УДК 681.3:002.651.028

О.А. Борисенко[1], В.Б.Чередниченко[2]

[1] *Сумський державний університет, Суми*
[2] *Сумська філія Харківського національного університету внутрішніх справ, Суми*

# ДО РІШЕННЯ ЗАДАЧ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

*Розглянуто позитивні зрушення останніх років у вирішенні задач електронного цифрового підпису. Описано ряд проблем, які не дозволяють забезпечити внутрішньої та зовнішньої крос-сертифікації ключів ЕЦП. Розглянуто напрямки їх подолання для досягнення відповідності нормам Європейського Союзу. Подальше удосконалення та розвиток Національної системи ЕЦП потребує комплексного, взаємоузгодженого вирішення широкого кола питань.*

***Ключові слова:*** *електронний цифровий підпис, крос-сертифікація, криптографічний захист інформації.*

## Вступ

У теперішній час розвиток держав обумовлюється ступенем впровадження інформаційних технологій в усі сфери економіки, виробництва та суспільного життя. Розвинуті держави світу у XXI столітті поставили за мету прискорено рухатись до нового інформаційного суспільства. Це дасть їм змогу здійснити перехід до економіки, заснованої на знаннях та електронних сервісах, залучити усіх громадян до найсучасніших технічних досягнень.

Процедури використання інформаційно-комунікаційних технологій базуються на забезпеченні інформаційної безпеки, як найважливішої умови передачі документів по каналах зв'язку. Відомо, що найбільш надійним та зручним засобом захисту даних при мережевому обміні є електронний цифровий підпис (ЕЦП). Він ретельно внормований документами ООН, стандартами Євросоюзу та законодавством багатьох країн [1]. У світі накопичено великий досвід розробки засобів ЕЦП та досягнуто позитивні результати в усіх сферах його впровадження.

**Метою** даної роботи є огляд проблем застосування цифрового підпису в Україні та напрямків їх подолання з метою гармонізації законодавчої та нормативно-правової бази з вимогами Європейського союзу, що сприятиме розвитку національної інфраструктури ЕЦП.

## Виклад матеріалу

У 2002- 2004 р.р. в Україні було прийнято низку законодавчих актів та нормативно-технічних документів про ЕЦП [2].

З того часу ця галузь пройшла етап становлення та зараз перебуває у стані активного розвитку.

Як подальший дороговказ, можна виділити прийняту Кабінетом міністрів України «Стратегію розвитку інформаційного суспільства в Україні» від 15 травня 2013 р. № 386-р. В ній окреслено основні напрямки інновацій: електронне урядування, електронна демократія, електронна економіка, електронна комерція, електронна послуга, електронна освіта, електронна медицина, електронна культура [3].

Станом на 1.01.2015 р. в Україні функціонує 18 акредитованих та 7 зареєстрованих центрів сертифікації ключів (ЦСК). Серед них можна виділити державні підприємства:

«Українські спеціальні системи»,

«Центр автентифікації національної системи конфіденційного зв'язку»,

а також потужні відомчі підприємства:

Центр сертифікації ключів Державної фіскальної служби (ДФС) України,

Акредитований засвідчувальний центр Національного банку України,

Єдиний державний портал адміністративних послуг та його регіональні центри,

Головний інформаційно-обчислювальний центр Державної адміністрації залізничного транспорту України.

За даними Центрального засвідчувального органу (ЦЗО) Міністерства юстиції України акредитованими центрами сертифікації протягом 2014 р. сформовано 3,3 млн. сертифікатів відкритих ключів, та надано 38, 7 млн. послуг фіксування часу, що набагато більше за попередній рік [4].

Як позитивний приклад, можна навести впровадження Державною фіскальною службою (ДФС) України сервісу "Електронний кабінет платника податків". Він забезпечує з 1.01.2014 р. надання підприємцям можливості створити пер-

сональний Електронний кабінет платника податків (веб-портал ДФС http://kpp.minrd.gov.ua/). У ньому за допомогою спеціального інструменту доступу (наприклад, електронної картки платника податків) на безоплатній основі та з використанням електронного цифрового підпису в режимі он-лайн фізична або юридична особа може:

заповнити чернетки податкової звітності,

надіслати остаточний варіант в електронному вигляді;

переглядати дані картки особового рахунка про стан розрахунків з бюджетом;

формувати та заповнювати платіжні документи щодо сплати податків, зборів та інших платежів до бюджету;

здійснювати такі сплати за допомогою банківських систем типу Інтернет-банкінг, тощо.

Щомісяця цим сервісом користуються сотні тисяч підприємців.

Починаючи з 01 січня 2015 року, відповідно до Податкового кодексу України податкові накладні складаються виключно в електронній формі та підлягають обов'язковій реєстрації в Єдиному реєстрі податкових накладних.

Слід зауважити, що несанкціонований доступ до такої інформації або її спотворення може нанести величезну шкоду суб'єкту господарювання. Тому Акредитований центр сертифікації ключів ДФС з 1.01.2014 р. перейшов на використання двох посилених сертифікатів ключів ЕЦП (згідно наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 р. №739 «Про затвердження Вимог до форматів криптографічних повідомлень»). Один ключ ЕЦП накладає керівник підприємства, другий ключ – головний бухгалтер, а при наявності печатки підприємства її електронний аналог також накладається на податковий документ третім співробітником. Така система використання ЕЦП багаторазово підсилює захист електронних документів.

Можна констатувати, що з метою вдосконалення функціонування ЕЦП в Україні в останні роки було прийнято ряд нормативних актів. Так, у 2012 році Міністерство юстиції України і Державна служба спеціального зв'язку та захисту інформації України врегулювали вимоги до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису [5].

Наказом Міністерства юстиції України від 29.01.2013 № 183/5 був затверджений новий Регламент роботи Центрального засвідчу вального органу.

Певний прогрес України у сфері ІКТ вплинув на її оцінки у світі. Так у рейтингу, що відображає загальну здатність країн до інновацій "The Global Innovation Index" (агентство Bloomberg) Україна посіла у 2015 р. 33 місце (у 2014 – 49, у 2013 – 42 місце).

Але по індексу ІКТ ми маємо 77 місце, а по мережевій готовності – тільки 81 місце з 140 держав [6].

Національна Система ЕЦП поки відстає від світового рівня розвитку (за деякими оцінками на 8 – 10 років [7].

Так, європейська бізнес-модель ЕЦП реалізує три види кваліфікованих підписів, вона є кваліфікованою інфраструктурою відкритих ключів (Qualified public key infrastructure, QPKI). Недолік прийнятої в Україні інфраструктури PKI - реалізація тільки одного, найпростішого різновиду підпису [8].

Ще одним недоліком НС ЕЦП є невизначеність механізмів внутрішньої крос-сертифікації ЦСК для забезпечення довіри між користувачами різних систем. В Україні згідно ДСТУ 4145 + ГОСТ 34.311 реалізований найпростіший неінтероперабельний варіант ЕЦП з єдиним комплектом підписів, що не допускає контрпідписи. У результаті клієнти зобов'язані використовувати ключі розрізнених систем ЕЦП, які є відомчими, що стримує розвиток процесів електронної взаємодії [7].

Також НС ЕЦП позбавлена зовнішньої інтероперабельності зважаючи на негармонізований з нормативами Євросоюзу алгоритм підписання, який не забезпечує взаємодію з міжнародно визнаними криптографічними алгоритмами.

НС ЕЦП також не готова до транскордонного визнання сертифікатів ключів, виданих за межами України, тобто нездатна до зовнішньої крос-сертифікації з будь-якою державою [9].

Слід вказати на проблеми процесу акредитації центрів сертифікації ключів (ЦСК). Перевірці експертною комісією ЦЗО підлягає програмно-технічний комплекс (ПТК) і його компоненти та компетентність персоналу ЦСК, але не оцінюються функціональність і працездатність ПТК. Відповідність конкретних продуктів встановлюють незалежні і компетентні оцінювачі. Але в Україні порушено принцип незалежності таких оцінювачів, оскільки де-факто технічний нагляд проводить контролюючий орган, причому через нормативно неврегульований механізм «позитивних експертних висновків».

У Євросоюзі процедура оцінки відповідності максимально формалізована згідно системі стандартів ISO 9000 і виконується он-лайн по Інтернету.

Для довіри іноземних партнерів Центральному засвідчу вальному органу України необхідно

розробити і впровадити он- лайн методику акредитації ЦСК, та підтримати таку процедуру спеціальним тестовим стендом [10].

Також експерти виділяють ряд загроз, що виникають при багаторічному зберіганні електронних документів (у т.ч. й архівному). До таких загроз можна віднести:

зміну технологій і стандартів ЕЦП;

відсутність гарантій доступності сертифіката ключа в довгостроковій перспективі;

зміну програмно-апаратних платформ кожні 2-3 роки; компрометацію секретного ключа або технологій ЕЦП.

Наслідок – відсутність гарантії того, що через декілька років можна довести юридичну правомочність електронного документа в результаті неможливості використання старих засобів перевірки ЕЦП [9].

У сучасному світі кількість мобільних пристроїв (смартфони, планшетні ПК, тощо) бурхливо зростає. Тому вже на часі необхідність вирішення питань, пов'язаних з процедурами використання таких пристроїв користувачами ЕЦП. Виникла необхідність стандартизації для таких сценаріїв [11]:

а) Локальне підписання, при якому підпис створюється з використанням ключа, який зберігається на мобільному пристрої користувача.

б) Дистанційне підписання, при якому підпис створюється з використанням ключа, який зберігається на віддаленому сервері.

в) Процедури перевірки ЕЦП з використанням мобільного пристрою.

Слід констатувати наявність позитивних зрушень у вирішенні деяких вищезгаданих проблем.

Так, створено Науково-експертну раду з питань розвитку інфраструктури відкритих ключів при Міністерстві юстиції України (наказ 13.06.2014 № 932/5).

Інститутом кібернетики ім. В.М. Глушкова розроблено та закінчено у 2014 р. створення Стенду для тестування функціональної сумісності засобів ЕЦП. На ньому спеціалістами ЦЗО Мінюсту була досліджена можливість сумісності тестових ключів та програмного забезпечення 15 АЦСК (9 розробників засобів ЕЦП, файли 7 типів).

Станом на 1.01.2015 р. за допомогою Стенду встановлена сумісність процедур та продуктів ЕЦП серед 7 вітчизняних ЦСК та несумісність у 8 центрів [12].

Держспецзв'язком у 2014 р. прийнято два нових стандарти криптографічного захисту інформації як національних.

Один з них – ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція хешування», вводиться в дію 01 квітня 2015 року.

Другий – ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення».

Введення в дію нових національних стандартів забезпечить захист систем, засобів і протоколів криптографічного захисту інформації, що розробляються в Україні, у тому числі у сфері електронного цифрового підпису. Це відповідає сучасним і перспективним вимогам Європейського Союзу, а передбачені криптографічні алгоритми підтримують довжину ключа від 128 до 512 бітів, що є унікальним у світі [13].

## Висновок

Зважаючи на вищевикладене можна стверджувати, що основними задачами впровадження в Україні надійних механізмів довіри в НС ЕЦП слід назвати відсутність гармонізації національного електронного цифрового підпису до QPKI та до алгоритмів за міжнародними стандартами у сфері електронних підписів Європейського інституту по стандартизації в галузі телекомунікацій (ETSI) Євросоюзу.

Дослідженнями провідних науковців встановлено, що для подолання цих недоліків та гармонізації використання електронного цифрового підпису з міжнародними стандартами головними напрямками руху є запровадження кросс-сертифікаційних механізмів у політику підпису, реалізація прозорої он-лайн процедури акредитації через впровадження сучасних тестових стендів для контролю сумісності програмно-технічних комплексів різних ЕЦП та їх базових показників безпеки.

Також необхідно розвивати систему незалежних оцінювачів, прийняти нову редакцію Закону України про ЕЦП та пов'язані з ним нормативно-технічні регламенти, укладати угоди з державами Євросоюзу про взаємне визнання сертифікатів відповідності ЕЦП.

Подальше удосконалення та розвиток Національної системи ЕЦП є багатокомпонентним завданням та потребуватиме комплексного, взаємоузгодженого вирішення широкого кола питань на законодавчому, нормативно-регламентному, загальносистемному, програмно-апаратному та функціонально-технічному рівнях.

## Список літератури

*1. Чередниченко В.Б. Електронний цифровий підпис – міжнародні правові аспекти [Текст] / В.Б. Чередниченко // Електроніка та системи управління. – К.: Київський національний авіаційний університет. - 2008. - №3(17). – С. 84-87.*

*2. Чередниченко В. Електронний цифровий підпис у правовому полі України [Текст] / В.Б. Чередниченко // Системи обробки інформації. – Х.: Харківський університет Повітряних Сил ім. І.Кожедуба, 2009. – Вип.7(79). – С. 123-124. – ISBN 1681-7710.*

*3. Стратегія розвитку інформаційного суспільства в Україні. Розпорядж. Кабміну України від 15.05.2013 р. №386р // Офіційний вісник України від 21.06.2013, № 44. – С. 79.*

*4. Кількість сформованих сертифікатів відкритих ключів та послуг фіксування часу в Україні за 2014 рік. [Електронний ресурс]. – Режим доступу до ресурсу: http://czo.gov.ua/news.*

*5. Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису. Мін'юст України, Держспецзв'язку України. Наказ від 27.12.2013 № 2782/5/689 // Офіційний вісник України від 24.01.2014 р., № 6. – С. 161.*

*6. Украина поднялась на 16 позиций в рейтинге инновационных стран. [Електронний ресурс]. – Режим доступу до ресурсу: http://biz.liga.net/all/it/novosti/2935544.*

*7. Клімушин П.С. Механізми забезпечення довіри в національній системі електронних цифрових підписів [Текст] / П.С. Клімушин // Теорія та практика державного управління: зб. наук. пр. – Х.: Вид-во ХарРІ НАДУ "Магістр", 2013. – Вип. 2 (41). – С. 51-58.*

*8. Кузнецов О.О. Захист інформації в інформаційних системах [Текст]: навч. посіб. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид-во ХНЕУ, 2011. – 512 с. – Бібліогр.: с. 498-505 (96 назв). – ISBN 978-966-676-442-6.*

*9. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика [Текст]: монографія / Ю.І. Горбенко, І.Д. Горбенко // Харк. нац. ун-т радіоелектрон., ЗАТ Інт інформ. технологій. – Х.: Форт, 2010. – 593 с.*

*10. Мелащенко А.О. Национальная система электронных цифровых подписей как открытая система [Текст] / А.О. Мелащенко, О.Л. Перевозчикова // Кибернетика и системный анализ. – Изд. Ин-т кибернетики НАНУ. – 2011. – № 5. – С. 180-188.*

*11. Горбенко Ю.І. Сценарії створення та перевірки вдосконалених електронних підписів в мобільному середовищі / Ю.І. Горбенко, К.В. Ісірова // Теоретичні та прикладні аспекти побудови програмних систем TAAPSD'2014: матеріали XI Міжнародної наукової конференції, Київ, 15-17 грудня 2014 р. - К. «Авангард», 2014. – С. 75-79.*

*12. Попередній аналіз внутрішньої сумісності суб'єктів електронного цифрового підпису. [Електронний ресурс]. – Режим доступу до ресурсу: http://czo.gov.ua/status-ecp.*

*13. Держспецзв'язку впроваджує нові стандарти криптографічного захисту інформації. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dstszi/ control/uk/publish.*

*Надійшла до редколегії 9.02.2015*

**Рецензент:** д-р фіз-мат наук, проф. О.С. Опанасюк, Сумський державний університет, Суми.

## К РЕШЕНИЮ ЗАДАЧ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

А.А. Борисенко, В.Б. Чередниченко

*Рассмотрены положительные сдвиги последних лет в решении задач электронной цифровой подписи. Описан ряд проблем, которые не позволяют обеспечить внутренней и внешней кросс-сертификации ключей ЭЦП. Рассмотрены направления их преодоления для достижения соответствия нормам Европейского Союза. Дальнейшее совершенствование и развитие Национальной системы ЭЦП требует комплексного, взаимно согласованного решения широкого круга вопросов.*

***Ключевые слова**: электронная цифровая подпись, кросс-сертификация, криптографическая защита информации.*

## TO SOLVING THE PROBLEM OF ELECTRONIC SIGNATURES

O.A. Borisenko, V.B. Cherednichenko

*Positive developments in recent years in solving problems of digital signature. The article describe a number of problems that do not allow internal and external cross-certification of electronic keys. Directions to overcome them to comply with EU standards. Further improvement and development of the National System of electronic signature requires a comprehensive, mutually solve a wide range of issues.*

***Keywords:** digital signature, cross-certification, cryptographic protection.*