ПЕРЕДМОВА

Успішне впровадження сучасних технологій електронного управління, електронного документообігу, електронного цифрового підпису не можливе без створення відповідної інфраструктури. Технологічною інфраструктурою реалізації вищевказаних та інших технологій є інфраструктура відкритих ключів. Рішення фундаментальних проблем впровадження систем електронного цифрового підпису потребує глибокого розуміння загальнотеоретичних і методологічних знань побудови та практичного впровадження інфраструктури відкритих ключів (ІВК). Розуміння цих основ є важливим елементом підготовки фахівців у галузі захисту інформації. Але не тільки для них. Розуміння технології ІВК є важливим і для тих, хто впроваджує та використовує системи електронного документообігу на будь-яких рівнях управління.

Запропонований матеріал висвітлює основні особливості побудови та впровадження ІВК: архітектуру, формати даних, моделі життєвого циклу сертифікатів, протоколи обміну інформацією тощо.

Методичні вказівки складаються з трьох частин та 12 розділів.

У першій частині посібника розкрито основи сертифікації відкритих ключів, спираючись на вимоги міжнародних стандартів, та сутність інфраструктури відкритих ключів, описано структуру та класифікацію сертифікатів відкритих ключів. Розглянуто модель життєвого циклу особистого ключа та сертифіката відкритого ключа, дано характеристику основних механізмів поширення інформації щодо статусу сертифікатів.

Використання електронних послуг із застосуванням цифрового підпису спирається на довіру між суб’єктами взаємодії, інфраструктуру відкритого ключа та спрямоване на реалізацію моделі довіри.

У другій частині розглянуто концепції довіри в ІВК та основних механізмів реалізації довіри.

В третій частині висвітлено питання нормативного регулювання та стандартизації в галузі сертифікації відкритих ключів. У розділах ідеться про вимоги міжнародних стандартів, особливості стандартизації в цій галузі, здійснюється порівняння національної та міжнародної нормативної бази.