

ЗМІСТ

ВСТУП	3
Розділ 1. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС ТА ЙОГО ЗАСТОСУВАННЯ...	11
1.1. Основні поняття та визначення	12
1.2. Особливості надання послуг безпеки в електронному документообігу	15
1.3. Асиметричні криптографічні перетворення	16
1.3.1. Сутність асиметричних криптоперетворень у кільці цілих чисел	17
1.3.2. Сутність асиметричних криптоперетворень у полі Гауа.....	18
1.3.3. Сутність асиметричних криптоперетворень у групі точок еліптичних кривих	18
1.3.4. Перетворення зі спарюванням точок еліптичних кривих	19
1.4. Основні характеристики ЕЦП	21
1.4.1. Класифікація ЕЦП	21
1.4.2. Вимоги до ЕЦП	23
1.4.3. Досвід застосування та основні проблемні питання щодо електронного цифрового підпису	25
1.4.4. Основні види атак на ЕЦП	27
1.4.5. Основні види загроз ЕЦП	27
1.5. Кільцеві та групові підписи	28
1.5.1. Визначення, вимоги та сутність групових підписів	28
1.5.2. Класифікація кільцевих підписів	31
1.6. Проблемні питання та напрями розвитку ЕЦП	32
Розділ 2. СУТНІСТЬ ТА ОСНОВИ ЗАСТОСУВАННЯ ЕЦП	35
2.1. Загальна характеристика існуючих ЕЦП та геш-функцій	35
2.2. ЕЦП згідно з ISO 11166 та FIPS 186-3	37
2.3. ЕЦП, що визначені у FIPS 186-1, ГОСТ 34.310-95 та ГОСТ Р 34.10-2001	38
2.3.1. Загально-системні параметри	38
2.3.2. ЕЦП ГОСТ Р 34.10-94 та ЕЦП ГОСТ 34.310-95	39
2.3.3. ЕЦП ГОСТ 34.10-2001	40
2.4. ЕЦП згідно з ISO/IEC 14888-3 (15946-2)	42
2.4.1. Загальний опис схем ЕЦП згідно з ISO/IEC 14888-3 (15946-2)	43
2.4.2. ЕЦП згідно з ECDSA та його застосування	45
2.4.3. ЕЦП згідно з EC-GDSA та його застосування	46
2.4.4. ЕЦП згідно з KCDSA та його застосування	47
2.4.5. Порівняння властивостей ЕЦП EC-DNA, EC-GDSA та EC-KCDSA	49
2.5. Електронний цифровий підпис згідно з ДСТУ 4145-2002	51
2.5.1. Обчислення та використання загальних параметрів ЕЦП	52
2.5.2. Перевірка правильності загальних параметрів ЕЦП	54
2.5.3. Порядок обчислення ключів ЕЦП	55
2.5.4. Перевірка правильності ключів ЕЦП	56
2.5.5. Порядок обчислення цифрового передпідпису	57
2.5.6. Порядок обчислення ЕЦП	57
2.5.7. Порядок перевіряння ЕЦП	58
2.5.8. Порівняння складності виконання ЕЦП національних та міжнародних стандартів	60

Розділ 3. МЕТОДИ ОЦІНКИ ТА ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ЕЦП З ДОДАТКОМ У ГРУПІ ТОЧОК ЕК	62
3.1. Критерії та показники оцінки властивостей і якості криптографічних перетворень типу ЕЦП, що ґрунтуються на еліптичних кривих	63
3.1.1. Безумовні критерії оцінки криптографічних перетворень типу ЕЦП, що ґрунтуються на еліптичних кривих	63
3.1.2. Умовні критерії оцінки криптографічних перетворень типу ЕЦП з додатком, що ґрунтуються на еліптичних кривих	65
3.1.3. Показники оцінки якості криптоперетворень типу ЕЦП з додатком в групі точок ЕК	66
3.1.4. Показники та порядок оцінки ЕЦП з додатком у групі точок еліптичних кривих методом ієрархій	70
3.2. Оцінка криптографічної стійкості ЕЦП в групі точок ЕК від атак типу «Повне розкриття»	74
3.2.1. Огляд методів розв'язання дискретного логарифма в групах точок на еліптичних кривих	74
3.2.2. ρ -метод Полларда розв'язання дискретного логарифмічного рівняння в групі точок еліптичних кривих	76
3.2.3. Виведення й аналіз класичної формули визначення складності дискретного логарифмування в групах точок еліптичної кривої	79
3.2.4. Оцінка складності криптоаналізу на основі ρ -методу Полларда з урахуванням імовірності колізії	80
3.2.5. Оцінка складності криптоаналізу на основі λ -методу Полларда з урахуванням імовірності колізії	82
3.2.6. Порівняння складності криптоаналізу	84
3.2.7. «Повне розкриття» на основі підписаних даних	86
3.3. Оцінка стійкості ЕЦП від атак типу «екзистенційна підробка»	88
3.4. Оцінка стійкості ЕЦП від атак типу «Селективна підробка»	89
3.5. Аналіз захищеності існуючих ЕЦП від атак на зв'язаних ключах	89
3.5.1. Аналіз захищеності ЕЦП ECDSA та EC-KCDSA	90
3.5.2. Аналіз захищеності алгоритму ЕЦП ГОСТ Р 34.10-2001 від атаки на зв'язаних ключах	93
3.5.3. Аналіз захищеності алгоритму ЕЦП ДСТУ 4145-2002 від атаки на зв'язаних ключах	96
3.5.4. Загальні оцінки захищеності ЕЦП від атак на зв'язаних ключах	98
3.6. Аналіз захищеності існуючих ЕЦП від атак на програмну реалізацію	99
3.6.1. Захищеність ЕЦП ISO/IEC 15946-2 від атак на реалізацію	100
3.6.2. Захищеність ЕЦП ДСТУ 4145-2002 від атак на реалізацію	102
3.6.3. Захищеність ЕЦП ГОСТ Р 34.10-2001 від атак на реалізацію	103
3.7. Атаки на ЕЦП спеціального виду та захист від них	103
3.7.1. Атака на основі апаратних помилок	104
3.7.2. Атака на основі внесення помилок у строго визначений період обчислень	105
3.7.3. Атака на основі внесення помилок у довільний момент обчислень	105
3.8. Методика порівняльного аналізу стандартів ЕЦП за інтегральним критерієм	107
3.8.1. Спрощений опис методу ієрархій	107
3.8.2. Безумовні критерії оцінки ЕЦП	109
3.8.3. Умовні критерії оцінки ЕЦП	110

3.8.4. Порівняння алгоритмів ЕЦП	111
3.8.5. Аналіз отриманих результатів порівняння.....	116
3.9. Порівняння ЕЦП з використанням Методу визначення вагових коєфіцієнтів на основі функції втрати ефективності систем	116
3.9.1. Метод визначення вагових коєфіцієнтів	116
3.9.2. Методика порівняння ЕЦП.....	121

Розділ 4. АНАЛІЗ ВЛАСТИВОСТЕЙ ТА ОБЛАСТЕЙ ЗАСТОСУВАННЯ ЦИФРОВИХ ПІДПИСІВ ІЗ ВІДНОВЛЕННЯМ ПОВІДОМЛЕННЯ

4.1. Загальна модель ЕЦП з відновленням повідомлень	126
4.1.1. Процес обчислення параметрів.....	126
4.1.2. Процес обчислення підпису	127
4.1.3. Процес перевіряння підпису	127
4.1.4. Особливості ЕЦП з відновленням повідомлення.....	128
4.1.5. Перелік функцій і процедур.....	129
4.1.6. Генерування (обчислення) асиметричної ключової пари ЦП	129
4.1.7. Генерування (обчислення) ключа сеансу та попереднього ЦП	130
4.1.8. Обчислення першої і другої частин підпису.....	130
4.1.9. Відновлення попереднього підпису та вхідних даних.....	130
4.2. Обчислення цифрового підпису.....	130
4.2.1. Формування ключа сеансу та попереднього підпису	131
4.2.2. Розщеплення повідомлення.....	132
4.2.3. Формування вхідних даних та обчислення ЦП	132
4.2.4. Порядок обчислення цифрового підпису.....	132
4.3. Перевіряння цифрового підпису.....	133
4.3.1. Відкриття підписаного повідомлення.....	134
4.3.2. Перевіряння розміру підпису, відновлення попереднього підпису та вхідних даних	134
4.3.3. Повторне обчислення геш-значення та зіставлення підпису	134
4.3.4. Форматування підписаного повідомлення	135
4.3.5. Функції перетворення та генерації маски	135
4.4. Цифровий підпис Ніберга-Рюпеля у скінченному полі (Nyrberg–Rueppel message recovery signature).....	136
4.5. Цифровий підпис Ніберга-Рюпеля в групі точок еліптичних кривих (Elliptic Curve Nyrberg–Rueppel (ECNR) message recovery signature).....	137
4.5.1. Ключі цифрового підпису ECNR.....	137
4.5.2. Обчислення цифрового підпису	137
4.5.3. Перевіряння цифрового підпису	138
4.6. Цифровий підпис Міяджі з відновленням повідомлення в групі точок еліп- тичної кривої (Elliptic Curve Miyaji message recovery signature (ECMR))...	139
4.6.1. Доменні параметри та параметри користувача.....	139
4.6.2. Процес обчислення (генерації) підпису	139
4.6.3. Перевіряння підпису	140
4.7. Цифровий підпис Абі-Окамото з відновленням повідомлення в групі точок еліптичної кривої (Elliptic Curve Abe-Okamoto message recovery signature (ECAO))	141
4.7.1. Доменні параметри та параметри користувача.....	141

4.7.2. Обчислення цифрового підпису	141
4.7.3. Перевіряння підпису	142
4.8. Цифровий підпис Пінтсова-Ванстона в групі точок еліптичних кривих (Elliptic Curve Pintsov-Vanstone (ECPV) message recovery signature)	143
4.8.1. Доменні параметри та параметри користувача.....	143
4.8.2. Обчислення цифрового підпису	144
4.8.3. Перевіряння цифрового підпису.....	144
4.9. Цифровий підпис KCDSA у групі точок еліптичної кривої (Elliptic Curve KCDSA/Nurberg-Rueppel (ECKNR)message recovery signature)	145
4.9.1. Доменні параметри та параметри користувача.....	145
4.9.2. Обчислення цифрового підпису	146
4.9.3. Перевіряння цифрового підпису	146
4.10. Приклади використання ЕЦП з відновленням повідомлення	147
4.10.1. Поштові марки	147
4.10.2. Підписування дуже короткого повідомлення	147
4.10.3. Підписування та відновлення повідомлень із надлишком у 20 байтів..	148
4.11. Стійкість ЕЦП ECPV (Пінтсова-Ванстона).....	148
4.12. Стійкість ЕЦП з відновленням повідомлень до колізій	149
4.13. Стійкість до колізій відновлюваної частини повідомлення	150
4.14. Аналіз складності реалізації ЕЦП з відновленням повідомлення.....	152
4.15. Число гешувань MGF	154
Висновки та рекомендації.....	155

Розділ 5. ФУНКЦІ ГЕШУВАННЯ. СУТНІСТЬ ПЕРЕТВОРЕНЬ, ЗАСТОСУВАННЯ ТА НАПРЯМИ РОЗВИТКУ

5.1. Визначення та вимоги до функцій гешування	157
5.2. Атаки на функції гешування	160
5.3. Аналіз існуючих стандартів функцій гешування	163
5.3.1. Функції гешування, що засновані на блокових шифрах	163
5.3.2. Функції гешування, засновані на асиметричних перетвореннях	166
5.3.3. Функції гешування, що розроблені за замовленням	167
5.4. Опис і аналіз алгоритму SHA-1.....	172
5.5. Опис і аналіз алгоритмів SHA-2.....	175
5.6. Сутність і властивості функції гешування ГОСТ 34.311-95 (ГОСТ Р 34.11-94).....	179
5.6.1. Крокова функція гешування.....	180
5.6.2. Процедура обчислення геш-значення.....	181
5.7. Завдання та попередні підсумки проекту створення SHA-3.....	182
5.7.1. Основні умови організації та проведення конкурсу	183
5.7.2. Вимоги до перспективних кандидатів на стандарт гешування.....	184
5.7.3. Аналіз підходів щодо побудування перспективних функцій гешування	185
5.8. Сутність і результати 2 етапу конкурсу SHA-3.....	191
5.8.1. Аналіз вимог до функцій гешування	192
5.8.2. Критерії та показники оцінки функцій гешування.....	194
5.8.3. Методики порівняння функцій гешування за критерієм складності ..	196
5.8.4. Прийняття рішень при порівнянні функцій гешування	200

Розділ 6. КРИПТОГРАФІЧНІ ПРОТОКОЛИ АВТЕНТИФІКАЦІ ТА ВСТАНОВЛЕННЯ КЛЮЧІВ НА ОСНОВІ ЕЦП	202
6.1. Визначення та класифікація криптографічних протоколів	202
6.2. Основні концепції автентифікації на основі ЕЦП	207
6.2.1. Ідентифікація та автентифікація.....	207
6.2.2. Об'єкти автентифікації	207
6.2.3. Інформація автентифікації.....	208
6.2.4. Основні положення надання послуг автентифікації.....	208
6.2.5. Фази автентифікації. Сутність фаз автентифікації.....	212
6.3. Класифікація комітентів і механізми автентифікації	216
6.4. Види атак на автентифікацію.....	220
6.4.1. Атаки типу «Повтор»	220
6.4.2. Атаки типу «Підміна», коли ініціатором є порушник.....	221
6.4.3. Атака типу «Підміна», у якій порушник є відповідачем	222
6.5. Основні механізми автентифікації.....	223
6.5.1. Класифікація вразливостей	223
6.5.2 Класи механізмів автентифікації, коли пред'явник є ініціатором	223
6.5.2.1. Незахищений клас автентифікації 0	223
6.5.2.2. Клас автентифікації 1 – Захищений від розкриття заявленої ІА ...	224
6.5.2.3. Клас автентифікації 2 – Захищений від розкриття заявленої ІА та атаки типу «Повтор» на різних перевірників	225
6.5.2.4. Клас автентифікації 3 – Захищений від розкриття заявленої ІА та атаки типу «Повтор» на одного перевірника	225
6.5.2.5. Клас автентифікації 4 – Захищений від розкриття заявленої ІА та атаки типу «Повтор» на одного перевірника та різних перевірників	226
6.5.3. Класи механізмів автентифікації, де перевірник є ініціатором	229
6.5.4. Взаємна автентифікація.....	230
6.5.5. Загальна характеристика класів	231
6.6. Взаємодія з іншими послугами/ механізмами	232
6.6.1. Контроль доступу.....	232
6.6.2. Цілісність даних	232
6.6.3. Конфіденційність даних.....	232
6.6.4. Неспростовність.....	232
6.7. Загальна модель загроз	233
6.7.1. Спрощена модель загроз.....	233
6.7.2. Вступ у теорію автентичності Сімонсона	234
6.8. Методи автентифікації з використанням електронних засобів та ЕЦП ...	237
6.8.1. Методи автентифікації з використанням ЕЗ.....	237
6.8.2. Автентифікація з використанням ЕЗ та шифрування	238
6.8.3. Особливості автентифікації із застосуванням сертифікатів відкритих ключів.....	239
6.8.4. Особливості біометричних методів автентифікації	241
6.9. Основні характеристики та реальні класи щодо криптографічних протоколів автентифікації з ЕЦП	244
6.9.1. Основні характеристики криптографічних протоколів на основі ЕЦП	244
6.9.2. Аналіз класів механізмів і криптографічних протоколів автентифікації...244	
6.9.2.1. Практичні класи механізмів автентифікації	245

6.9.2.2. Особливості здійснення протоколів взаємної автентифікації	249
6.9.3. Загальна характеристика класів захищеності	250
6.10. Криптографічні протоколи автентифікації користувачів і робочих станцій на основі ЕЦП.....	251
6.10.1. Криптографічні протоколи автентифікації користувачів і робочих станцій згідно з ДСТУ ISO/IEC 9798-3	251
6.10.2. Криптографічні протоколи автентифікації користувачів і робочих станцій згідно з ДСТУ ISO/IEC 15946-3	255
6.10.2.1. Сутність і характеристики протоколу	255
6.10.2.2. Функція вироблення ключа зі спільної таємниці	257
6.10.2.3. Особливості використання та властивості кофакторного множення	258
6.10.2.4. Аналіз властивостей протоколу встановлення ключів типу іффі-Геллмана з двома електронними цифровими підписами та підтвердженням ключів	259
6.10.3. Криптографічні протоколи автентифікації користувачів і робочих станцій згідно ДСТУ ISO/IEC 11770-3	261
6.10.3.1. Сутність і характеристики протоколу	261
6.10.3.2. Функція вироблення ключа зі спільної таємниці	263
6.10.4. Порівняння та вибір криптографічних протоколів автентифікації PC і користувачів з електронним ключем та встановлення ключів.....	264
6.10.4.1. Оцінка механізму та криптографічного протоколу автентифікації PC і користувачів з електронним ключем та встановлення ключів на основі використання ДСТУ ISO/IEC 9798-3	264
6.10.4.2. Оцінка механізму та криптографічного протоколу автентифікації PC і користувачів з електронним ключем та встановлення ключів на основі використання ДСТУ ISO/IEC 15946-3	265
6.10.4.3. Оцінка механізму та криптографічного протоколу автентифікації PC і користувачів з електронним ключем та встановлення ключів на основі використання ДСТУ ISO/IEC 11770-3	267
6.10.5. Висновки та рекомендації щодо вибору криптографічного протоколу автентифікації PC і користувачів з електронним ключем та встановлення ключів	268
6.11. Криптографічні протоколи автентифікації робочих станцій і серверів застосувань із сервером безпеки на основі ЕЦП	269
6.11.1. Аналіз криптографічних механізмів взаємної автентифікації об'єктів і встановлення ключів між робочими станціями та серверами застосувань із сервером безпеки на основі ЕЦП	269
6.11.2. Аналіз криптографічних механізмів взаємної автентифікації об'єктів та встановлення ключів між робочими станціями та серверами застосувань із серверами безпеки згідно з ДСТУ ISO/IEC 15946-3	272
6.11.2.1. Сутність протоколу узгодження ключів типу Діффі-Геллмана ..	272
6.11.2.2. Механізм автентифікації.....	273
6.11.2.3. Аналіз протоколу узгодження ключів типу Діффі-Геллмана з двома ключовими парами	273
6.11.3. Аналіз криптографічних механізмів взаємної автентифікації об'єктів і встановлення ключів між робочими станціями та серверами застосувань із серверами безпеки згідно з ДСТУ ISO/IEC 11770-3	275

6.11.3.1. Сутність протоколу автентифікації та встановлення ключів 3...	275
6.11.3.2. Властивості протоколу автентифікації та встановлення ключів 3	276
6.11.3.3. Особливості застосування протоколу 3.....	277
6.11.4. Порівняння та вибір криптографічних механізмів взаємної автентифікації об'єктів і встановлення ключів між робочими станціями та сервером застосувань і сервером безпеки	277
6.11.4.1. Паралельний двопрхідний механізм згідно із стандартом ДСТУ ISO/IEC 9798-3	277
6.11.4.2. Протокол узгодження ключів та автентифікації типу Діффі-Геллмана (протокол 5.5) згідно з ДСТУ ISO/IEC 15946-3.....	278
6.11.4.3. Протокол автентифікації та встановлення ключів 3 із ДСТУ ISO/IEC 11770-3.....	280
6.12. Криптографічні протоколи автентифікації робочих станцій та встановлення ключів між серверами безпеки різних ЛОМ на основі ЕЦП	281
6.12.1. Аналіз і вибір криптографічних механізмів взаємної автентифікації об'єктів і встановлення ключів між серверами безпеки різних ЛОМ згідно з ДСТУ ISO/IEC 9798-3	281
6.12.2. Аналіз та вибір криптографічних механізмів взаємної автентифікації об'єктів і встановлення ключів між серверами безпеки різних ЛОМ згідно з ДСТУ ISO/IEC 11770-3.....	284
6.12.2.1. Сутність та аналіз протоколу 5 [21, 22] узгодження ключів та автентифікації	285
6.12.3. Розробка вдосконаленого криптографічного протоколу взаємної автентифікації об'єктів і встановлення ключів між серверами безпеки різних ЛОМ	287
6.12.3.1. Сутність та аналіз перспективного удосконаленого протоколу автентифікації й узгодження ключів	287
6.13. Узагальнені висновки та рекомендації щодо криптографічних протоколів з ЕЦП.....	292

Розділ 7. СТАН СТВОРЕННЯ ТА ЗАСТОСУВАННЯ ІНФРАСТРУКТУР З ВІДКРИТИМИ КЛЮЧАМИ	297
7.1. Поняття сертифіката відкритого ключа.....	297
7.2. Загальна характеристика стандарту ДСТУ ITU-T Rec. X.509 ISO/IEC 9594-8	299
7.3. Формат сертифіката версії 3(v3) стандарту ДСТУ ITU-T Rec. X.509 ISO/IEC 9594-8	303
7.3.1. Формат сертифіката відкритого ключа	303
7.3.2. Список скасування сертифікатів та його розширення	308
7.4. Особливості структури сертифікатів ІВК США та Європейського Союзу ...	312
7.5. Сертифікати відкритих ключів атрибутів	317
7.6. Інфраструктура управління повноваженнями	322
7.6.1. Загальна модель управління повноваженнями	323
7.6.2. Застосування інфраструктур управління повноваженнями	324
7.6.3. Модель ролей утримувачів	326
7.6.4. Основні способи надання повноваження у сертифікатах атрибутів ...	327

7.6.5. Особливості повноважень, що задаються в сертифікатах відкритого ключа	328
Висновки та рекомендації	329
Розділ 8. ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ ТА СЕРТИФІКАЦІЇ АТРИБУТІВ РОЗВИНЕНИХ ДЕРЖАВ.....	
8.1. Стан створення, структура та застосування ІВК в США.....	330
8.1.1. Історична довідка, стан і загальні проблемні питання впровадження ІВК в США	330
8.1.2. Архітектура федеральної ІВК США	333
8.1.3. Федеральний профіль сертифіката США	334
8.1.4. Федеральний профіль списку скасованих сертифікатів.....	336
8.1.5. Основні напрями підвищення інтероперабельності компонентів ІВК ...	337
8.2. Стан застосування та розвитку ІВК в Канаді.....	338
8.2.1. Загальні підходи до створення ІВК	338
8.2.2. Архітектура ІВК Уряду Канади.....	339
8.2.3. Особливості побудови ІВК УК	340
8.2.4. Перелік стандартів, алгоритмів і протоколів, що підтримуються ІВК УК	341
8.3. Стан застосування та розвитку ІВК у Європейському союзі	343
8.3.1. Аналіз вимог європейського законодавства щодо ЕЦП.....	343
8.3.2. Стандартизація ЄС в галузі ІВК.....	345
8.4. Стан створення та застосування ІВК в Російській Федерації	351
8.5. Особливості застосування ІВК в Австралії	357
Висновки та проблемні питання.....	358
Розділ 9. СИСТЕМА ЕЦП УКРАЇНИ ТА ЇЇ ЗАСТОСУВАННЯ.....	
9.1. Нормативно-правова база створення та застосування системи ЕЦП в Україні	360
9.2. Вимоги до системи ЕЦП України.....	362
9.2.1. Загальні вимоги до системи ЕЦП України	362
9.2.2. Вимоги до системи ЕЦП України.....	363
9.3. Інформаційна структура системи ЕЦП України.....	371
9.4. Вимоги до структури та призначення комплексу технічних засобів центру ...	378
9.5. Вимоги до програмно-технічного комплексу	382
9.5. Акредитований центр сертифікації ключів	387
9.5.1. Технічна структура програмно-технічного комплексу	387
9.5.2. Режими функціонування та експлуатації програмно-технічного комплексу	389
9.5.3. Склад і функціональні обов'язки персоналу, що відповідає за експлуатацію програмно-технічного комплексу	390
9.5.4. Управління АЦСК.....	390
9.5.5. Регламент АЦСК.....	391
9.5.6. Умови, процедури, механізми надання послуг абонентам	393
9.6. Комплексна система захисту інформації центру	399
9.6.1. Призначення комплексної системи захисту інформації Центру	399
9.6.2. Організаційна структура Центру	400
9.7. Робота із сертифікатами та списками сертифікатів	402

9.7.1. Зчитування сертифікатів і списків відкритих сертифікатів (СВС).....	404
9.7.2. Перегляд сертифікатів	404
9.7.3. Перегляд СВС	405
9.7.4. Завантаження СВС	405
9.7.5. Блокування власного сертифіката	405
9.8 Робота з особистим ключем	406
9.8.1. Зчитування особистого ключа	406
9.8.2. Генерація особистого ключа.....	406
9.8.3. Резервне копіювання особистого ключа.....	407
9.8.4. Зміна пароллю захисту особистого ключа	407
9.8.5. Знищення особистого ключа на носії	408
9.8.6. Знищення особистого ключа в пам'яті ПЕОМ	408
9.9. Робота з файлами	408
9.9.1 Підпис файлів	408
9.9.2. Перевірка підпису.....	409
9.9.3. Шифрування файлів	409
9.9.4. Розшифрування файлів.....	410
9.10. Інші завдання	410
9.10.1. Встановлення параметрів	410
9.10.2. Режим роботи з ЦСК.....	413
9.11. Стан застосування та проблемні питання розвитку системи ЕЦП	413

**Розділ 10. ВИМОГИ ДО ЗАСОБІВ КЗІ ТА УПРАВЛІННЯ КЛЮЧАМИ
В ПЕРСПЕКТИВНИХ ІВК.....**

10.1. Рівні гарантій Федерального мосту США	420
10.2. Аналіз та обґрунтування вимог до засобів криптографічного захисту інформації в ІВК та принципи їх забезпечення.....	422
10.3. Розроблення та дослідження властивостей апаратних засобів генерування ключів і випадкових послідовностей для ІВК.....	429
10.4. Аналіз та обґрунтування вимог до систем управління та сертифікації ключів в ІВК та принципи їх забезпечення.....	435
10.5. Аналіз та обґрунтування вимог щодо вибору криптографічних алгоритмів і розмірів ключів.....	447

**Розділ 11. ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ТА ЗАСТОСУВАННЯ
ЗАСОБІВ КЗІ В НАЦІОНАЛЬНІЙ СИСТЕМІ ІВК (ЕЦП).....**

11.1. Апаратний засіб типу електронний ключ «Кристал-1»	453
11.2. Апаратний генератор випадкових чисел (АГВЧ)	460
11.3. Апаратний модуль цифрового підпису «Гряда-41П»	462
11.4. Апаратно-програмний криптографічний засіб «Гряда-61».....	471
11.5. Мережевий криптомодуль «Гряда-301»	474

**Розділ 12. ОСНОВНІ ПОЛОЖЕННЯ РЕАЛІЗАЦІЇ ПЕРСПЕКТИВНОЇ
ПОЛІТИКИ СЕРТИФІКАЦІЇ X-509.....**

12.1. Загальні положення.....	481
12.1.1. Початкові положення	481
12.1.2. Рівні гарантій	483
12.1.3. Учасники ІВК	484

12.1.4. Характеристика об'єктів ІВК	484
12.1.5. Використання сертифікатів	485
12.1.6. Сутність основних рівнів гарантій використання сертифікатів	487
12.1.7. Репозиторії та публікації.....	489
12.2. Ідентифікація та автентифікація в ІВК.....	490
12.2.1. Іменування в СА.....	490
12.2.2. Порядок початкового посвідчення особи	491
12.2.3. Ідентифікація й автентифікація для перекодування запитів.....	495
12.3. Вимоги до періоду дії сертифіката.....	496
12.3.1. Порядок подання заяви на сертифікат	496
12.3.2. Процес подачі заяви на сертифікат.....	498
12.3.3. Випуск сертифіката	498
12.3.4. Прийняття сертифіката.....	498
12.3.5. Ключова пара та використання сертифіката	498
12.3.6. Відкритий ключ і використання сертифіката	499
12.3.7. Відновлення сертифіката.....	499
12.3.8. Перекодування сертифіката	499
12.3.9. Модифікування сертифіката	500
12.3.10. Скасування та припинення дії сертифіката.....	500
12.3.11. Депонування та відновлення ключів.....	503
12.4. Генерація та інсталяція ключових пар.....	504
12.4.1. Генерація ключових пар.....	504
12.4.2. Постачання особистих ключів абонентам	505
12.4.3. Постачання відкритих ключів до емітента сертифікатів	505
12.4.4. Постачання відкритих ключів залежним сторонам.....	506
12.4.5. Розміри ключів	506
12.4.6. Генерація загальних параметрів та перевірка якості ключів	507
12.4.7. Області використання ключів (цілі використання ключів).....	507
12.5. Захист особистих ключів і особливості проектування криптографічних модулів.....	508
12.5.1. Стандарти й засоби управління криптографічними модулями.....	508
12.5.2. Багатостороннє управління особистим ключем	509
12.5.3. Депонування особистих ключів	509
12.5.4. Резервування особистих ключів	509
12.5.5. Запис або зчитування особистих ключів з криптографічного модуля	510
12.5.6. Зберігання особистого ключа в криптографічному модулі	511
12.5.7. Метод активації особистого ключа	511
12.5.8. Метод дезактивації особистого ключа	511
12.5.9. Метод знищення особистого ключа	511
12.5.10. Інші аспекти управління ключовими парами.....	511
12.6. Дані активації	512
12.6.1. Генерування та інсталяція даних активації	512
12.6.2. Захист даних активації	512
12.7. Засоби управління комп'ютерним захистом	513
12.7.1. Устаткування СА і OSCP користувача.....	513
12.7.2. Технічні засоби управління життєвим циклом.....	513
12.8. Профіль захисту.....	514

12.8.1. Номер версії	514
12.8.2. Розширення сертифіката	515
12.8.3. Алгоритмічні об'єктні ідентифікатори	515
12.8.4. Форми імен	517
12.8.5. Обмеження імен	517
12.8.6. Об'єктний ідентифікатор політики сертифікації	517
12.8.7. CRL профіль	517
12.8.8. OCSP профіль	518
12.9. Устаткування та засоби управління експлуатацією	518
12.9.1. Фізичні засоби управління.....	518
12.9.2. Процедурні засоби управління	520
12.9.3. Персональні засоби управління	522
12.9.4. Процедури ведення контрольного журналу	524
12.9.5. Архівація записів.....	526
12.9.6. Заміна ключів	527
12.9.7. Компрометація та відновлення після лиха	528

**Розділ 13. РОБЛЕМНІ ПИТАННЯ ТА НАПРЯМИ РОЗВИТКУ
ІНФРАСТРУКТУР З ВІДКРИТИМИ КЛЮЧАМИ**

13.1. Основні теоретичні та практичні проблемні питання	530
13.2. Існуючі та перспективні методи криптоперетворень для ЕЦП	533
13.3. Криптоперетворення в гіпереліптичних кривих.....	534
13.4. Особливості застосування гіпереліптичних кривих для ЕЦП	537
13.4.1. Введення в асиметричну криптографію на ідентифікаторах.....	539
13.5. Метод шифрування на базі ідентифікаторів.....	540
13.6. Цифровий підпис на базі ідентифікаторів	542
13.7. Метод ЕЦП із використанням ідентифікаційних даних на основі стандарту ДСТУ 4145-2002	544
13.8. Безпечний протокол розділення таємниці на ідентифікаторах.....	549
13.9. Тристоронній протокол узгодження ключів Діффі-Геллмана на ідентифікаторах	551
13.10. Стан стандартизації ІВК, що ґрунтуються на використанні ідентифікаторів	551

**Додаток А. ОСНОВНІ ПОЛОЖЕННЯ ТА МАТЕМАТИЧНІ МЕТОДИ
КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ У ГРУПІ ТОЧОК
ЕЛІПТИЧНИХ КРИВИХ.....**

Вступ	554
Терміни і визначення	554
Позначення	555
A.1. Поля Галуа.....	556
A.1.1. Прості кінцеві поля $F(p)$	556
A.1.2. Кінцеві поля $F(p^m)$	556
A.1.3. Квадрати і неквадрати в полі $F(q)$	557
A.2. Еліптичні криві.....	557
A.2.1. Визначення еліптичних кривих.....	557
A.2.1.1. Еліптичні криві над $F(p^m)$	557
A.2.1.2. Еліптичні криві над полем $F(2^m)$	557

A.2.1.3. Еліптичні криві над $F(3^m)$	557
A.3. Груповий закон для еліптичних кривих E над $F(q)$ з $p > 3$	558
A.3.1. Огляд систем координат	558
A.3.2. Груповий закон в афінних координатах	558
A.3.3. Груповий закон у проєктивних координатах	559
A.3.4. Груповий закон у проєктивних координатах Якобі	560
A.3.5. Груповий закон у модифікованих координатах Якобі	560
A.3.6. Змішані координати	561
A.4. Криптографічне білінійне відображення.....	561
A.4.1. Існування спарювання	561
A.4.2. Визначення спарувань Вейла і Тейта	562
A.4.3. Криптографічне білінійне відображення.....	562
A.5. Функції перетворення.....	562
A.5.1. Перетворення рядків октетів на бітові рядки OS2BSP і навпаки BS2OSP	562
A.5.2. Перетворення бітових рядків на цілі числа BS2IP і навпаки I2BSP ...	563
A.5.3. Перетворення рядків октетів на цілі числа OS2IP і навпаки I2OSP ...	563
A.5.4. Перетворення елементів кінцевого поля на цілі числа FE2IP _F	563
A.5.5. Перетворення рядків октетів на елементи кінцевого поля: OS2FE _{FP} , і навпаки FE2OS _{FP}	563
A.5.6. Перетворення точок еліптичної кривої на октетові рядки: EC2OSPE, і навпаки OS2ECPE.....	564
A.6. Параметри області еліптичної кривої та відкритий ключ.....	566
A.6.1. Параметри області еліптичної кривої над $F(q)$	566
A.6.2. Генерація ключів еліптичної кривої	566
A.7. Основна інформація щодо еліптичних кривих	566
A.7.1. Властивості еліптичних кривих.....	566
A.7.2. Аномальні та суперсингулярні криві	567
A.7.3. Груповий закон для еліптичних кривих над полем $F(2^m)$	567
A.7.3.1. Груповий закон в афінних координатах	567
A.7.3.2. Груповий закон у проєктивних координатах над полем $F(2^m)$	568
A.7.4. Груповий закон для еліптичних кривих над полем $F(3^m)$	568
A.7.4.1. Груповий закон в афінних координатах	568
A.7.4.2. Груповий закон у проєктивних координатах	569
A.7.5. Умови існування еліптичної кривої.....	570
A.7.5.1. Порядок еліптичної кривої, що визначена над полем $F(P)$	570
A.7.5.2. Порядок еліптичної кривої, що визначена над полем $F(P^m)$	570
A.7.5.3. Порядок еліптичної кривої, що визначена над полем $F(3^m)$	570
A.8. Базова інформація щодо криптосистем, що ґрунтуються на еліптичних кривих	571
A.8.1. Основні задачі при атаках на особисті ключі.....	571
A.8.1.1. Задача дискретного логарифмування в групі точок еліптичної кривої (ECDLP).....	571
A.8.1.2. Обчислювальна задача Діффі-Геллмана в групі точок еліптичної кривої (ECDHP)	571
A.8.1.3. Вирішувальна задача Діффі-Геллмана в групі точок еліптичної кривої (ECDDHP)	571

A.8.1.4. Білінійна задача Діффі-Геллмана (BDH)	572
A.8.2. Алгоритми визначення дискретних логарифмів у групі точок еліптичної кривої	572
A.8.2.1. Складність дискретного логарифмування в групі точок еліптичної кривої (ECDLP)	572
A.8.2.2. Методи дискретного логарифмування в групі точок еліптичної кривої	572
A.8.2.3. MOV умова	573
A.8.3. Алгоритми скалярного множення точок еліптичної кривої	573
A.8.3.1. Базові алгоритми скалярного множення	573
A.8.3.2. Алгоритм скалярного множення з попередньо обчисленою таблицею	574
A.8.4. Алгоритми обчислення спарювань точок ЕК	574
A.8.4.1. Допоміжні функції обчислень	574
A.8.4.2. Алгоритм обчислення спарювання Вейла	575
A.8.4.3. Алгоритм обчислення спарювання Тейта	576
A.8.5. Перевірка достовірності загальних параметрів еліптичної кривої та відкритого ключа	576
A.8.5.1. Перевірка достовірності загальних параметрів ЕК над полем $F(q)$	576
A.8.5.2. Перевірка достовірності відкритого ключа	577
A.9. Складність обчислень у різних системах координат	577
ПЕРЕЛІК ДЖЕРЕЛ	579

Автори вдячні робочій групі видавництва «Форт», яка взяла участь у виданні книги. Зокрема Едуарду Миколайовичу Олійнику за інтерес, що був виявлений до цієї книги, й активне співробітництво; Кліменко Світлані Олександрівні, яка читала й редагувала рукопис; Фокіній Людмилі Іванівні, яка правила верстаний матеріал і готувала рукопис до друку. Ми щиро вдячні їм за критичні зауваження та пропозиції, окремо за увагу й терпіння. Якщо, незважаючи на наші зусилля, похибки чи помилки в тексті все ж таки залишилися, то відповідальність за них автори залишають за собою.

Науково-методичне видання

*Горбенко Юрій Іванович,
Горбенко Іван Дмитрович*

**ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ.
ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС.
ТЕОРІЯ ТА ПРАКТИКА**

Монографія

*Відповідальний за випуск В. П. Ровенець
Комп'ютерна верстка Л. І. Фокіної
Коректор С. О. Кліменко*

Підписано до друку 23.09.2010 р.

Формат 70×100/16. Папір офсет. Друк ксерографічний.

Умов. друк. арк. 49,4. Обл.-вид. арк. 30,4. Тираж 300 прим. Зам. №

ТОВ «Видавництво «Форт»

**Свідоцтво про внесення до Державного реєстру видавців
ДК № 333 від 09.02.2001 р.**

61023, м. Харків, а/с 10325. Тел. (057) 714-09-08