ronic resource]. – Mode of access: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_ book_introduction.pdf. – Title from screen.

[6] *Foscarini F.* InterPARES 2 and the Records-Related Legislation of the European Union // Archivaria: The Journal of the Association of Canadian Archivists. – Spring, 2007. – Vol. 63. – P. 121–136.

[7] Module 1: Introduction – A Framework for Digital Preservation. InterPARES [Electronic resource] / ICA DRAFT July 2012. – Mode of access: http://www.ciscra.org/. – Title from screen.

[8] The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 3 Project [Electronic resource]. – Mode of access: http://www.interpares.org/ip3/ip3_general_studies.cfm. – Title from screen.

[9] Проект «Пам'ять світу» – один з найстаріших міжнародних проектів по створенню електронної колекції пам'ятників культури, ініційований ЮНЕСКО у рамках Програми захисту і збереження Всесвітньої документальної спадщини, заснованої 1992 р. Хартію про зберігання цифрової спадщини «Charter on the Preservation of the Digital Heritage» прийнято ЮНЕСКО на 32 сесії Генеральної Конференції 17 жовтня 2003 р. Режим доступу: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/charter_preservation_digital_heritage_en.pdf.

[10] *Duranti L.* The Future of Our Digital Memory. The Contribution of the InterPARES Project to the Preservation of the Memory of the World [Electronic resource]. – Mode of access: http://www.unesco.org/new/fileadmin / MULTIMEDIA/HQ/CI/CI/pdf/mow/interpares_en.pdf. – Title from screen.

[11] *Goh E., Duranti L., Chu S.* Archival Legislation for Engendering Trust in an Increasingly Networked Digital Environment [Electronic resource]. – Mode of access: http://www.ica2012.com/files/data/Full%20papers% 20upload/ica12Final00287.pdf. – Title from screen.

Вадим Малиновський

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ КРИПТОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Нині майже не існує систем електронного документообігу, які б не містили засобів криптографічного захисту інформації (далі – КЗІ), зокрема засобів, що дозволяють використовувати в електронному документообігу електронний цифровий підпис.

Однак, як для суб'єктів захисту електронних документів, так і для розробників засобів криптографічного (далі – криптозасобів) захисту електронних документів до нині залишається ще не вирішеною низка проблем:

– створення об'єктивної і оптимальної системи оцінок безпеки електронних документів та криптографічної стійкості засобів шифрування й електронного цифрового підпису;

– вдосконалення методів і способів ефективної апаратної та програмної реалізації криптографічних алгоритмів;

– розробка високоефективних систем криптоаналізу для дослідження сучасних систем криптозахисту даних;

– створення інформаційних систем у державних архівах та формування підходів і вимог до забезпечення їхньої безпеки.

Найнадійнішими криптосистемами є системи, засновані на апаратних засобах КЗІ. Вони реалізуються на основі програмованих та апаратно-орієнтованих процесорах. Апаратно-програмні та програмні засоби з точки зору криптографії переваг перед апаратними засобами КЗІ не мають.

Тепер активно досліджується проблема вразливості й атак на кінцеві реалізації криптоалгоритмів через побічні канали витоку інформації.

Програмні засоби шифрування є реалізацію одного або декількох криптоалгоритмів на мові програмування високого або низького рівня, у вигляді модулів, бібліотек, окремих програм із функцією криптографічного захисту.

Для успішного проходження сертифікації програмний засіб захисту повинен обов'язково відповідати певним критеріям, зокрема вимогам безпеки.

Вимоги до програмних засобів КЗІ встановлюються нормативними документами. В кожній країні розробляються власні нормативні документи з даного напряму діяльності, найчастіше – стандарти.

Склад та структура засобів криптографічного захисту електронних документів залежить від призначення системи електронного документообігу, середовища функціонування та наявності документів з обмеженим доступом. Засоби КЗІ застосовуються не тільки в захищених системах, де є потреба в високому рівні конфіденційності, а й в системах, де є певні вимоги до забезпечення цілісності, ідентифікації та автентифікації, наприклад у системах електронного документообігу органів виконавчої влади.

Порівняння вітчизняної нормативної бази (не враховуючи керівні документи, що мають гриф обмеження доступу) з закордонною дає підстави зробити висновок, що в законодавстві України відсутня низка документів, які б відкрили можливість унормувати деякі важливі питання щодо засобів КЗІ.

На нашу думку, враховуючи особливості вітчизняного законодавства, передовий досвід інших країн (Сполучені Штати Америки, Німеччина) та досягнення вітчизняних та закордонних учених у галузі криптології, актуальним питанням є розроблення власних стандартів, в яких були б детально викладені вимоги до технічної реалізації як криптозасобів у цілому, так і засобів електронного підпису.