Створення Довірчого центру

Міністерства юстиції України – вікно держави у світовий простір електронного цифрового підпису

О. В. Костенко
заступник начальника Управління функціонування центрального засвідчувального органу

У статті досліджується проблема Національної системи електронного цифрового підпису України, досягнення її інтероперабельності шляхом створення Довірчого центру Міністерства юстиції України.
Ключові слова: *електронний цифровий підпис, інтероперабельність, Довірчий центр, стандарти.*

В статье исследованы проблемы Национальной системы электронной цифровой подписи Украины, достижения ее интероперабельности путем создания Доверительного центра Министерства юстиции Украины.
Ключевые слова: *электронная цифровая подпись, интероперабельность, Доверительный центр, стандарты.*

In the article the problem of the National system of electronic digital signature of Ukraine to achieve its interoperability by creating a Trustee of the center of the Ministry of Justice of Ukraine.
Keywords: *digital signature, interoperability, the Trustee center, standards.*

Розвиток суспільних відносин від стародавніх часів і дотепер характеризувався потребою в гарантуванні певних правил, що забезпечували функціонування механізмів діяльності держави та громадян – довірчих відносин. Тривалий період характеристикою довірчих відносин було «слово честі», яке підкріплювалося рівнем особистої репутації, умовно прийнятої в певних публічних колах. Згодом розвиток паперового діловодства створив більш надійну інфраструктуру довіри, що охарактеризувалася виникненням класу спеціальних довірчих послуг – вчинення нотаріальних дій з використанням підписів, печаток та документів, які визначають юридичну силу документа.

Сучасна інформатизація різних сфер життя та цифрові технології сприяють прискоренню розвитку світової економіки, що зумовлює соціальну трансформацію суспільства. Розвиток інформаційного суспільства є одним з важливих пріоритетів України і розглядається як загальнонаціональне завдання. Інформаційно-телекомунікаційним технологіям відведена роль необхідного інструменту соціально-економічного прогресу, одного з ключових чинників інноваційного процвітання економіки.

Прийняття у 2003 році Закону України «Про електронний цифровий підпис» [1], відповідних постанов Кабінету Міністрів України та декількох актів уповноважених державних органів які були спрямовані на забезпечення регулювання з боку держави впровадження в Україні технології електронного цифрового підпису в першу чергу в державному секторі. Створена на основі цього Закону Національна система електронного цифрового підпису (далі – НСЕЦП) від імені держави гарантує якість та надійність послуг електронного цифрового підпису (далі – ЕЦП).

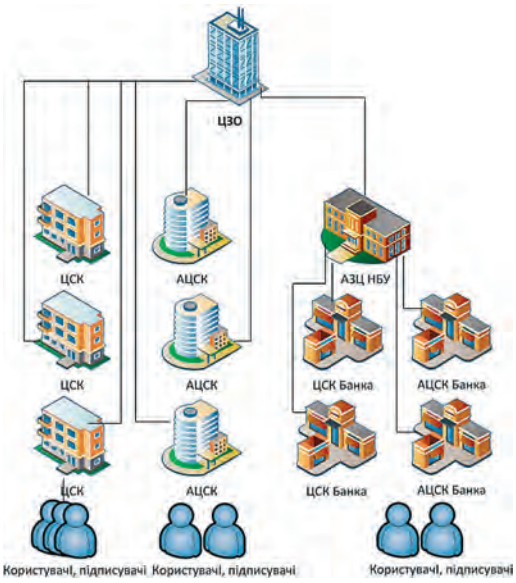
НСЕЦП в Україні розвивалась під керівництвом Державної служби спеціального зв'язку та захисту інформації України і Державного агентства з питань науки інновацій та інформатизації України. Паралельно розбудовується ініційована Національним банком України система ЕЦП у банківській сфері.

Тривалий час регулювання у сфері ЕЦП здійснювалось в «ручному режимі», а просування нових форматів і технологій було ситуативним, часто шляхом спроб та помилок, що спричинило технологічну несумісність програмно-технічних комплексів, які використовуються акредитованими центрами сертифікації ключів, замовниками, розробниками, виробниками та організаціями, що призводить до нерівнозначності різних електронних цифрових підписів у системі та внеможливлює інтеграцію до європейської системи електронного цифрового підпису.

Сьогодні відповідно до Переліку центральних органів виконавчої влади, на які покладаються функції технічного регулювання у визначених сферах діяльності, затвердженого постановою Кабінету Міністрів України від 13 березня 2002 р. № 288, на Міністерство юстиції України покладено функцію технічного регулювання у сфері електронного цифрового підпису.

Відповідно до Положення про Міністерство юстиції України, затвердженого Указом Президента України від 6 квітня 2011 № 395, Мін'юст виконує функції центрального засвідчувального органу (далі – ЦЗО) [2, 3], регулює сферу електронного цифрового підпису шляхом акредитації та державного нагляду за діяльністю центрів сертифікації, а також формує основні напрямки та засади політики НСЕЦП України.

Діюча в Україні НСЕЦП за схемою сертифікації та ієрархією належить до кореневих (мал. 1). Кореневий центр сертифікації ЦЗО видає сертифікати підлеглим центрам сертифікації (відповідно – засвідчувальним органам або акредитованим/зареєстрованим центрам сертифікації ЦСК/АЦСК/АЗЦ НБУ) і йому безпосередньо довіряють кінцеві користувачі підлеглих цен-



Мал 1. Національна система електронного цифрового підпису України. Схема.

трів сертифікації. Використовуючи загальний сертифікат кореневого – центрального засвідчувального органу, можна перевірити всі сертифікати користувачів зареєстрованих та АЦСК, а також АЗЦ НБУ.

Для інтеграції та вигідної співпраці України з європейським та світовим співтовариством, з метою євроінтеграції та розвитку експорту всіх вітчизняних галузей виробництва необхідно запровадити в нашій державі відповідні норми ООН, СОТ та ЄС, забезпечивши їх технологічну підтримку в частині цілісності та неспростовності обміну електронними документами, засвідченими електронним цифровим підписом.

Згідно зі статтею 17 Закону України «Про електронний цифровий підпис» іноземні сертифікати ключів, засвідчені відповідно до законодавства тих держав, де вони видані, визнаються в Україні чинними у порядку, встановленому законом [1].

Однак сьогодні в нашій державі правовий механізм регулювання визнання іноземних сертифікатів ключів відсутній.

У зв'язку з цим однією з ключових проблем, які постали сьогодні перед державою у сфері надання послуг електронного цифрового підпису, є відсутність інтероперабельності Національної системи електронного цифрового підпису як у межах України, так і з іншими державами.

Досвід країн Європейського Союзу (далі – ЄС) щодо розбудови національних інфраструктур електронного цифрового підпису базується на положеннях Директиви 1999/93/ЄС [4] та стандартах розроблених на її основі. Національні системи об'єднані в систему континентального масштабу і мають технічну спорідненість та алгоритмічну сумісність застосованих програмно-технічних рішень в сфері ЕЦП.

Зокрема прийнята у ЄС комітетом JTC1 система ISO/IEC відкрита за визначенням і має властивості інтероперабельності, масштабності, мобільності, унормованості. Інфраструктура інформаційного суспільства має забезпечити дві складові подання даних та засоби довіри до цих даних.

Альтернативними до кореневого рішеннями є Довірчий центр сертифікації ключів «Bridge CA» або шлюзовий центр сертифікації ключів «Gateway CA», а також формування списків довіри (у ЄС та США використовують змішане рішення Bridge – Gateway CA із одночасним формуванням списків довіри).

З розвитком програми електронного уряду в країнах ЄС органи державного управління все ширше використовують електронні сертифікати для безпеки комунікацій, шифрування та електронного підпису, в тому числі в міждержавних відносинах в межах ЄС. Виникла необхідність встановлення відносин довіри між ЦСК (англ. CA), які використовуються національними органами державного управління. Це необхідно для того, щоб державні службовці держав ЄС могли використовувати електронні сертифікати, випущені їх національними ЦСК, в загальноєвропейській (pan-European) державній мережі.

У зв'язку з цим основною метою є встановлення системи взаємної довіри між ЦСК європейських державних (недержавних) органів. Це дасть змогу підприємствам і громадянам, які володіють електронними сертифікатами, випущеними національними ЦСК (державними та недержавними), взаємодіяти в межах ЄС як між собою, так і з державними органами та в електронній комерції ЄС.

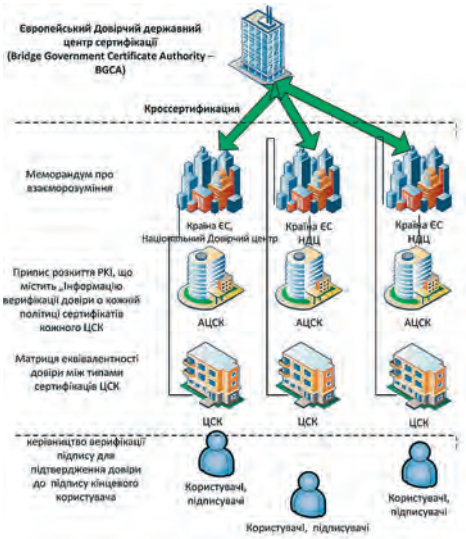
Аналогічні задачі виникають і при розбудові національної системи ЦСК в Україні, яка має поєднувати в собі функції обслуговування громадян та організацій України і забезпечувати можливість їх взаємодії з громадянами й організаціями ЄС. У ці завдання входить також і забезпечення взаємодії державних органів України з офіційними органами та недержавними організаціями держав ЄС. Тому дуже важливо вивчити досвід інших держав та запроваджувати в Україні найбільш перспективні моделі побудови національної інфраструктури електронного підпису.

Традиційна модель інфраструктури з відкритими ключами (PKI – Public Key Infrastructure) дає змогу вирішити питання щодо встановлення відносин довіри між ЦСК через механізм «крос-сертифікації» («cross-certification»).

Як вищезазначено, такий механізм – це «Bridge CA» або «Gateway CA» (Шлюзовий ЦСК) використовується в США, Канаді, ЄС тощо для побудови Національних PKI. В ЄС ініціатива «European Bridge-CA» була ініційована Дойче банком (Deutsche Bank) та Дойче Телекомом (Deutsche Telekom).

Зокрема в ЄС використовується Державний шлюзовий ЦСК, «Bridge CA» (BGCA – Bridge Government Certificate Authority, див. мал. 2), призначений забезпечити такий ступінь довіри, який необхідний для використання електронних сертифікатів як на національному, так і на європейському рівнях.

Відповідна робоча програма ЄС щодо створення «Bridge CA» (BCA) на рівні ЄС була розпочата в 2001 р. Базою для програми «Bridge CA» був проект PKI для замкнутих груп (PKICUG – Public Key Infrastructure for Closed User Groups) користувачів ЄС, який був розпочатий в січні 1999 р., як частина програми Обміну даними між урядами (IDA – Interchange of Data between administrations), що призначена для розвитку та виконання між урядами країн ЄС електронного обміну даними через транс'європейські мережі.



Мал 2. Державний шлюзовий ЦСК, «Bridge CA» (BGCA). Схема.

Шлюзова модель BCA PKI (Bridge CA PKI) складається з поєднання т. зв. Web/Internet довірчої моделі (Web/Internet Trust Model) та Шлюзової моделі (Bridge/Gateway Model). У термінах UML (Unified Modelling Language), яка є визнаним засобом при розробці програмних проектів, компонентами цієї моделі є:

– Шлюзовий ЦСК (Bridge/Gateway CA);

– окрема інфраструктура PKI сектору CUG.

У цій моделі Шлюзовий ЦСК виконує дві ролі:

– крос-сертифікація з іншими ЦСК замкнутих груп CUG;

– випуск Списків довіри (Trust Lists) для різних груп та/або різних секторів.

Будь-яка окрема інфраструктура PKI в межах об'єднання в шлюзову модель BCA PKI має змогу завантажити Список довіри, випущений Шлюзовим ЦСК або завантажити крос-сертифікати для того, щоб дозволити відносини довіри з іншою PKI інфраструктурою, яка є членом BCA PKI.

Досить цікавий механізм трансграничної взаємодії в межах Митного союзу реалізовано Республікою Білорусь та Російською Федерацією. Для вирішення проблеми скорочення митного обслуговування вантажів, що циркулюють в межах Митного союзу було прийнято рішення про впровадження міждержавного Довірчого центру, призначеного для ведення електронного документообігу та електронного цифрового підпису, в тому числі і для забезпечення процедури «декларування митної вартості».

Першим етапом виконання цього проекту було гармонізовано національне законодавство, зокрема Закон Російської Федерації «Про електронний цифровий підпис» № 1-ФЗ від 10.01.2002 р. (в редакції Федерального закону від 08.11.2007 р. № 258-ФЗ), Закон Російської Федерації «Про електронний цифровий підпис» № 63-ФЗ, Закон Республіки Білорусь від 28.12.2009 р. № 113-З «Про електронний документ та електронний цифровий підпис».

Наступним кроком стало приведення нормативної бази ряду стандартів СТБ [5-11] та Російської Федерації [12-15].

Також 15 грудня 2011 року затверджено спільні міждержавні документи «Профіль захисту архіву електронних документів», «Інформаційні технології. Архів електронних документів. Формат електронних документів».

Сьогодні програмно-технічний комплекс Довірчого центру, розроблений російськими компаніями з використанням білоруської криптографії, впроваджено і використовується не тільки для оформлення електронних документів під час перевезення вантажів залізничним транспортом між Росією та Республікою Білорусь, а й при закупівлях, які проводяться в електронній формі на електронних торговельних площинах цих країн.

Головною проблемою, яка постала перед Україною у сфері надання послуг електронного цифрового підпису, є відсутність сучасної інтероперабельної Національної системи електронного цифрового підпису (мал. 3), що характеризується [15]:

– недостатністю актуальних національних стандартів та технічних регламентів;

– невизнанням національних стандартів, що забезпечують технічне регулювання інфраструктури відкритих ключів та надання послуг електронного цифрового підпису на міжнародному рівні;

– відсутністю органу та технічного інструментарію з оцінки відповідності державним стандартам та технічним регламентам функціонування інфраструктури відкритих ключів та послуг електронного цифрового підпису;

– відсутністю організаційно-технічної структури, яка забезпечить на міжнародному рівні регулювання інфраструктури відкритих ключів та надання послуг електронного цифрового підпису.

Вирішити зазначені проблеми можливо шляхом сприяння розвитку інфраструктури відкритих ключів, забезпечення технічного регулювання інфраструктури відкритих ключів та надання кваліфікованих електронних довірчих послуг з використанням як міжнародних стандартів з національними особливостями, так і вітчизняних національних стандартів.

Одним з ключових елементів сучасної інтероперабельної Національної системи електронного цифрового підпису може стати створення на базі Міністерства юстиції України Довірчого центру, що сприятиме досягненню сумісності технічних рішень у сфері використання електронного цифрового підпису шляхом технологічної уніфікації компонентів Національної системи елек-

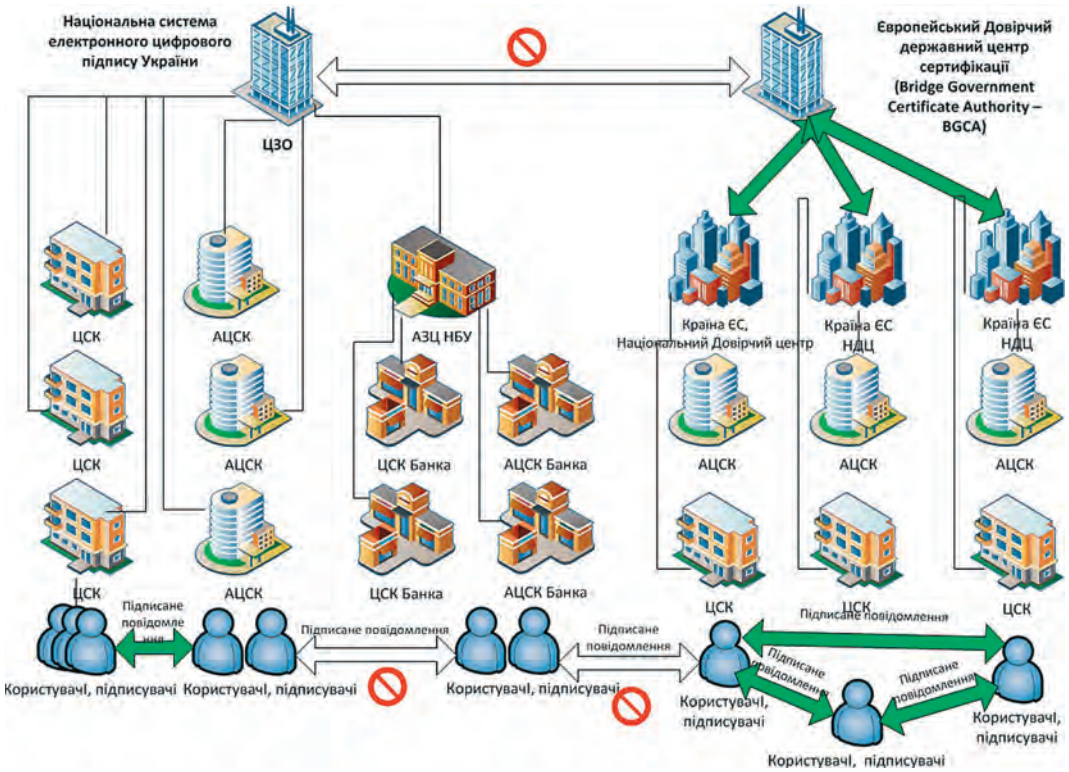


Рис 3. НСЕЦП України сьогодні. Схема.

тронного цифрового підпису з використанням як міжнародних стандартів з національними особливостями, так і вітчизняних національних стандартів, а також взаємного визнання сертифікатів за двосторонніми та багатосторонніми угодами.

Довірчий центр Міністерства юстиції України повинен забезпечити:

– випуск перехресних крос-сертифікатів, обмін і оновлення належним чином сертифікатів з «Головним ЦСК» кожного члена PKI;

– регулярне розсилання сертифікатів «Списків довіри» членам PKI;

– ведення служби каталогу (репозиторію) випущених головних сертифікатів кожному члену PKI, а також відповідні Списки анулювання сертифікатів, які потрібно регулярно оновлювати;

– підтримання веб-вузла, що публікує меморандуми та інші документи щодо політики;

– on-line квитування статусу сертифіката через OCSP (Online Certificate Status Protocol);

– технічні інтерфейси взаємодії з Довірчим центром Міністерства юстиції України;

– базові основи тестування інтерфейсу з вузлом BGCA, призначені для нових претендентів на підключення.

Таким чином, Довірчий центр Міністерства юстиції України не тільки об'єднає суб'єктів Національної системи електронного цифрового підпису, а й вирішить головне інтероперабельне питання – адаптацію НСЕЦП України в європейську та світову системи електронного документообігу та електронного цифрового підпису [16] (мал. 4.)

Крім того, для створення Довірчого центру Міністерства юстиції України потрібно врахувати вимоги ЄС щодо відкритості стандартів.

Мінімальними вимогами ЄС щодо стандартів і специфікацій для Довірчого центру є:

– послуги (сертифікації та списки відкликаних сертифікатів) Довірчого центру повинні відповідати Інтернет-стандартам, необхідним для підтримки інфраструктури відкритого ключа та відповідним специфікаціям;

– служби каталогу (мережі/домену) Довірчого центру повинні бути як мінімум X.500 сумісні (каталоги відповідно стандарту X.500 надають централізовану інформацію про всі іменні/названі об'єкти мережі для швидкого пошуку в мережі) та підтримувати LDAP запити (запити не як веб- клієнт, а через службу каталогів до окремого сервера придатків – LDAP);

– дотримання стандартів ETSI (European Telecommunications Standards Institute) щодо центрів сертифікації ключів, які випускають «прості» (не регульовані державою) сертифікати відкритих ключів та посилені сертифікати.

Процеси визнання Довірчого центру Міністерства юстиції України сертифікатів відкритих ключів ЕЦП, виданих у різних країнах на міждержавному рівні, в рамках СОТ і у процесах взаємодії з ЄС потребують перевірки на відповідність будь-яких створюваних або використовуваних під час розробки і супроводження програмного забезпечення потреб та інтересів користувачів та замовників цього програмного забезпечення. Крім того, у випадку визнання сертифікатів відкритих ключів ЕЦП, виданих у різних країнах, з ЄС необхідно забезпечити повномасштабну перевірку і автоматичне Інтернет-тестування всієї НСЕЦП з одночасним аналізом її законодавчої бази.

Майбутнє розширення сфери використання ЕЦП в Україні та відповідне зростання кількості користувачів поставить також завдання кластерізації (спеціальні програмно-апаратні рішення для балансування навантаження доступу користувачів, підвищення доступності та зменшення часу відгуку), надійності, резервування до обладнання центрального засвідчувального органу. Ці завдання одночасно зі створенням спеціального депозитарію списків довіри, а також веденням бази сертифікатів та списків відкликаних сертифікатів пропонується вирішувати в межах функціонування Довірчого центру Міністерства юстиції України.

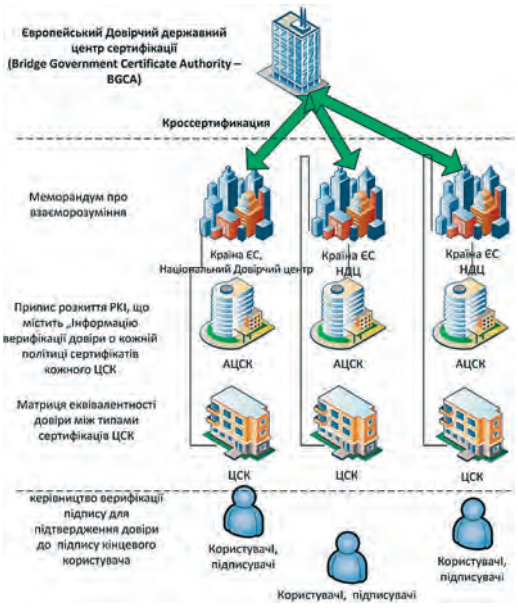


Рис 4. Інтероперабельна НСЕЦП України. Довірчий центр. Схема.

Таким чином, впровадження Довірчого центру Міністерства юстиції України безпосередньо сприятиме інтероперабельності Національної системи електронного цифрового підпису України, технологічній уніфікації компонентів Національної системи електронного цифрового підпису з використанням як міжнародних стандартів з національними особливостями, так і вітчизняних національних стандартів, її гармонізації до міжнародних нормативно-правових актів, що нормалізують правовідносини у інформаційному суспільстві та вчасному реагуванню на потреби населення та бізнесу до сервісів електронного врядування, електронного документообігу та інших Інтернет-послуг з використанням електронного цифрового підпису.

Список використаної літератури

1. Про електронний цифровий підпис : Закон України від 22 травня 2003 р. №852-IV// Відомості Верховної Ради України. – 2003. – № 36. – С. 278.
2. Про затвердження Переліку центральних органів виконавчої влади, на які покладаються функції технічного регулювання у визначених сферах діяльності та розроблення технічних регламентів : постанова Кабінету Міністрів України від 13 березня 2002 р. № 288 // Офіційний вісник України. – 2002. – № 28. – С. 23.
3. Про затвердження Положення про центральний засвідчувальний орган : постанова Кабінету Міністрів України від 29 листопада 2004 р. № 1451 // Офіційний вісник України. – 2004. – № 1451. – С. 1.
4. Директива Європейського парламенту та Ради «Про систему електронних підписів, що застосовується в межах Співтовариства». – 1999. – 1999/93/ЄС. – С. 1-6.
5. Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи // Госстандарт Республики Беларусь. – 1999. – СТБ 1176.2-99. – С. 3-5.
6. Информационная технология. Защита информации. Функция хеширования // Госстандарт Республики Беларусь. – 1999. – СТБ 1176.1-99. – С. 1-6.
7. Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи на основе эллиптических кривых // Госстандарт Республики Беларусь. – 2011. – СТБ П 34.101.45. – 2011. – С. 2-7.
8. Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности // Госстандарт Республики Беларусь. – 2011. – СТБ 34.101.31. – 2011.– С. 3-7.
9. Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел // Госстандарт Республики Беларусь. – 2012. – СТБ 34.101.47. – 2012. – С. 2-4.
10. Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации // Госстандарт Республики Беларусь. – 2011. – СТБ 34.101.27. – 2011. – С. 2-10.
11. Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей // Госстандарт Республики Беларусь. – 2012. – СТБ 34.101.19.
12. Об утверждении требований к сердствам электронной подписи и требований к средствам удостоверяющего центра : приказ Федеральной службы безопасности Российской Федерации от 27 ноября 2011 р. № 796. – С. 3-11.
13. Информационная технология. Криптографическая защита информации. Функция хеширования // ГостРФ. – 1994. – ГОСТ 34.11. – С. 2-12.
14. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи // ГостРФ. – 2001. – ГОСТ Р 34.10. – С. 23.
15. *Мелащенко А., Скарлат О.* Електронне діловодство // Інститут кібернетики імені В. М. Глушкова НАН України. – 2013. – С. 6-118.
16. *Мелащенко А., Перевозчикова О.* Організація кваліфікованої інфраструктури відкритих ключів // Видавництво «Наукова думка» НАН України». – 2010. – С. 47-58.