

Ю. І. Когут

# **КІБЕРТЕРОРИЗМ** (історія, цілі, об'єкти)

ПРАКТИЧНИЙ ПОСІБНИК

Київ  
Консалтингова компанія «СІДКОН»  
2021

УДК 351.746.1+004.946.5.056

K57

**Рецензент:**

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

**Когут Ю. І.**

K57 Кібертероризм (історія, цілі, об'єкти) : практичний посібник / Ю. І. Когут. – Київ : Консалтингова компанія «СІДКОН», 2021. – 304 с.

ISBN 978-617-95100-0-7

Практичний посібник підготовлено Когутом Юрієм Івановичем – експертом з більш ніж 20-ти річним практичним досвідом в сфері кібербезпеки та корпоративної безпеки бізнесу, та є першим українським виданням, в якому системно розкриті питання феномену кібертероризму в світі, ризики та загрози, пов'язані з цим явищем на рівні держави, суспільства, бізнесу та особистості.

В посібнику приведені ефективні системні заходи протидії кібертероризму та забезпечення кібербезпеки критично важливих об'єктів інфраструктури, державних та приватних підприємств в епоху цифрової економіки.

Посібник рекомендується до використання як практикам — власникам та керівникам бізнесу, керівникам відповідних підрозділів підприємств, компаній та банків, спеціалістам сфери цифрової трансформації, інформаційної безпеки та кібербезпеки, державним посадовцям, що працюють у секторі діджиталізації, так і науковцям у сфері кібербезпеки, докторантам, аспірантам та студентам 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**

*Всі 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., 2021

© ТОВ «Консалтингова компанія  
«СІДКОН», 2021

ISBN 978-617-95100-0-7

# ЗМІСТ

<b>ПЕРЕДМОВА</b> .....	3
<b>ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ</b> .....	5
<b>ВСТУП</b> .....	6
<b>1. ФЕНОМЕН КІБЕРТЕРОРИЗМУ У СВІТІ В УМОВАХ ГЛОБАЛІЗАЦІЇ ТА ЦИФРОВІЗАЦІЇ. НОВІ РИЗИКИ ДЛЯ МІЖНАРОДНОЇ БЕЗПЕКИ, ПОВ'ЯЗАНІ З КІБЕРТЕРОРИЗМОМ</b> .....	10
1.1. Генезис та еволюція кібертероризму: сутність, особливості, причини виникнення, історія розвитку, форми прояву .....	10
1.2. Цілі та об'єкти атак кібертерористів .....	24
1.3. Основні напрями та способи використання глобальної інформаційно-телекомунікаційної мережі Інтернет та кіберпростору у терористичних цілях. Використовувані кібертерористами віруси як прообрази сучасної кіберзброї. Тактика кібертерористів .....	51
1.4. Сучасні тенденції кібертероризму у світі та трансформація діяльності міжнародних терористичних організацій у кіберпросторі .....	62
<b>2. КІБЕРТЕРОРИЗМ ЯК ЕЛЕМЕНТ ДЕСТАБІЛІЗАЦІЇ СУСПІЛЬНО-ПОЛІТИЧНОЇ ОБСТАНОВКИ ТА СИСТЕМИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У СУСПІЛЬСТВІ</b> .....	87
2.1. Найвідоміші атаки кібертерористів на об'єкти критичної інфраструктури, електронний уряд, банківські системи та приватні компанії у світі та в Україні в історичній ретроспективі та у сучасному економіко-політичному просторі .....	87
2.2. Хакерство, кібершпигунство, кібердиверсії, кіберрозвідка та кібертероризм: взаємозалежності. Політичний та ідеологічний «хактивізм» в епоху інформатизації соціуму. Історія розвитку хактивізму на міжнародному рівні .....	125
2.3. Кібертерористи – на службі у держави як невидима складова кібервійськ .....	147

2.4. Інформаційна зброя в терористичних акціях та локальних конфліктах у кіберпросторі як інструмент силової політики. Загроза міжнародного інформаційного тероризму: відомі дезінформаційні кампанії та війни у кіберпросторі .....	169
<b>3. ПРОТИДІЯ КІБЕРТЕРОРИЗМУ – НАЙВАЖЛИВІШЕ ЗАВДАННЯ СУЧАСНОГО СУСПІЛЬСТВА ТА ДЕРЖАВИ .....</b>	<b>197</b>
3.1. Критична інфраструктура у світі та в Україні як мішень кібертероризму .....	197
3.2. Система суб'єктів національної системи кібербезпеки щодо протидії кібертероризму та забезпечення безпеки критично важливих об'єктів інфраструктури від загроз кібертероризму .....	212
3.3. Кібертероризм як елемент та глобальна зброя гібридної війни – війни нового технологічного рівня в інформаційному просторі України .....	228
3.4. Забезпечення кібербезпеки України від загроз кібертероризму: системний підхід до організації протидії. Концептуальні засади кібернетичної могутності держави .....	267
<b>ВИСНОВКИ .....</b>	<b>288</b>
<b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ .....</b>	<b>291</b>