достатньо відомі. Однак проведені розрахунки дозволяють все ж таки суттєво покращити техніко-конфіденційні характеристики ЕЦП. Вимоги часу щодо ЕЦП та вимоги до посилення його конфіденційності дозволили посилити останню і зробити її універсальною, затверджуючи такий підхід на законодавчому рівні [11]. Як відомо, до його вступу в силу діяв Закон України «Про електронний цифровий підпис» зі змінами [12], який втратив чинність на підставі Закону № 2155-VIII від 05.10.2017, ВВР, 2017, № 45, ст. 400 «Про електронні довірчі послуги» [11]. Відзначимо, що Закон [12] не враховував питання конфіденційності та не був спрямований на вирішення пов'язаних з нею задач. З аналізу технічної та юридичної сторони реалізації багатьох питань в галузі інформаційних технологій та їх захисту відомо, що технічна сторона завжди випереджає юридичну. Тому таке співвідношення не є дивним. Однак законодавчий складник має підтягуватися до технічних змін більш швидкими темпами і, як наслідок, прийняття зазначеного Закону слід вважати вельми прогресивною подією. Закон [11] розширив розуміння ряду дефініцій, зокрема, ввівши в нього такі поняття, як відкриті та особисті (авт. – закриті) ключі, кваліфікований підпис, під яким розуміється удосконалений електронний підпис, створений з використанням засобу кваліфікованого електронного підпису і базований на кваліфікованому сертифікаті відкритого ключа, а також розкривши питання надання електронних довірчих послуг, а саме, запроваджуються такі механізми, як електронна ідентифікація, електронний підпис, електронна печатка, реєстрована електронна доставка, тощо. Так, у цьому Законі передбачено взаємне визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів. Однак ще потрібні технічні та організаційні доробки питань, пов'язаних саме з ЕЦП. В зв'язку саме з цим згідно з пунктом 1 (див. розділ VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги») його введення було перенесено на рік, а пункт 5 (VII розділу цього Закону), щодо ЕЦП та відкритого ключа, законодавчо залишається не введеним досі, а чинні сертифікати продовжуватимуть діяти. Однак не можна не відмітити з юридичної сторони, що Закон [11] інтегрує в собі всі попередні здобутки у сфері застосування ЕЦП.

Висновки. Отже, завдяки дослідженню сутності ЕЦП у контексті його конфіденційності, практично доведено, що, відображаючи організацію гарантованого застосування ЕЦП криптографічною системою з відкритим ключем, за якої відкритий ключ передається по відкритому (незахищеному) каналу зв'язку та використовується як для перевірки ЕЦП, так і для шифрування повідомлення, практично реалізується його підвищена конфіденційність та надійність за рахунок відповідного гешування, а також така важлива властивість, що практично його (ЕЦП) стає неможливо підробити. ЕЦП, як кваліфікований електронний підпис, закріплено вже діючим українським законодавством, але ще не повністю реалізовано технічно. Однак за умови технічній спроможності ЕЦП реалізується в режимі підвищеної конфіденційності. При цьому створюється посилений сертифікат розділу ключа, котрий підтверджує його використання саме в режимі підвищеної конфіденційності через наявність кваліфікованого сертифікату електронного підпису, що має йому відповідати. Перспективами подальшої роботи вбачаємо продовження досліджень в галузі вдосконалення елементів, що підвищують конфіденційність вказаного підпису.

Список літератури:

1. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія. Харків : Видавництво «Форт», 2010. 608 с.
2. Computer Security Division I.T.L. Post-Quantum Cryptography | CSRC | CSRC, CSRC | NIST. 2017. URL: https://content.csrc.e1c.nist.gov/Projects/Post-Quantum-Cryptography/faqs
3. Overbeck R., Sendrier N. Code-based cryptography. Post-Quantum Cryptography / Ed. Bernstein D.J., Buchmann J., Dahmen E. Berlin, Heidelberg: Springer, 2009. P. 95–145.
4. Матов О.Я., Василенко В.С., Василенко М.Ю. Несиметричне кодування з використанням лишкових класів. Матеріали Міжнар. наук.-практ. конф. Aplikovan vedecke novinke – 2013. (Прага, 27 липня – 05 серпня 2013 р.). Praha : Publishing House: Edication and Science. s.r.o. 2013. Т. 13. С. 35–40.
5. Василенко В.С. Код условных вычетов: монография. LAMBERT Academic Publishing, Saarbrucken, Deutschland. 2013. 238 с.
6. Kuznetsov A., et al. Code-based electronic digital signature. 2018 IEEE 9-th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2018. P. 331–336.
7. Kuznetsov A., et al. New Approach to the Implementation of Post-Quantum Digital Signature Scheme. 2020 IEEE. 11-th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2020. P. 166–171.
8. Kuznetsov A., et al. Code-Based Schemes for Post-Quantum Digital Signatures. 2019. 10-th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications (IDAACS). 2019. Vol. 2. P. 707–712.
9. Courtois N.T., Finiasz M., Sendrier N. How to Achieve a McEliece-Based Digital Signature Scheme. Advances in Cryptology. ASIACRYPT 2001 / ed. Boyd C. Berlin, Heidelberg: Springer, 2001. P. 157–174.
10. FIPS Digital Signature standard: 2009. National Institute of standard and technology. 2009. https://csrc.nist.gov/csrc/media/publications/fips/186/3/archive/2009-06-25/documents/fips_186-3.pdf
11. Закон України «Про електронні довірчі послуги» № 2155-VIII від 05.10.2017 зі змінами, внесеними згідно із Законом № 440-IX від 14.01.2020. *Відомості Верховної Ради.* 2017. № 45. Ст. 400.
12. Закон України «Про електронний цифровий підпис» № 852-IV від 22.05.2003 зі змінами внесеними в різні роки, останні зміни, внесені згідно з Законом № 1666-VIII від 06.10.2016. *Відомості Верховної Ради України.* 2003. № 36. Ст. 276.

Vasilenko M.D., Zolotoverkh D.S., Novikov V.P., Rachuk V.O. TECHNICAL AND CONFIDENTIAL ASPECTS OF THE PRACTICAL IMPLEMENTATION OF THE ELECTRONIC-DIGITAL SIGNATURE

The meaning of the concept of EDS is revealed and the factors, on which its reliability depends, are determined in the article. It is demonstrated how the EDS carries out the signature with the provision of reliable confidentiality. It is noted that EDS always requires the preservation of confidentiality, the maintenance of which makes it impossible to obtain information by an unauthorized person, representing a set of data obtained as a result of a certain cryptographic transformation of a data set. EDS is created based on the message hash, which allows it to be a constant length of sufficient simplicity of any message. The characteristics of the hash function are presented in the form of a computer algorithm that converts data array of random length into a string of bits of definite length. It is shown in practice how it happens with the use of public and private keys. The threats that may arise from the use of the hash function are identified. The types of encryption that are used by EDS algorithms are determined. Some algorithms are considered in practice; the basic steps of creation of EDS are established. It is determined that the use of public key and improvement of current legislation are the main means for improving EDS. The types of counterfeits and ways of their reproduction are described. The mechanism of preservation and strengthening of confidentiality at transfer of such signature, as well as its legislative regulation in the context of the changes connected with development of information technologies is reflected. Herewith, the development of the latter always precedes the development of improved legislation. The adoption of the Law of Ukraine "On Electronic Trust Services" was noted as a significant positive step, but it was mentioned that technical and organizational improvements in EDS-related issues are currently needed. The disclosure of the essence of EDS practically proves that reflecting the organization of guaranteed use of EDS by a cryptographic system with a public key, in which the public key is transmitted over the public (unprotected) and is used for both EDS verification and message encryption, its increased confidentiality and reliability should be stated. Also, it is almost impossible to fake it.

Key words: *signature, electronic-digital, confidentiality, key, hash function, encryption.*