УДК 342.9(075.8)

АНТОНЕНКО С.А., співробітник НДІІП НАПрН України

КРИПТОГРАФІЧНІ ОСНОВИ ЗАСТОСУВАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ В УКРАЇНІ

Анотація. *У статті розглядаються питання застосування технологій і стандартів електронного цифрового підпису в Україні на основі сучасних криптографічних методів захисту інформації*

Ключові слова: *криптографічний захист інформації, електронний цифровий підпис, алгоритми шифрування, інфраструктура відкритих ключів*

Аннотация. *В статье рассматриваются вопросы применения технологий и стандартов электронной цифровой подписи в Украине на основе современных криптографических методов защиты информации*

Ключевые слова: *криптографическая защита информации, электронная цифровая подпись, алгоритмы шифрования, инфраструктура открытых ключей*

Summary. *This article reviewes the issues of the usage of technologies and standards of electronic digital signature in Ukraine on the basis of up-to-date cryptographic methods of information protection.*

Keywords: *cryptographic information protection, electronic digital signature, encryption-decryption algorithms, public key infrastructure.*

Постановка проблеми. Інформаційні технології на сьогодні охоплюють практично всі сфери сучасного життя, діяльності органів державного управління, фінансово-кредитної сфери, інформаційного обслуговування підприємницької діяльності, науки та освіти.

Все більше документів створюється, відправляється, передається, одержується, обробляється, використовується та зберігається в електронній формі, що дозволяє значно прискорити процеси прийняття управлінських рішень, підвищити їх якість, заощадити бюджетні кошти, відмовившись від паперових технологій обробки інформації.

Впровадження електронного документообігу з використанням електронного цифрового підпису (далі – ЕЦП), як пріоритетний напрямок державної політики електронного урядування, визначено в рішеннях Президента України, Кабінету Міністрів України та Верховної Ради України.

ЕЦП є обов’язковим реквізитом електронного документу, який використовується для ідентифікації автора та/або підписувача іншими суб’єктами електронного документообігу. Накладанням ЕЦП завершується створення електронного документу.

Становлення та розвиток національної системи ЕЦП є багатокомпонентним завданням, яке потребує комплексного, взаємоузгодженого вирішення питань на різних рівнях.

Метою статті є дослідження питань застосування технологій і стандартів ЕЦП на основі сучасних криптографічних методів захисту інформації, розроблення і гармонізації міжнародних стандартів, створення відповідної законодавчої та нормативно-правової бази для становлення й розвитку національної інфраструктури відкритих ключів в Україні.

Виклад основних положень. Впродовж багатьох століть людство використовувало криптографічні методи для захисту інформації при її передачі та зберіганні.

З часом ці методи сформувалися в окрему галузь математики – криптологію, яка вивчає захист інформації та підрозділяється на криптографію, що займається розробленням нових методів і обґрунтуванням їх коректності, і криптоаналіз, завданням якого є інтенсивне вивчення існуючих методів.

Криптографія і криптоаналіз знаходяться в тісній взаємодії одне з одним, та з практичними потребами, а також розвиваються паралельно закритими урядовими організаціями багатьох держав та міжнародним науковим співтовариством [1].

Тривалий час в криптографії використовувалися лише алгоритми симетричного шифрування, в яких відправник повинен був передати отримувачу разом із зашифрованим повідомленням і свій секретний ключ, яким було зашифроване це повідомлення, що створювало необхідність наявності закритого каналу для передачі секретного ключа та збільшувало ризики розкриття інформації.

Асиметричні алгоритми шифрування (на відміну від симетричних) використовують пару споріднених ключів – відкритий та секретний. При цьому, незважаючи на пов’язаність ключів у парі, обчислення секретного ключа на основі відкритого вважається технічно неможливим. В асиметричних криптосистемах відкритий ключ може вільно розповсюджуватись, в той час як приватний ключ має зберігатись в таємниці.

Як відомо, дослідження в напрямку криптографії з відкритим ключем були розпочаті в 1975 році шляхом об’єднання зусиль двох незалежних груп вчених Уїтфілда Діффі – Мартіна Хеллмана та Ральфа Меркла в Стенфордському університеті, що призвело в подальшому до відкриття, відомого як алгоритм Діффі – Хеллмана – Меркля (протокол обміну ключами), яке стало основою для створення міжнародної інфраструктури відкритих ключів (та сама схема була розроблена Малькольмом Вільямсоном в 1970-х, але трималася в секреті до 1997 року).

Роком пізніше групою вчених Массачусетського технологічного інституту Рональдом Рівестом, Аді Шаміром та Леонардом Адлеманом був винайдений перший алгоритм асиметричного шифрування RSA (названий по перших літерах прізвищ його винахідників), який дозволив вирішити проблему спілкування через незахищений канал та став основою для створення ЕЦП – складової інфраструктури відкритих ключів.

ЕЦП створювався для аутентифікації текстів, що передаються по телекомунікаційних каналах, зі збереженням основних властивостей звичайного рукописного підпису (засвідчує, що підписаний текст виходить саме від особи, що поставила підпис – *автентичність*, і не дає саме цій особі можливості відмовитися від зобов’язань, пов’язаних із підписаним текстом – *неспростовність*).

За реалізацією ЕЦП є невеликою кількістю додаткової інформації, що передається разом із підписаним текстом.

На відміну від шифрування, при формуванні ЕЦП використовується секретний ключ, а при перевірці – відкритий.

Алгоритм генерації цифрового підпису повинен забезпечувати неможливість створення ЕЦП без секретного ключа, який при перевірці буде визнаний правильним.

ЕЦП використовуються для того, щоб підтвердити, що повідомлення надійшло дійсно від даного відправника (за припущення, що лише відправник володіє секретним ключем, відповідним його відкритому ключу).

Також ЕЦП використовуються для проставляння штампу часу (timestamp) на документах: сторона, якій ми довіряємо, підписує документ із штампом часу за допомогою свого секретного ключа і, таким чином, підтверджує, що документ вже існував на момент, оголошений в штампі часу [2].

Стан, сутність, проблемні питання теорії та практики застосування ЕЦП в інформаційних та інформаційно-телекомунікаційних системах різноманітного призначення детально розглянуті у двох монографіях видатних українських вчених у галузі криптографії Горбенка І.Д. та Горбенка Ю.І.: “Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика” [3], “Прикладна криптологія. Теорія. Практика. Застосування” [4], які були опубліковані в 2010 та 2012 роках відповідно.

Як зазначають автори, основні послуги систем криптографічного захисту, такі як цілісність, справжність і неспростовність відправника можуть бути забезпечені за умови обов’язкового використання ЕЦП. Обов’язковим елементом, що використовується в ЕЦП, є хеш-функція, за допомогою якої обчислюється хеш-значення від електронних даних і взагалі інформації, що підписується.

Криптографічні хеш-функції використовуються зазвичай для генерації дайджесту повідомлення при створенні ЕЦП. Хеш-функції відображають повідомлення в те, що має фіксований розмір хеш-значення таким чином, що вся безліч можливих повідомлень розподіляється рівномірно по безлічі хеш-значень.

При цьому криптографічна хеш-функція робить це таким чином, що практично неможливо підігнати документ до заданого хеш-значення.

В системі ЕЦП криптографічна хеш-функція повинна забезпечувати стійкість до колізій (різні результати перетворення для різних наборів даних) та необоротність (неможливість обчислити вхідні дані за результатом перетворення).

Криптографічні хеш-функції зазвичай створюють значення довжиною у 128 та більше біт, що значно перевищує кількість повідомлень, які будь-коли існуватимуть у світі.

Багато надійних криптографічних хеш-функцій доступно безкоштовно. Широко відомими є MD5 і SHA [2].

До основних математичних методів, що застосовуються в системах ЕЦП є на сьогодні асиметричні перетворення у кільцях, полях Галуа та групі точок еліптичних кривих [4].

Основи регулювання правових відносин щодо захисту інформації в автоматизованих системах (в редакції Закону України від 31.05.05 р. № 2594-IV – інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах) за умов дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації були закріплені в Законі України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.94 р. № 80/94-ВР [5].

В законодавстві України вперше визначення терміну *криптографічного захисту* як виду захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства міститься у “Положенні про порядок здійснення криптографічного захисту інформації в Україні” затвердженому Указом Президента України від 22.05.98 р. № 505/98 [6].

Положення також надавало визначення *засобу криптографічного захисту інформації, криптографічної системи, системи криптографічного захисту інформації* та покладало функції зі здійснення державної політики щодо криптографічного та технічного захисту інформації на Головне управління урядового зв’язку (з 27.10.1999 р. Департамент спеціальних телекомунікаційних систем та захисту інформації) Служби безпеки України, а з 11.04.08 р. – Державну службу спеціального зв’язку та захисту інформації України.

З метою вироблення єдиного підходу, відкритого для різних технологій та послуг, що надає можливість засвідчувати інформацію електронним шляхом в умовах швидкого розвитку технологій і глобальної мережі Інтернет, Європейським парламентом та Радою Європейського Союзу була прийнята Директива 1999/93/ЄС **“**Про систему електронних підписів, що застосовується в межах Співтовариства**”** від 13.12.99 р. [7] та Рішення Комісії 2000/709/ЄС Європейського парламенту та Ради **“**Про мінімальні критерії, які враховуватимуться Державами-членами під час визначення органів, згідно статті 3(4) Директиви 1999/93/ЄС Європейського парламенту та Ради про систему електронних підписів, що застосовуються в межах Співтовариства**”** від 06.11.00 р.

На сьогодні положення Директиви 1999/93/ЄС реалізовано у вигляді відповідних технічних європейських та міжнародних стандартів (ETSI та RFC).

Підґрунтям розбудови національної системи ЕЦП в Україні стали фундаментальна теоретична база і багаторічні практичні напрацювання вітчизняних наукових шкіл у кібернетичній та криптографічній галузях, вивчення та адаптація кращого міжнародного досвіду, врахування міжнародних стандартів і рекомендацій:

- RFC 2631 “Diffie-Hellman Key Agreement Method”, June 1999;
- RFC 2785 “Methods for Avoiding the “Small-Subgroup” Attacks on the Diffie-Hellman Key Agreement for S/MIME”, March 2000;
- RFC 3279 “Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, April 2002;
- RFC 3281 “An Internet Attribute Certificate Profile for Authorization”, April 2002;
- RFC 3370 “Cryptographic Message Syntax (CMS) Algorithms”, August 2002;
- RFC 3394 “Encryption Standard (AES) Key Wrap Algorithm”, September 2002;
- RFC 3852 “Cryptographic Message Syntax (CMS)”, July 2004;
- RFC 4490 - Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS), May 2006;
- RFC 5008 “Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)”, September 2007;
- RFC 5480 “Elliptic Curve Cryptography Subject Public Key”, March 2009;
- RFC 5652 “Cryptographic Message Syntax (CMS)”, September 2009,

а також розроблення чи гармонізація в Україні міжнародних стандартів криптографічного захисту інформації:

- ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”;
- ДСТУ ISO/IEC 11770-3:2002 “Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів”;
- ДСТУ ISO/IEC 15946-3:2006 “Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Установлення ключів”;
- ДСТУ ISO/IEC 10118-3:2005 “Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції”;
- ДСТУ ISO/IEC 9594-8:2006 “Інформаційні технології. Взаємозв’язок відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів”
- ДСТУ ГОСТ 28147-2009 “Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования”,

і міждержавних стандартів:

- ДСТУ ГОСТ 34.310-95 “Информационные технологии. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма”;

- ДСТУ ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хеширования”.

Національний стандарт ДСТУ 4145-2002 визначив механізм ЕЦП, який ґрунтується на властивостях груп точок еліптичних кривих, що при застосуванні з необхідною ймовірністю гарантує цілісність підписаного повідомлення, автентичність його автора та неспростовність підписаного документу [3].

Рішенням шостого засідання Міжвідомчої координаційної ради з адаптації законодавства України до законодавства ЄС **“**Щодо стану роботи з адаптації законодавства України до законодавства Європейського Союзу**”** від 28.09.01 р. [8] Директива 1999/93/ЄС [7] була включена до орієнтовного переліку нормативних актів ЄС, до яких мало бути адаптоване законодавство України протягом 2002 – 2004 років.

В подальшому, з метою встановлення основних організаційно-правових засад електронного документообігу, використання електронних документів, визначення правового статусу ЕЦП та врегулювання відносин, що виникають при його використанні в Україні, були розроблені (суб’єкт ініціативи: Кабінет Міністрів України) і прийняті одночасно два Закони України “Про електронні документи та електронний документообіг” від 22.05.03 р. № 851-IV [9] та “Про електронний цифровий підпис” від 22.05.03 р. № 852-IV [10], які набрали чинності з 1 січня 2004 року.

В основу побудови Національної системи електронного цифрового підпису України була закладена модель централізованої інфраструктури управління відкритими ключами (ієрархії довіри), яка на відміну від іншої моделі – розподіленої інфраструктури (мережі довіри), потребує наявності центрального засвідчувального (ЦЗО) та контролюючого органів в цій системі.

Закон України “Про електронний цифровий підпис” визначив правовий статус ЕЦП та врегулював на законодавчому рівні відносини, що виникають при його використанні.

Законом закріплені визначення термінів, що використовуються у сфері ЕЦП. Зокрема, це поняття ЕЦП, засобу ЕЦП, особистого та відкритого ключів, засвідчення чинності відкритого ключа, сертифікату та посиленого сертифікату відкритого ключа, процедур акредитації, послуг ЕЦП, надійного засобу ЕЦП та ін.

Так під *електронним цифровим підписом* розуміється вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

Встановлено також, що ЕЦП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Закон визначає процедури генерації ключів, підписування та перевірки ЕЦП, формування, розповсюдження, скасування, зберігання, блокування та поновлення сертифікатів відкритих ключів (у тому числі й посилених), послуг фіксування часу та ін.

На виконання вимог Закону [10] постановами Кабінету Міністрів України протягом 2004 року були затверджені:

- порядок засвідчення наявності електронного документу (електронних даних) на певний момент часу [11];

- положення про ЦЗО [12];

- порядок акредитації центру сертифікації ключів (ЦСК) [13];

- порядок обов’язкової передачі документованої інформації [14];

- порядок застосування ЕЦП органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності [15].

Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.05 р. № 3, зареєстрованим у Міністерстві юстиції України, були затверджені Правила посиленої сертифікації [16].

Прийняття цих документів дозволило розпочати побудову в Україні національної системи ЕЦП.

Роботи зі створення ПТК ЦЗО розпочалися у 2004 році на базі державного підприємства **“**Державний центр інформаційних ресурсів України**”** Міністерства транспорту та зв’язку.

Також у 2007 – 2008 роках відповідними наказами Адміністрації Державної служби спеціального зв’язку та захисту інформації України, зареєстрованими у Міністерстві юстиції України, були затверджені:

- правила проведення робіт із сертифікації засобів захисту інформації [17];
- положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації [18];
- положення про державну експертизу у сфері криптографічного захисту інформації [19].

У 2012 році Міністерство юстиції України та Державна служба спеціального зв’язку та захисту інформації України спільним наказом **“**Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису**”** від 20.08.12 р. № 1236/5/453 [20], зареєстрованим у Міністерством юстиції України, затвердили розроблені вимоги до форматів посиленого сертифікату відкритого ключа, списку відкликаних сертифікатів, підписаних даних; структури об’єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами; а також вимоги до протоколів фіксування часу та визначення статусу сертифікату.

Наказ також встановив строки застосування положень цих вимог у ПТК акредитованих центрів сертифікації ключів та надійних засобах ЕЦП (для їх замовників, розробників, виробників та організацій, що здійснюють експлуатацію).

З метою визначення технічних умов щодо забезпечення сумісності засобів криптографічного захисту інформації різних розробників шляхом встановлення єдиних форматів криптографічних повідомлень Державною службою спеціального зв’язку та захисту інформації України був виданий наказ **“**Про затвердження Вимог до форматів криптографічних повідомлень**”** від 18.12.12 р. № 739, зареєстрований Міністерством юстиції України від 14.01.13 р. № 108/22640 [21].

В цих Вимогах визначено синтаксис (формат представлення) криптографічних повідомлень (зашифрованих даних) в електронній формі, а також протоколи, які повинні застосовуватися для цього синтаксису з метою узгодження ключів.

Положення Вимог є обов’язковими для засобів криптографічного захисту інформації (КЗІ) та надійних засобів ЕЦП, що використовуються в системах електронного документообігу. Правильність реалізації у засобах КЗІ та ЕЦП наведених у Вимогах форматів і протоколів повинна бути підтверджена позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації.

Наказом Міністерства юстиції України від 29.01.13 р. № 183/5 був затверджений новий Регламент роботи ЦЗО [22].

У вересні 2012 року до закінчення терміну дії попереднього сертифікату ЦЗО був виданий новий кореневий сертифікат терміном на 10 років (з 28.09.12 р. по 28.09.22 р.), а

також протягом 2012 – 2013 рр. сформовані та видані сертифікати ключів Центрів, що надають послуги, пов’язані з ЕЦП, терміном на 5 років.

На сьогодні в Україні діє 21 АЦСК, що пройшли акредитацію ЦЗО (з них державної власності: ДП **“**Українські спеціальні системи**”** (2 центри: **“**Центр автентифікації національної системи конфіденційного зв’язку**”** та **“**УСС-Цезаріс**”**), КП **“**Головний інформаційно-комунікаційний і науково-виробничий центр**”** Дніпропетровської обласної ради, ДП **“**Головний інформаційно-обчислювальний центр Державної адміністрації залізничного транспорту України**”**, Центр сертифікації ключів Інформаційно-довідкового департаменту Міністерства доходів і зборів України, Державної казначейської служби України). Також діє один Акредитований засвідчувальний центр Національного банку України.

Різні аспекти застосування ЕЦП обговорювалися протягом останніх років за нашою участю разом з іншими актуальними питаннями на міжнародних конференціях, конгресах, форумах та інших заходах. Найбільш важливими та змістовними з них були:

- Перший та Другий Міжнародні Форуми з ЕЦП **“**PKI-FORUM УКРАЇНА 2012**”** (16-18 травня 2012 р., м. Київ), **“**PKI-FORUM УКРАЇНА 2013**”** (10-12 квітня 2013 р., м. Київ);

- Міжнародні наукові конгреси **“**З розвитку інформаційно-комунікаційних технологій та розбудови інформаційного суспільства в Україні**”** (17-18 листопада 2011 р., м. Київ) та **“**Інформаційне суспільство в Україні**”** (25-26 жовтня 2012 р., м. Київ);

- “Дні електронного урядування-2011” (16-20 травня 2011 р., м. Київ), та **“**Дні інформаційного суспільства-2012**”** (24-25 квітня 2012 р., м. Київ), **“**Дні інформаційного суспільства-2013**”** (20-21 травня 2013 р., м. Київ);

- VI Міжнародна науково-практична конференція “Наука і соціальні проблеми суспільства: інформатизація та інформаційні технології” (24-25 травня 2011 р., м. Харків);

- Перший український міжнародний форум з електронного урядування “International Ukrainian E-governance - Forum” (26-28 листопада 2012 р., м. Київ).

За результатами обговорень, при довготривалому зберіганні електронних документів (у т. ч. й архівному), експерти виділяють такі загрози, як: зміна технологій і стандартів ЕЦП; компрометація секретного ключа та технологій ЕЦП; відсутність гарантій доступності сертифіката ключа в довгостроковій перспективі; зміна програмно-апаратних платформ і як наслідок – неможливість використання старих засобів перевірки ЕЦП.

У відповідності з концепцією асиметричних систем щодо застосування особистих ключів безумовно мають бути дотримані вимоги забезпечення їх конфіденційності, цілісності, справжності, доступності та неспростовності. Указані вимоги мають бути забезпечені кожним із користувачів, оскільки особистий ключ доступний тільки його власнику, і він повинен і може зберігати його в таємниці.

Значно складнішими є задачі захисту відкритих ключів, що пояснюється тим, що відкриті ключі мають бути доступні всім користувачам, які виконують перевірку електронних документів, даних тощо. За таких умов необхідно забезпечити їх цілісність, справжність, доступність і неспростовність. Вирішення цієї задачі ґрунтується на використанні концепції сертифікатів відкритих ключів, причому для різних додатків – направленого шифрування, ЕЦП, криптографічного протоколу тощо [3, с. 7].

Компрометація особистого ключа можлива в результаті його викрадення у будь-який спосіб або його підробки – відтворення (реконструкції) секретного (особистого) ключа на основі знання відкритої частини ключа (з якою він пов’язаний певним математичним співвідношенням, оскільки разом вони утворюють ключову пару), методу шифрування, вихідного і зашифрованого текстів (на практиці процес підробки

особистого ключа потребує наявності спеціальних апаратних і програмних засобів, а також величезних витрат обчислювального часу). За ступенем складності розрізняють екзистенційну, вибіркову та універсальну підробки.

Визнають також можливість колізії хеш-функції – отримання однакового значення функції для різних повідомлень. Можливість швидкого знаходження цих колізій рівноцінна дискредитації, бо надає можливість підробки ЕЦП (ступенем криптографічної стійкості хеш-функції вважається обчислювальна складність знаходження колізій). Якщо для деякої хеш-функції знаходиться спосіб знайдення колізій, значно швидший за повний перебір, тоді ця хеш-функція припиняє вважатися криптостійкою і використовуватись для передачі і збереження секретної інформації [3].

Як перспективні розглядаються перетворення зі спарюванням точок еліптичних кривих та на гіпереліптичних кривих. Ці перетворення вивчені теоретично, створені та випробовуються дослідні версії, розроблені рекомендації та обговорюється необхідність створення регіональних та міжнародних стандартів [4].

Висновки.

На сьогодні в Україні в основному створено нормативно-правове підґрунтя та технологічну основу для функціонування ЕЦП:

- прийнятий Національний стандарт ДСТУ 4145-2002, що визначив механізм ЕЦП та з необхідною ймовірністю гарантує цілісність підписаного повідомлення, автентичність його автора та неспростовність підписаного документа;

- законами та підзаконними актами України встановлені процедури генерації ключів, підписування та перевірки ЕЦП, формування, розповсюдження, скасування, зберігання, блокування та поновлення сертифікатів відкритих ключів (у тому числі й посилених), послуг фіксування часу та ін.;

- розроблені вимоги до форматів посиленого сертифіката відкритого ключа, списку відкликаних сертифікатів, підписаних даних; структури об’єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами; а також вимоги до протоколів фіксування часу та визначення статусу сертифіката;

- встановлені єдині вимоги до форматів криптографічних повідомлень із визначенням синтаксису (формату представлення) криптографічних повідомлень (зашифрованих даних) в електронній формі, а також протоколів, які повинні застосовуватися для цього синтаксису з метою узгодження ключів;

- створений ПТК ЦЗО, діють ЦСК та АЦСК, затверджений новий регламент роботи ЦЗО, виданий новий кореневий сертифікат, сформовані та видані сертифікати ключів Центрів, що надають послуги, пов’язані з ЕЦП.

Подальше удосконалення та розвиток національної системи ЕЦП (за баченням провідних вчених вітчизняних наукових шкіл у кібернетичній та криптографічній галузях) потребуватиме узгодженого вирішення питань на законодавчому (нормативно-правовому), загальносистемному, процедурно-функціональному, функціонально-технічному та програмно-технічному рівнях.

Використана література

1. Терехов А.Н. Криптография с открытым ключом: от теории к стандарту / А.Н.Терехов, А.В. Тискин // Программирование РАН. – 1994. – № 5. – С. 17-22.

2. Tatu Ylonen “Introduction to Cryptography”. – Режим доступу : //www.cs.hut.fi/ssh/crypto/intro.html

3. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія / Ю.І. Горбенко, І.Д. Горбенко ; Харк. нац. ун-т радіоелектрон., ЗАТ Ін-т інформ. технологій. – Х. : Форт, 2010. – 593 с.

4. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І. Горбенко ; Харк. нац. ун-т радіоелектрон., ЗАТ **“**Ін-т інформ. технологій**”**. – Х. : Форт, 2012. – 868 с.

5. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.94 р. № 80/94-ВР. – Режим доступу : http://zakon.rada.gov.ua

6. Про Положення про порядок здійснення криптографічного захисту інформації в Україні : Указ Президента України від 22.05.98 р. № 505/98. – Режим доступу : http://zakon.rada. gov.ua

7. Про систему електронних підписів, що застосовується в межах Співтовариства : Директива 1999/93/ЄС Європейського парламенту та Ради від 13.12.99 р. – Режим доступу : http://zakon.rada.gov.ua

8. Щодо стану роботи з адаптації законодавства України до законодавства Європейського Союзу : Рішення шостого засідання Міжвідомчої координаційної ради з адаптації законодавства України до законодавства ЄС від 28.09.01 р. – Режим доступу : http://zakon.rada. gov.ua

9. Про електронні документи та електронний документообіг : Закон України від 22.05.03 р. № 851-IV. – Режим доступу : http://zakon.rada.gov.ua

10. Про електронний цифровий підпис : Закон України від 22.05.03 р. № 852-IV. – Режим доступу : http://zakon.rada.gov.ua

11. Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу : Постанова Кабінету Міністрів України від 26.05.04 р. № 680. – Режим доступу : http://zakon.rada.gov.ua

12. Про затвердження Положення про центральний засвідчувальний орган : Постанова Кабінету Міністрів України від 28.10.04 р. № 1451. – Режим доступу : http://zakon.rada.gov.ua

13. Про затвердження Порядку акредитації центру сертифікації ключів : Постанова Кабінету Міністрів України від 13.07.04 р. № 903. – Режим доступу : http://zakon.rada.gov.ua

14. Про затвердження Порядку обов’язкової передачі документованої інформації : Постанова Кабінету Міністрів України від 28.10.04 р. № 1454. – Режим доступу : http://zakon.rada.gov.ua

15. Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності : Постанова Кабінету Міністрів України від 28.10.04 р. № 1452. – Режим доступу : http://zakon.rada.gov.ua

16. Про затвердження Правил посиленої сертифікації : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.05 р. № 3. – (Зареєстрований Міністерством юстиції України від 27.01.05 р. № 104/10384). – Режим доступу : http://zakon.rada.gov.ua

17. Про затвердження Правил проведення робіт із сертифікації засобів захисту інформації : наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України, Державного комітету України з питань технічного регулювання та споживчої політики від 25.04.007 р. № 75/91. – (Зареєстрований Міністерством юстиції України від 14.05.07 р. № 498/13765). – Режим доступу : http://zakon.rada.gov.ua

18. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації : наказ Державної служби спеціального зв’язку та захисту інформації України від 20.07.07 р. № 141. – (Зареєстрований Міністерством юстиції України від 30.07.07 р. № 862/14129). – Режим доступу : http://zakon.rada.gov.ua

19. Про затвердження Положення про державну експертизу у сфері криптографічного захисту інформації : наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 23.06.08 р. № 100. – (Зареєстрований Міністерством юстиції України від 16.07.2008 р. № 651/15342). – Режим доступу : http://zakon.rada.gov.ua

20. Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису : наказ Міністерства юстиції України та Державної служби спеціального зв’язку та захисту інформації України від 20.08.12 р. № 1236/5/453. – (Зареєстрований Міністерством юстиції України від 20.08.12 р. № 1398/21710). – Режим доступу : http://zakon.rada.gov.ua

21. Про затвердження Вимог до форматів криптографічних повідомлень : наказ Державної служби спеціального зв’язку та захисту інформації України від 18.12.12 р. № 739. – (Зареєстрований Міністерством юстиції України від 14.01.13 р. № 108/22640). – Режим доступу : http://zakon.rada.gov.ua

22. Про затвердження Регламенту роботи центрального засвідчувального органу : наказ Міністерства юстиції України від 29.01.13 р. № 183/5. – (Зареєстрований Міністерством юстиції України від 30.01.13 р. № 191/22723). – Режим доступу : http://zakon.rada.gov.ua

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~