

## ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ .....	VII
ГЛОСАРІЙ ТЕРМІНІВ ТА ПОНЯТЬ .....	IX
ВСТУП .....	1
РОЗДІЛ 1. ПОХОДЖЕННЯ ТА ТЕОРЕТИЧНІ ЗАСАДИ КЛЕПТОГРАФІЇ .....	3
1.1. ВИЗНАЧЕННЯ КЛЕПТОГРАФІЇ .....	3
1.2. ІСТОРІЯ ТЕРМІНУ ТА ПЕРШІ ДОСЛІДЖЕННЯ .....	7
1.3. МЕЖІ МІЖ КЛЕПТОГРАФІЄЮ, КРИПТОГРАФІЄЮ І СТЕГАНОГРАФІЄЮ .....	10
1.3.1. Криптоаналіз vs Клептографія .....	10
1.3.2. Стеганографія vs Клептографія .....	11
1.4. КЛЕПТОГРАФІЯ ЯК ІНТЕЛЕКТУАЛЬНЕ ДЖЕРЕЛО СУЧАСНИХ ПАРАДИГМ КІБЕРБЕЗПЕКИ .....	13
1.4.1. Supply Chain Security — безпека ланцюга постачання .....	14
1.4.2. Trusted Hardware Auditing — аудит “довіреного” обладнання .....	14
1.4.3. Zero Trust by Design — недовіра за замовчуванням .....	15
1.4.4. Прозорість компіляторів (Transparency of Compilers) .....	16
1.4.5. Формальні моделі зрадливого розробника (malicious developer / compiler) .....	16
1.5. КЛЕПТОГРАФІЯ ЯК НАУКА ПРО ДОВІРУ, КОНТРОЛЬ І ЗРАДУ .....	17
1.5.1. Контроль як структурна вбудованість .....	18
1.5.2. Зрада як методологічна категорія .....	18
1.5.3. Клептографія як мегадисципліна .....	18
1.5.4. Пояснювальна сила клептографії .....	19
1.6. КЛЕПТОГРАФІЯ ЯК СИНТЕЗ ТЕХНІЧНОЇ РОЗВІДКИ ТА АРХІТЕКТУРНОГО КОНТРОЛЮ .....	20
1.6.1. Генетика клептографії у технічній розвідці .....	21
1.6.2. Архітектура втручання: Crypto AG, Siemens, Mils Electronics .....	24
1.6.3. Архітектурна клептографія як стратегія системного впливу .....	28
Висновки .....	30
РОЗДІЛ 2. ТИПОЛОГІЯ ТА КЛАСИФІКАЦІЯ КЛЕПТОГРАФІЧНИХ ЗАГРОЗ .....	34
2.1. КЛАСИФІКАЦІЯ КЛЕПТОГРАФІЧНИХ ЗАГРОЗ ЗА РІВНЕМ РЕАЛІЗАЦІЇ .....	35
2.1.1. Алгоритмічний рівень .....	36
2.1.2. Програмний рівень .....	36
2.1.3. Апаратний рівень .....	37
2.1.4. Протокольний рівень .....	37
2.1.5. Системний рівень .....	38
2.1.6. Нормативно-інституційний рівень .....	38
2.2. КЛАСИФІКАЦІЯ КЛЕПТОГРАФІЧНИХ ЗАГРОЗ ЗА СПОСОБОМ ВИТОКУ ІНФОРМАЦІЇ .....	40
2.2.1. Активні загрози .....	41
2.2.2. Пасивні загрози .....	42
2.2.3. Умовні загрози .....	43
2.2.4. Відкладені загрози .....	45
2.3. КЛАСИФІКАЦІЯ КЛЕПТОГРАФІЧНИХ ЗАГРОЗ ЗА ТИПОМ АКТИВАЦІЇ .....	47
2.3.1. Автоматична активація (“by default”) .....	49
2.3.2. Умовна активація (“triggered on condition”) .....	49
2.3.3. Відкладена активація (“time-delayed / event-based”) .....	50
2.3.4. Віддалена активація (керована ззовні) .....	50
2.3.5. Комбіновані та ієрархічні схеми .....	51
2.4. КЛАСИФІКАЦІЯ КЛЕПТОГРАФІЧНИХ ЗАГРОЗ ЗА ІНСТИТУЦІЙНИМ ПОХОДЖЕННЯМ .....	53
2.4.1. Державна клептографія (національно-стратегічна) .....	54
2.4.2. Корпоративна клептографія (“white-label”/ комерційна) .....	54
2.4.3. Інсайдерська клептографія (від зрадника-розробника) .....	55
2.4.4. Делегована клептографія (через підрядника) .....	56
2.4.5. Ситуативна (хаотична) клептографія .....	56
2.5. СЕМАНТИЧНА КЛАСИФІКАЦІЯ КЛЕПТОГРАФІЧНИХ ЗАГРОЗ .....	58
2.5.1. Експортна клептографія (export-grade kleptography) .....	59

2.5.2. Інсайдерська клептографія ( <i>insider-grade kleptography</i> ) .....	59
2.5.3. Інституційна клептографія ( <i>institutional-grade kleptography</i> ) .....	60
2.5.4. Інфраструктурна клептографія ( <i>critical-path kleptography</i> ) .....	60
2.5.5. Символічна / демонстративна клептографія ( <i>symbolic kleptography</i> ) .....	61
Висновки.....	63
<b>РОЗДІЛ 3. ЖИТТЄВИЙ ЦИКЛ КЛЕПТОГРАФІЧНОГО БЕКДОРУ .....</b>	<b>66</b>
3.1. ЕТАПИ ЖИТТЄВОГО ЦИКЛУ КЛЕПТОГРАФІЧНОГО БЕКДОРУ .....	66
3.1.1. Проектування ( <i>Design Phase</i> ).....	67
3.1.2. Інтеграція та реалізація ( <i>Implementation Phase</i> ).....	67
3.1.3. Розповсюдження ( <i>Distribution Phase</i> ).....	68
3.1.4. Активація ( <i>Activation Phase</i> ).....	68
3.1.5. Експлуатація та виведення ( <i>Exfiltration &amp; Exit Phase</i> ).....	68
3.2. МЕТОДИ МАСКУВАННЯ КЛЕПТОГРАФІЧНИХ БЕКДОРІВ .....	72
3.2.1. Архітектурне маскування .....	72
3.2.2. Програмно-криптографічне маскування .....	73
3.2.3. Операційне маскування.....	73
3.3. МЕТОДИ ВИЯВЛЕННЯ БЕКДОРУ НА КОЖНОМУ ЕТАПІ ЖИТТЄВОГО ЦИКЛУ .....	75
3.3.1. Етап проектування ( <i>Design Phase</i> ).....	76
3.3.2. Етап реалізації ( <i>Implementation Phase</i> ) .....	77
3.3.3. Етап розповсюдження ( <i>Distribution Phase</i> ) .....	77
3.3.4. Етап активації ( <i>Activation Phase</i> ).....	77
3.3.5. Етап експлуатації ( <i>Exfiltration &amp; Exit Phase</i> ) .....	78
3.4. Точки втручання для виявлення, блокування або нейтралізації КЛЕПТОГРАФІЧНОГО БЕКДОРУ .....	78
Висновки.....	81
<b>РОЗДІЛ 4. АНАЛІЗ ІСТОРИЧНИХ І СУЧАСНИХ КЕЙСІВ КЛЕПТОГРАФІЇ .....</b>	<b>83</b>
4.1. Кейс 1: CRYPTO AG — МІЖНАРОДНЕ ШПИГУНСТВО ПІД ВИГЛЯДОМ КОМЕРЦІЙНОГО ШИФРУВАННЯ .....	85
4.2. Кейс 2: SNOWDEN REVELATIONS — ДОКТРИНА ІНСТИТУЦІЙНОЇ КЛЕПТОГРАФІЇ .....	87
4.3. Кейс 3: DUAL_EC_DRBG — АЛГОРИТМІЧНИЙ БЕКДОР У СТАНДАРТИЗОВАНОМУ ГЕНЕРАТОРІ ВИПАДКОВИХ ЧИСЕЛ .....	89
4.4. Кейс 4: RSA SECURITY — \$10 МЛІЙОНІВ ЗА ІНТЕГРАЦІЮ БЕКДОРУ .....	90
4.5. Кейс 5: JUNIPER NETSCREEN — ПОДВІЙНИЙ БЕКДОР У VPN-ІНФРАСТРУКТУРІ КОРПОРАТИВНОГО РІВНЯ.....	91
4.6. Кейс 6: ENCROCHAT І SKY ECC — КОНТРОЛЬОВАНІ ПРИСТРОЇ З “ВШИТИМ” БЕКДОРОМ .....	94
4.7. Кейс 7: КИТАЙСЬКІ ІР-КАМЕРИ З БЕКДОРАМИ ДЛЯ ЗОВНІШНЬОГО КЕРУВАННЯ .....	95
4.8. СИСТЕМАТИЗАЦІЯ ІНШИХ КЕЙСІВ КЛЕПТОГРАФІЇ .....	97
4.9. ПОРІВНЯЛЬНА ГЕОСТРАТЕГІЯ КЛЕПТОГРАФІЇ: США, КИТАЙ, РОСІЯ .....	99
Висновки.....	101
<b>РОЗДІЛ 5. МЕТОДИ ВИЯВЛЕННЯ І ПРОТИДІЇ .....</b>	<b>104</b>
5.1. ФОРМАЛЬНІ МЕТОДИ ВИЯВЛЕННЯ КРИПТОГРАФІЧНИХ АНОМАЛІЙ .....	105
5.2. ПОВЕДІНКОВИЙ АНАЛІЗ, ФУЗЗИНГ, ТРАСУВАННЯ І ПОБІЧНІ КАНАЛИ ЯК ІНСТРУМЕНТИ ВИЯВЛЕННЯ .....	111
5.2.1. Поведінковий аналіз.....	111
5.2.2. Фуззинг .....	113
5.2.3. Динамічне трасування ( <i>dynamic tracing</i> ) .....	115
5.2.4. Інверсійне або зворотне тестування ( <i>inversion testing</i> ).....	116
5.2.5. Побічні канали ( <i>англ. side-channels</i> ).....	117
5.3. АНАЛІЗ ШАБЛОНІВ І СТАТИСТИЧНЕ ПРОФІЛЮВАННЯ ЯК ЗАСОБИ НЕПРЯМОГО ВИЯВЛЕННЯ.....	119
5.4. МОДЕЛЬ «ПІДОЗРІЛОГО ТРИКУТНИКА».....	124
Висновки.....	127
<b>РОЗДІЛ 6. КЛЕПТОГРАФІЯ ЯК ПАРАДІГМА ПРОФІЛАКТИКИ.....</b>	<b>129</b>

6.1. ПРИНЦИПИ ПРОЗОРОСТІ, ВІДПОВІДАЛЬНОСТІ ТА ТРАСОВАНOSTІ.....	131
6.1.1. Прозорість як інженерна і етична вимога.....	131
6.1.2. Відповідальність: розподілений обов'язок та фактор довіри.....	132
6.1.3. Трасованість: гарантія цифрової спадковості.....	134
6.1.4. Функціоналізація принципів у сучасних практиках безпеки.....	134
6.2. PEER-REVIEW, РЕВІЗІЯ ЗАЛЕЖНОСТЕЙ ТА ПРАВО НА АУДИТ.....	136
6.2.1. Peer-review як гарантія колективної довіри.....	136
6.2.2. Ревізія залежностей: запобігання транзитивним загрозам.....	137
6.2.3. Право на аудит — як цифрове громадянське право.....	138
6.3. РІВНІ ВПРОВАДЖЕННЯ КЛЕПТОГІГІЄНИ.....	139
6.3.1. Технічний рівень: проектування, реалізація, верифікація.....	139
6.3.2. Організаційний рівень: політики, процеси, компетенції.....	140
Висновки.....	142
<b>РОЗДІЛ 7. ВПРОВАДЖЕННЯ КЛЕПТОГІГІЄНИ В КРИТИЧНИХ СЕКТОРАХ.....</b>	<b>145</b>
7.1. ТЕЛЕКОМУНІКАЦІЇ: МІЖ ДОСТУПОМ І КОНТРОЛЕМ.....	145
7.2. ЕНЕРГЕТИКА: ІНФРАСТРУКТУРА, ШО НЕ МАЄ ПРАВА НА ПОМИЛКУ.....	148
7.3. БАНКІВСЬКИЙ СЕКТОР: КРИПТОГРАФІЯ ДОВІРИ ЧИ РИЗИКУ?.....	151
7.3.1. HSM: апаратна довіра з архітектурними ризиками.....	151
7.3.2. SDK у мобільних додатках: прихований ризик на клієнтському рівні.....	151
7.3.3. Проблеми у сфері PKI та сертифікатів.....	152
7.3.4. Клептогігієнічні практики в банківському секторі.....	152
7.4. КРИПТОІНФРАСТРУКТУРА ТА СЕРТИФІКАЦІЙНІ ЦЕНТРИ.....	153
7.4.1. Компрометація Root CA як стратегічна загроза.....	154
7.4.2. Інституційний ризик у сертифікаційній інфраструктурі.....	154
7.4.3. Архітектурні ризики бібліотек та підпису.....	155
7.4.4. Клептогігієна криптоінфраструктури.....	155
7.5. ПОЛІТИКИ ЦИФРОВОЇ ДОВІРИ В ЄС, США, КИТАЇ.....	156
7.5.1. Європейський Союз: стратегічна автономія та відкритість.....	156
7.5.2. США: централізована модель керованої довіри.....	157
7.5.3. Китай: криптографічний ізоляціонізм і внутрішній контроль.....	157
7.6. РЕКОМЕНДАЦІЇ ДЛЯ РОЗРОБНИКІВ І РЕГУЛЯТОРІВ.....	158
7.6.1. Рекомендації для розробників.....	159
7.6.2. Рекомендації для регуляторів і політики виробників.....	160
Висновки.....	161
<b>РОЗДІЛ 8. ПОЛІТИЧНІ ТА ЕТИЧНІ ВИМІРИ ЦИФРОВОГО СУВЕРЕНІТЕТУ.....</b>	<b>163</b>
8.1. ГЕОПОЛІТИКА ЦИФРОВИХ БЕКДОРІВ.....	163
8.2. ЦИФРОВА АВТОНОМІЯ ТА МОДЕЛЬ ZERO TRUST.....	165
8.3. ЕТИКА РОЗРОБНИКА І ПОСТАЧАЛЬНИКА.....	168
8.4. НАЦІОНАЛЬНА КІБЕРГРАМОТНІСТЬ: ІНТЕЛЕКТУАЛЬНИЙ ФУНДАМЕНТ ЦИФРОВОГО СУВЕРЕНІТЕТУ.....	170
8.4.1. Цифрова освіта як основа політичної захищеності.....	171
8.4.2. Потреба в незалежній експертизі.....	172
8.4.3. Роль університетів, спільнот, peer-review.....	172
Висновки.....	173
<b>ПІСЛЯМОВА: КЛЕПТОГІГІЄНА ЯК НОВА РАМКА ЦИФРОВОЇ ДОБРОЧЕСНОСТІ.....</b>	<b>177</b>
<b>ПІСЛЯМОВА ПІСЛЯМОВИ: КОЛИ НАВІТЬ ЗАВЕРШЕННЯ ВИЯВЛЯЄТЬСЯ ПОЧАТКОМ... 179</b>	
<b>ДОДАТКИ: АНАЛІТИЧНІ ВІЗУАЛІЗАЦІЇ ДО РОЗДІЛІВ МОНОГРАФІЇ.....</b>	<b>181</b>
Додаток А. Життєвий цикл та типологія бекдорів у цифрових системах.....	181
Додаток Б. Сценарії атак на основі бекдорів: моделі, цілі, наслідки.....	188
Додаток В. Кейси клептографічних втручань: типологія, механізми та наслідки.....	191
Додаток Г. Індикатори клептографічного втручання.....	198
Додаток Д. Стандартизація та регулювання у сфері клептографії.....	202
Додаток Е. Алгоритм виявлення бекдорів за поведінковими ознаками.....	208

Додаток Ж. Поведінковий профіль системи для виявлення клептографічних загроз .....	212
Додаток З. Чеклисти клептогієни для цифрових систем.....	215
Додаток І. Формалізовані моделі та структури довіри у цифрових системах.....	218
Додаток Й. Галерея клептографічної загрози.....	224
<i>Інфографіка 1. Сутність клептографії .....</i>	225
<i>Інфографіка 2. Життєвий цикл клептографічного бекдору .....</i>	228
<i>Інфографіка 3. Порівняльна таблиця типів бекдорів: алгоритмічні, програмні, апаратні ....</i>	232
<i>Інфографіка 4. Класифікаційне дерево загроз .....</i>	233
<i>Інфографіка 5. Точки втручання у життєвий цикл бекдору .....</i>	236
<i>Інфографіка 6. Топологія впровадження бекдорів у технологічному стеку та інфраструктурних доменах .....</i>	240
<i>Інфографіка 7. Механізми активації клептографічних бекдорів: класи, приклади та методи виявлення .....</i>	246
<i>Інфографіка 8. Матриця виявлення та профілювання клептографічних бекдорів .....</i>	252
<i>Інфографіка 9. Типова структура сценарію атаки на основі клептографічних бекдорів .....</i>	262
<i>Інфографіка 10. Інституційна екосистема клептографії.....</i>	270
<i>Інфографіка 11. Спектр цифрового суверенітету: від зовнішнього контролю до автономії ...</i>	276
<b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ .....</b>	<b>283</b>
<b>АЛФАВІТНИЙ ПОКАЖЧИК АВТОРІВ.....</b>	<b>300</b>