УДК 342.9(075.8) **Сергій Антоненко ***

КРИПТОГРАФІЧНІ ОСНОВИ ЗАСТОСУВАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ В УКРАЇНІ

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.

Антоненко С. А. Криптографические основы применения электронной цифровой подписи в Украине.

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.

Antonenko S. A. Cryptographic grounds of the usage of electronic digital signature in Ukraine.

In this article are reviewed 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. Усе 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.

Упровадження електронного документообігу з використанням електронного цифрового підпису (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 документа, який використовується для ідентифікації автора та/або підписувача іншими суб'єктами електронного документообігу. Накладанням ЕЦП завершується створення електронного документа.

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 поділяється на криптографію, що займається розробленням нових методів і обгрунтуванням їх коректності, і криптоаналіз, завданням якого є інтенсивне вивчення існуючих методів [1].

Тривалий час у 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 учених У. Діффі – М. Хеллмана та Р. Меркла в Стенфордському університеті, що призвело в подальшому до відкриття відомого як алгоритм Діффі–Хеллмана–Меркла (протокол обміну ключами), яке стало основою для створення міжнародної інфраструктури відкритих ключів (та сама схема була розроблена М. Вільямсоном у 1970-х, але трималася в секреті до 1997 року).

Роком пізніше групою вчених Массачусетського технологічного інституту Р. Рівестом, А. Шаміром та Л. 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 штампа 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 у 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 учених у галузі криптографії Горбенка І. Д. та Горбенка Ю. І.: «Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика» [3] та «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 дайджеста 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.

У 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 бітів, що значно перевищує кількість повідомлень, які коли-небудь 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 інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах були закріплені в Законі України від 05.07.1994 № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах» [5].

У законодавстві України вперше визначення терміна «*криптографічний захист*» 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 22.05.1998 № 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 27.09.1999 Департамент спеціальних телекомунікаційних систем та захисту інформації) Служби безпеки України, а з 11.04.2008 – на 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 «Про систему електронних підписів, що застосовується в межах Співтовариства» від 13.12.1999 № 1999/93/ЄС [7].

На сьогодні положення Директиви 1999/93/ЄС реалізовано у вигляді відповідних технічних європейських та міжнародних стандартів (ETSI та RFC) [3, с. 8–9].

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.

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.

Рішенням шостого засідання Міжвідомчої координаційної ради з адаптації законодавства України до законодавства ЄС від 28.09.2001 «Щодо стану роботи з адаптації законодавства України до законодавства Європейського Союзу» Директива 1999/93/ЄС [7] була включена до орієнтовного переліку нормативних актів ЄС, до яких мало бути адаптоване законодавство України протягом 2002–2004 років.

У подальшому, з метою встановлення основних організаційно-правових засад електронного документообігу, використання електронних документів, визначення правового статусу електронного цифрового підпису (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» № 851-IV [8] та «Про електронний цифровий підпис» № 852-IV від 22.05.2003 [9], 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 [9] постановами Кабінету Міністрів України протягом 2004 року були затверджені:

– порядок засвідчення наявності електронного документу (електронних даних) на певний момент часу;

– положення про ЦЗО;

– порядок акредитації центру сертифікації ключів (ЦСК);

– порядок обов'язкової передачі документованої інформації;

– порядок застосування ЕЦП органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності.

Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.2005 № 3, зареєстрованим у Міністерстві юстиції України, були затверджені Правила посиленої сертифікації [10].

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;

– порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації;

– порядок проведення державної експертизи у сфері криптографічного захисту інформації.

У 2012 році Міністерство юстиції України і Державна служба спеціального зв'язку та захисту інформації України спільним наказом від 20.08.2012 № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису» [11], 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 від 18.12.2012 № 739 «Про затвердження Вимог до форматів криптографічних повідомлень», зареєстрований Міністерством юстиції України 14.01.2013 за № 108/22640 [12].

У 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 29.01.2013 № 183/5 був затверджений новий Регламент роботи ЦЗО [13].

У вересні 2012 року до закінчення терміну дії попереднього сертифікату ЦЗО був виданий новий кореневий сертифікат терміном на 10 років (з 28.09.2012 по 28.09.2022), 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 активно 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. Також кожним із користувачів ЕЦП повинні бути дотримані вимоги щодо забезпечення конфіденційності, цілісності, справжності, доступності та неспростовності (для відкритих та особистих ключів), а також конфіденційності (для особистих ключів) [3, с. 7].

Компрометація особистого ключа можлива в результаті його викрадення або підробки – відтворення на основі знання відкритої частини ключа (з якою він пов'язаний певним математичним співвідношенням), методу шифрування, вихідного і зашифрованого текстів. 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;

– встановленні 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.

Список використаних джерел:

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» [Електронний ресурс] – Режим доступу : http://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.

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 05.07.1994 № 80/94-ВР [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.

6. Про Положення про порядок здійснення криптографічного захисту інформації в Україні : Указ Президента України від 22.05.1998 № 505/98 [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.

7. Про систему електронних підписів, що застосовується в межах Співтовариства : Директива Європейського Парламенту та Ради Європейського Союзу від 13.12.1999 № 1999/93/ЄС [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.

8. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.

9. Про електронний цифровий підпис : Закон України від 22.05.2003 № 852-IV [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.

10. Про затвердження Правил посиленої сертифікації : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.2005 № 3 [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.

11. 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 20.08.2012 № 1236/5/453 [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.

12. Про затвердження Вимог до форматів криптографічних повідомлень : наказ Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.

13. Про затвердження Регламенту роботи центрального засвідчувального органу : наказ Міністерства юстиції України від 29.01.2013 № 183/5 [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.

**** Антоненко Сергій Анатолійович – завідувач наукового відділу системної інформатизації законотворчої діяльності НДІІП НАПрН України, лауреат премії імені Ярослава Мудрого.***