

М.М. БРАІЛОВСЬКИЙ, С.В. ЗИБІН, А.А. КОБОЗЄВА,
В.О. ХОРОШКО, Ю.Є. ХОХЛАЧОВА

004.056

А64

АНАЛІЗ КІБЕРЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

КИЇВ 2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

М. М. Браїловський, С. В. Зибін, А. А. Кобозєва,

В. О. Хорошко, Ю. Є. Хохлачова

АНАЛІЗ КІБЕРЗАХИЩЕНОСТІ

ІНФОРМАЦІЙНИХ СИСТЕМ

Монографія

Київ 2021

УДК 004.056.5

ББК 32.973я7

Б 17

Рекомендовано до друку Вченою Радою факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету (протокол № 8 від 15.09.2021 р.)

Рецензенти:

доктор технічних наук, професор Лаптев О. А.

доктор технічних наук, професор Опірський І. Р.

доктор технічних наук, професор Шелест М. Є.

Б17 Браїловський М. М. Аналіз кіберзахищеності інформаційних систем: монографія / Браїловський М. М., Зибін С. В., Кобозєва А. А., Хорошко В. О., Хохлачова Ю. Є. – К.: ФОП Ямчинський О. В., 2021. – 360 с.

ISBN 978-617-8049-61-4

У монографії на основі теорії керування та загального математичного підходу розглядається оцінювання створення і функціонування систем кіберзахищеності у сучасних умовах, а також методів синтезу, без чого неможлива побудова розвиненого та адекватного наукового базису кібербезпеки. Також розглядається дуже велика кількість наступних питань: аналіз задач кібербезпеки, інформації та інформаційні технології; концепції та моделювання кіберзахисту, керування кібербезпекою та кіберзахистом інформаційних технологій.

Монографія буде корисна фахівцям у галузі інформаційної безпеки та кіберзахисту, аспірантам та студентам, які займаються цією тематикою.

УДК 004.056.5

ББК 30

ISBN 978-617-8049-61-4

© Браїловський М. М., Зибін С. В.,
© Кобозєва А. А., Хорошко В. О.,
© Хохлачова Ю. Є.

ЗМІСТ

Перелік прийнятих скорочень.....	7
Вступ.....	9
Розділ 1. Інформація та її зв'язок із галуззю діяльності суспільства.....	11
1.1. Види інформації.....	11
1.2. Інформація для ухвалення рішень.....	13
1.2.1. Інформація для стратегічних рішень.....	13
1.2.2. Інформація для тактичних рішень.....	14
1.2.3. Інформація для вирішення оперативних питань.....	15
1.3. Збирання та обробка інформації.....	16
1.3.1. Шлях інформації.....	16
1.3.2. Канали інформації.....	18
1.3.3. Обробка інформації.....	19
1.3.4. Цикл інформації.....	20
1.3.5. Помилкова інформація.....	20
1.3.6. Витік інформації.....	23
Розділ 2. Необхідність кіберзахисту інформації в сучасних умовах.....	25
2.1. Класифікація цілей захисту.....	25
2.2. Основні положення концепції кіберзахисту.....	30
2.3. Визначення та аналіз поняття загрози інформації.....	32
2.4. Система показників уразливостей інформації та вимоги до первинних даних.....	35
Розділ 3. Аналіз задач кібербезпеки в сучасних умовах.....	38
Розділ 4. Інформація та інформаційні технології.....	49
4.1. Класифікація інформації за режимом доступу до неї.....	49
4.2. Інформаційні технології та їх основні складові елементи.....	54
4.3. Програмне забезпечення інформаційних технологій.....	62
Розділ 5. Формалізація інформаційного процесу.....	76
5.1. Неперервний інформаційний процес.....	77
5.2. Дискретний інформаційний процес.....	81
5.3. Матричне представлення перетворення інформаційних систем.....	82
Розділ 6. Дослідження структури інформаційного процесу.....	90
6.1. Параметри інформаційного процесу і зв'язок між ними.....	90
6.2. Варіаційна матриця інформаційного процесу.....	92
6.3. Граф інформаційного процесу.....	97

6.4. Паралельні форми інформаційного процесу	98
6.5. Введення у функціональні дослідження структури інформаційного процесу	102
Розділ 7. Концепція та моделі кібербезпеки.....	106
7.1. Концепція керування безпекою інформаційних технологій	106
7.2. Елементи кібербезпеки	108
7.3. Процес керування безпекою інформаційних технологій	113
7.4. Моделі кібербезпеки	119
7.5. Архітектура кібербезпеки	124
7.6. Аналіз моделей моніторингу	127
Розділ 8. Загальні критерії оцінювання кіберзахисності.....	132
Розділ 9. Аналіз стану та процесу функціонування систем кіберзахисту.....	139
9.1. Розробка моделей системи кіберзахисту	139
9.2. Моделювання атаки на захищену інформаційну систему	141
9.3. Аналіз стійкості систем кіберзахисту до передбачуваного супротивника	156
9.4. Метод оцінювання стійкості системи кіберзахисту до передбачуваного супротивника	169
Розділ 10. Дослідження життєвого циклу систем кіберзахисту.....	176
10.1 Неформальний опис життєвого циклу системи кіберзахисту	176
10.1.1. Аналіз та етапи моделювання життєвого циклу системи кіберзахисту	176
10.1.2. Моделі життєвого циклу системи кіберзахисту	180
10.2. Моделі життєвого циклу програмних механізмів захисту системи кіберзахисту	184
Розділ 11. Моделювання процесу кіберзахисту.....	196
11.1. Методи моделювання систем кіберзахисту	196
11.2. Аналіз моделей кіберзахисту	199
11.3. Аналіз кіберзахисності систем	211
11.4. Визначення показників якості захищеності моделі кіберзахисту	220
Розділ 12. Керування безпекою інформаційних технологій.....	228
12.1. Процес підтримки безпеки інформаційних технологій	228
12.2. Методика безпеки інформаційних технологій	231
12.3. Організаційні аспекти керування безпекою інформаційних технологій	233
12.4. Вибір стратегії аналізу ризику	238
12.5. Рекомендації щодо захисту інформаційних технологій	241
12.6. Методика захисту системи інформаційних технологій	242
Розділ 13. Керування кіберзахистом інформаційних технологій.....	245

13.1. Підходи та рекомендації щодо кіберзахисту інформаційних технологій	245
13.2. Методика кіберзахисту системи інформаційних технологій	247
13.3. План кіберзахисту інформаційних технологій	248
13.4. Впровадження засобів кіберзахисту	249
13.5. Компетентність у кіберзахисті	250
Розділ 14. Керування кібербезпекою.....	253
14.1. Політика інформаційної безпеки	253
14.2. Програма управління кібербезпекою	258
14.3. Основні класи заходів процедурного рівня	260
14.4. Керування інцидентами кібербезпеки	266
14.5. Керування кіберзахистом автоматизованих робочих місць	277
Розділ 15. Методи керування кібербезпекою.....	285
15.1. Методика керування кібербезпекою інформаційних технологій	285
15.2. Цілі, стратегії методики кібербезпеки інформаційних технологій	286
15.3. Варіанти стратегії аналізу ризику	290
15.4. Реалізація змішаного підходу до аналізу ризиків	294
15.5. Застосування плану безпеки інформаційних технологій	318
Розділ 16. Методи та підходи в управлінні кібербезпекою	325
16.1. Метод наукового управління	325
16.2. Метод адміністративного управління	326
16.3. Метод людських відносин	327
16.4. Метод кількісного підходу в управлінні	331
16.5. Процесний підхід в управлінні	334
16.6. Системний підхід в управлінні	337
16.7. Ситуаційний підхід в управлінні	343
16.8. Використання методів і підходів в управлінні кібербезпекою	350
Література.....	354