



SIDCON
INTERNATIONAL
CONSULTING COMPANY

КІБЕР

МІЖНАРОДНА ЛІГА
КІБЕРБЕЗПЕКИ



ВІЙНИ
ТЕРОРИЗМ
ЗЛОЧИННІСТЬ

КОНЦЕПЦІЇ СТРАТЕГІЇ ТЕХНОЛОГІЇ

K57
351.74:007(045)

Ю. І. Когут

КІБЕРВІЙНИ, КІБЕРТЕРОРИЗМ, КІБЕРЗЛОЧИННІСТЬ (концепції, стратегії, технології)

Київ
Консалтингова компанія «СІДКОН»

 **Дакор**
2022

УДК 351.746.1+004.946.5.056

K57

Рецензенти:

Гордієнко Сергій Георгійович, доктор юридичних наук, доцент, полковник запасу, завідувач кафедри національної безпеки Навчально-наукового інституту права ім. князя Володимира Великого МАУП.

Ткачук Тарас Юрійович, доктор юридичних наук, доцент, заступник директора (з навчальної та наукової роботи) Навчально-наукового гуманітарного інституту Національної академії Служби безпеки України.

Якушик Валентин Михайлович, доктор політичних наук, кандидат юридичних наук, професор Національного університету біоресурсів і природокористування України.

Когут Ю. І.

K57 Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології) : практичний посібник / Ю. І. Когут. – Київ : Консалтингова компанія «СІДКОН» ; ВД «Дакор» 2022. – 284 с.

ISBN 978-617-95100-6-9

ISBN 978-617-8066-15-4

У книзі розкриті питання щодо основних концепцій, технологій та стратегій здійснюваних зараз у світі кібервійн, асиметричних, гібридних, мережевоцентричних (мережевих), інформаційних війн, засад теорії проведення спеціальних інформаційних операцій, проблем та перспектив застосування кіберзброї в сучасній мережевій війні, загроз застосування у процесі розгортання кібервійн штучного інтелекту, теоретико-правових аспектів кібертероризму, напрямів та способів використання кіберпростору в терористичних цілях, нових викликів і стратегій протидії кіберзлочинності.

Результати роботи можуть бути використані практиками – фахівцями з безпеки, науковцями у сфері кібербезпеки, докторантами, аспірантами та студентами вищих навчальних закладів спеціальностей 12.125 «Кібербезпека», 12.121 «Інженерія програмного забезпечення», 12.122 «Комп'ютерні науки та інформаційні технології», 25.251 «Державна безпека», 25.256 «Національна безпека» та інших спеціальностей у сфері інформаційних технологій та кібербезпеки.

УДК 351.746.1+004.946.5.056

*Усі права на матеріал належать ТОВ «Консалтингова компанія «СІДКОН».
Копіювання або використання фрагментів матеріалу можливе тільки
з письмового дозволу ТОВ «Консалтингова компанія «СІДКОН».*



© Когут Ю. І., 2022

© ТОВ «Консалтингова компанія «СІДКОН», 2022

785710

ПЕРЕДМОВА	5
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	9
ВСТУП	10
РОЗДІЛ 1. ПРОТИДІЯ ГІБРИДНИМ ТА АСИМЕТРИЧНИМ ПРОЯВАМ КІБЕРВІЙН ЯК СКЛADOVA ДЕРЖАВНОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ	13
1.1. Кібервійна: поняття, історія, особливості, сучасні тенденції та етапи здійснення. Співвідношення понять «кібератака», «кіберзлочинність», «комп'ютерна злочинність» та «кібервійна»	13
1.2. Гібридний (асиметричний) вимір кібервійн. Технології та стратегії гібридних війн	27
1.3. Концепція та технології мережевоцентричної (мережевої) війни. Проблеми та перспективи застосування кіберзброї у сучасній мережевоцентричній війні. Історія створення кіберзброї	42
1.4. Штучний інтелект у перегонах кіберозброєнь: загрози застосування у ході розгортання кібервійн	68
1.5. Основні засади концепції інформаційної війни та концепції «стратегічних комунікацій». Теорія та практика проведення спеціальних інформаційних операцій	75
1.6. Застосування норм міжнародного права до кібервійн. Глобальне кібернетичне протистояння та механізми стримування, стабілізації та протидії кіберзагрозам	96
РОЗДІЛ 2. КІБЕРТЕРОРИЗМ ЯК РІЗНОВИД КІБЕРЗЛОЧИННОСТІ ТА ОДНА З ОСНОВНИХ ЗАГРОЗ КІБЕРБЕЗПЕЦІ ДЕРЖАВИ	103
2.1. Кібертероризм: історія розвитку, прояви та сучасні тенденції. Кібертерористи у ролі нових акторів світової гібридної війни ...	103
2.2. Теоретико-правові аспекти кібертероризму. Класифікація кібертероризму	119
2.3. Основні цілі, об'єкти кібертерористичних атак, напрями та способи використання кіберпростору у терористичних цілях	129
2.4. Кібертероризм, кібер-хактивізм, кібершпигунство, кібердиверсії та кіберекстремізм як сучасні загрози національній і міжнародній безпеці: співвідношення понять	140

2.5. Зарубіжний досвід щодо розвитку державної системи протидії загрозам кібертероризму	154
США	154
Німеччина	156
Ізраїль	156
Російська Федерація	158
Естонія	158
Литва	159
Латвія	161
Нідерланди	162
Великобританія	164
Франція	166
Польща	166
Канада	167
Австрія	167
Іспанія	168
Австралія	169
2.6. Організаційно-правові питання протидії кіберзлочинності (зокрема кібертероризму) в Україні	170

РОЗДІЛ 3. НОВІ ВИКЛИКИ ТА СТРАТЕГІЇ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

3.1. Кіберзлочинність: поняття, ознаки, причини, наслідки, класифікація, структура, ризики, загрози, сучасні особливості та тенденції. Типи кіберзлочинців	182
3.2. Кіберзлочинність у структурі транснаціональної злочинності. Сучасні тенденції організованої кіберзлочинності	212
3.3. Міжнародно-правова протидія та міжнародне співробітництво у боротьбі з кіберзлочинністю. Роль міжнародних організацій у протидії кіберзлочинності	220
3.4. Організаційно-правове забезпечення протидії кіберзлочинності у зарубіжних країнах	236
3.5. Способи та методи попередження та протидії легалізації доходів, одержаних кіберзлочинцями	250
3.6. Підготовка фахівців з кібербезпеки та протидії кіберзлочинності у зарубіжних країнах та в Україні	256

ВИСНОВКИ

Ключові завдання та напрями протидії кібертероризму, кіберзлочинності та гібридним проявам кібервійн в Україні	266
--	-----

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	270
---	------------