

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ	5
ПЕРЕДМОВА	6
ЧАСТИНА I. ОСНОВИ СЕРТИФІКАЦІЇ ВІДКРИТИХ КЛЮЧІВ	7
РОЗДІЛ 1. ВСТУП ДО ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ.....	7
1.1. Загальні положення.....	7
1.2. Основні терміни та визначення, що використовуються у сфері ІВК.....	8
1.3. Склад та призначення основних підсистем ІВК	8
1.4. Програмно-технічна реалізація підсистеми управління СВК.....	15
1.5. Національна інфраструктура відкритих ключів України.	17
<i>Запитання та завдання для самоконтролю</i>	24
РОЗДІЛ 2. СТРУКТУРА СЕРТИФІКАТА ВІДКРИТОГО КЛЮЧА	25
2.1. Формат сертифіката відкритого ключа	25
2.2. Розширення сертифіката	28
<i>Запитання та завдання для самоконтролю</i>	30
РОЗДІЛ 3. КЛАСИФІКАЦІЯ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ	31
3.1. Сертифікати кінцевих об'єктів.....	31
3.2. Сертифікати уповноважених на сертифікацію	32
3.3. Самопідписані сертифікати	34
<i>Запитання та завдання для самоконтролю</i>	36
РОЗДІЛ 4. ЖИТТЄВИЙ ЦИКЛ ОСОБИСТОГО КЛЮЧА	
І СЕРТИФІКАТА ВІДКРИТОГО КЛЮЧА	37
4.1. Життєвий цикл особистого ключа	37
4.2. Життєвий цикл сертифіката відкритого ключа.....	41
<i>Запитання та завдання для самоконтролю</i>	46
РОЗДІЛ 5. ФОРМАТ СПИСКІВ ВІДКЛИКАНИХ СЕРТИФІКАТІВ	47
5.1. Формат списку відкликаних сертифікатів	48
5.2. Розширення СВС	51
5.3. Розширення записів СВС	53
5.4. Розширення для пунктів розповсюдження СВС та дельта-СВС	55
<i>Запитання та завдання для самоконтролю</i>	59
РОЗДІЛ 6. МЕХАНІЗМИ РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ	
ЩОДО ВІДКЛИКАННЯ СЕРТИФІКАТІВ	60
6.1. Механізми періодичної публікації.....	60
6.2. Механізми онлайн-запитів	66
6.3. Інші режими відкликання.....	67
<i>Запитання та завдання для самоконтролю</i>	68
ЧАСТИНА II. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ	
ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ	69
РОЗДІЛ 7. МОДЕЛІ ТА МЕХАНІЗМИ ДОВІРИ	69
7.1. Концепція довіри в ІВК	69

7.2. Моделі довіри	70
7.3. Механізм крос-сертифікації	77
<i>Запитання та завдання для самоконтролю</i>	78
РОЗДІЛ 8. БАЗОВІ АРХІТЕКТУРИ ІВК. ПОБУДОВА	
ШЛЯХІВ СЕРТИФІКАЦІЇ	79
8.1. Загальні положення	79
8.2. Прості архітектури ІВК.....	81
8.3. Корпоративні архітектури ІВК.....	85
8.4. Гібридні архітектури ІВК.....	91
8.5. Архітектура національної ІВК	100
8.6. Структура ЦЗО та порядок взаємодії його складових частин	102
<i>Запитання та завдання для самоконтролю</i>	109
РОЗДІЛ 9. ВАЛІДАЦІЯ ШЛЯХІВ СЕРТИФІКАЦІЇ	111
9.1. Загальні вимоги до процедури валідації шляхів сертифікації	111
9.2. Валідація шляху сертифікації.....	113
<i>Запитання та завдання для самоконтролю</i>	118
ЧАСТИНА ІІІ. НОРМАТИВНЕ РЕГУЛЮВАННЯ ТА СТАНДАРТИЗАЦІЯ	
ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ	119
РОЗДІЛ 10. СТАНДАРТИЗАЦІЯ У ГАЛУЗІ ІВК	119
10.1. Органи зі стандартизації у галузі ІВК.....	119
10.2. Класифікація стандартів у галузі ІВК	120
10.3. Характеристика напрямів стандартизації в галузі ІВК.....	123
<i>Запитання та завдання для самоконтролю</i>	128
РОЗДІЛ 11. ГРУПИ ПРОТОКОЛІВ ІВК	129
11.1. Група операційних протоколів.....	129
11.2. Група протоколів управління	130
11.3. Група протоколів валідації	133
<i>Запитання та завдання для самоконтролю</i>	136
РОЗДІЛ 12. ПОЛІТИКА ТА РЕГЛАМЕНТ. НАБІР ПОЛОЖЕНЬ	
ПОЛІТИКИ СЕРТИФІКАЦІЇ	137
12.1. Політика застосування сертифікатів	137
12.2. Регламент УС.....	138
12.3. Застосування ідентифікаторів об'єктів у регламенті та ПЗС.....	139
12.4. Набір положень політики ІВК.....	141
<i>Запитання та завдання для самоконтролю</i>	146
Лабораторний практикум.....	147
Список використаної літератури	323