

Ю. І. Когут

КІБЕРБЕЗПЕКА ТА РИЗИКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ КОМПАНІЙ

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 Кібербезпека та ризики цифрової трансформації компаній : практичний посібник / Ю. І. Когут. – Київ : Консалтингова компанія «СІДКОН», 2021. – 372 с.

ISBN 978-966-97546-9-1

Практичний посібник підготовлено експертом з більш ніж 20-ти річним практичним досвідом в сфері кібербезпеки та корпоративної безпеки бізнесу, та є першим українським виданням, в якому акумульовані теоретичні знання та практичний досвід, системно розкриті питання та технології забезпечення кібербезпеки на рівнях держави, суспільства, бізнесу та особистості в епоху цифрової економіки.

В посібнику вперше системно проаналізовано загрози безпеці держави, суспільства, бізнесу та особистості у кіберпросторі, в т.ч. кіберзлочини як окремий вид кіберзагроз та запропоновані технології протидії та боротьби з ними.

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» та інших спеціальностей у сфері інформаційних технологій.

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».

ISBN 978-966-97546-9-1

© Когут Ю. І., 2021

© ТОВ «Консалтингова компанія
«СІДКОН», 2021

ЗМІСТ

ПЕРЕДМОВА	3
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	5
ВСТУП	6
РОЗДІЛ 1. КИБЕРТЕРОРИЗМ В АСПЕКТІ ГЛОБАЛІЗАЦІЇ: АКТУАЛЬНІ ПРОБЛЕМИ НАЦІОНАЛЬНОЇ ТА МІЖНАРОДНОЇ КИБЕРБЕЗПЕКИ	10
1.1. Кібертероризм: історія розвитку та сучасні тенденції	10
1.2. Загрози кібертероризму та найбільш відомі кібератаки в сучасному цифровому суспільстві як інформаційні виклики національній безпеці	21
1.3. Правові засади формування та розвитку державної системи протидії кібертероризму в Україні як загрози інформаційній безпеці	39
1.4. Зарубіжний досвід щодо розвитку систем протидії загрозам кібертероризму на державному рівні: національні структури, які забезпечують кібербезпеку у зарубіжних країнах, а також кібервійська провідних держав світу, їх можливості та перспективи	48
1.5. Національні команди реагування на надзвичайні комп'ютерні інциденти CERT/CSIRT	80
1.6. Міжнародні структури, які забезпечують кібербезпеку на глобальному рівні. Суб'єкти національної системи кібербезпеки України	92
РОЗДІЛ 2. КИБЕРТЕРОРИЗМ ТА ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ	115
2.1. Стратегії кібербезпеки у зарубіжних країнах. Запровадження в Україні кращих практик реалізації державних стратегій та імплементація вимог міжнародно-правових документів з протидії кібертероризму	115

2.2. Загрози кібертероризму критичній інфраструктурі та забезпечення її кібербезпеки у зарубіжних країнах	129
2.3. Правові засади кіберзахисту критично важливих об'єктів України. Розробка національної стратегії протидії кібертероризму для об'єктів критичної інфраструктури держави	142
2.4. Кіберпростір як сфера геополітичного протистояння. Кіберзброя – суспільно небезпечний продукт цифрових технологій у міжнародних конфронтаціях	160
2.5. Проблематика міжнародної кібербезпеки – кібератаки, кібервійни, інформаційні війни, мережевоцентричні війни, їх ознаки та особливості	184
2.6. Кібертероризм, політичний хактивізм, кібершпигунство, кібердиверсії та кіберекстремізм як сучасні загрози національній і міжнародній безпеці	194
РОЗДІЛ 3. КІБЕРБЕЗПЕКА БІЗНЕСУ	200
3.1. Основні напрямки і ризики використання новітніх технологій цифрової економіки в бізнесі: ідентифікація сучасних загроз кібербезпеці бізнесу	200
3.2. Необхідні умови для впровадження системи кібербезпеки в компаніях в умовах цифрової трансформації	221
3.3. Завдання щодо досягнення надійної системи кібербезпеки компанії, яка б відповідала міжнародним стандартам кібербезпеки й управління ризиками	224
3.4. Державно-приватне партнерство для забезпечення кібербезпеки бізнесу та держави	232
3.5. Управління інцидентами кібербезпеки в компаніях за умов розвитку процесів цифровізації бізнесу	236
3.6. Основні заходи щодо організації ефективної системи управління кібербезпекою в компаніях у сучасних умовах розвитку цифрової економіки та зростання ризиків кібертероризму	245
РОЗДІЛ 4. КІБЕРБЕЗПЕКА ОСОБИСТОСТІ ТА СУСПІЛЬСТВА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ	253
4.1. Генезис проблеми кібербезпеки в контексті формування інформаційного суспільства	253

4.2. Суспільство як об'єкт інформаційного управління	257
4.3. Державна стратегія з протидії кібертероризму в Україні	262
4.4. Забезпечення захисту персональних даних в умовах розвитку цифрового суспільства та економіки	270
4.5. Технології глобального управління соціополітичними процесами в умовах реалізації кіберзагроз та ведення кібервійн	278
4.6. Засоби протистояння кібервпливу на особистість в умовах цифровізації суспільства	291
РОЗДІЛ 5. СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ ВІД ЗАГРОЗ КІБЕРТЕРОРИЗМУ	295
5.1. Забезпечення національних інтересів України в глобальному та національному кіберпросторах шляхом модернізації механізмів реалізації стратегії протидії кібертероризму в Україні	295
5.2. Проблеми відповідності національної системи кібербезпеки України європейським вимогам та стандартам	308
5.3. Удосконалення суб'єктного складу національних структур, які забезпечують кібербезпеку на державному рівні	315
5.4. Протидія кібертероризму в цифрову епоху: напрями удосконалення захисту інформаційного простору України від загроз кібертероризму	324
5.5. Кібертероризм та мережеві війни на державному рівні: підходи, доктрини, практика. Геополітичні, національні пріоритети України в кіберпросторі за умов посилення міждержавного інформаційного протистояння між основними геополітичними гравцями	331
5.6. Ключові завдання щодо забезпечення інформаційної безпеки держави та протидії кібертероризму	342
ВИСНОВКИ	346
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	350
ДОДАТКИ	364