

**В.Л. БУРЯЧОК
Р.В. ГРИЩУК
В.О. ХОРОШКО**



**ПОЛІТИКА
ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ**



БКК 351.86:004.056](075/8)

Б 91

УДК 67.401.212,73

Бурячок В. Л., Гришук Р. В., Хорошко В. О.

Політика інформаційної безпеки: підручник. / В. Л. Бурячок, Б 91 Р. В. Гришук, В. О. Хорошко /. За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К. : ПВП «Задруга», 2014. – 222 с.

ISBN 978–966–2970–87–6

У підручнику розглядаються основи політики інформаційної безпеки інформаційних технологій. Розкривається сутність та зміст інформаційної безпеки та її складових. Значна увага приділяється методології формування множини загроз інформаційній безпеці. Приводиться порядок здійснення процедур щодо вибору засобів захисту інформації, їх доопрацювання в процесі експлуатації за призначенням та управління безпекою інформаційних технологій.

Підручник орієнтований на фахівців у галузі інформаційної безпеки та захисту інформації, а також наукових та науково-педагогічних працівників, профіль діяльності яких пов'язаний з цими процесами. Викладений матеріал може бути корисним для аспірантів, магістрантів і студентів вищих навчальних закладів, котрі спеціалізуються у сфері управління інформаційною безпекою та систем захисту інформації й навчаються за спеціальностями освітнього напрямку "Інформаційна безпека".

БКК 67.401.212,73

УДК 351.86:004.056](075/8)

784711

*Рекомендовано вченою радою Національного авіаційного університету
до друку та використання в навчальному процесі
(протокол № 9 від 23.12.2013 року)*

Рецензенти:

Єрохін В. Ф. – доктор технічних наук, професор.
Ленков С. В. – доктор технічних наук, професор.
Самохвалов Ю. Я. – доктор технічних наук, професор.
Соснін О. В. – доктор політичних наук, професор.

© В. Л. Бурячок, 2014,

© Р. В. Гришук, 2014,

© В. О. Хорошко, 2014.

ISBN 978–966–2970–87–6

ЗМІСТ

	<i>стр.</i>
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	5
ПЕРЕДМОВА	6
РОЗДІЛ 1. ІНФОРМАЦІЯ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ	9
1.1. Інциденти у сфері високих технологій	9
1.2. Етапи життєвого циклу інформації та її загальні властивості	18
1.3. Мета застосування та засоби реалізації сучасних інформаційних технологій.....	27
1.3.1. Особливості розробки та застосування програмного забезпечення інформаційних систем	45
1.3.2. Види ліцензійних угод на розповсюдження програмного забезпечення інформаційних систем	51
Запитання для самоконтролю	54
РОЗДІЛ 2. НЕОБХІДНІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ	55
2.1. Основні положення системно-концептуального підходу до захисту інформації. Класифікація цілей захисту	55
2.2. Визначення і аналіз поняття загрози безпеці інформації	58
2.2.1. Формалізована модель оцінювання загроз безпеці інформації за метою реалізації	67
2.2.2. Аналіз функціонування інформаційних систем в умовах загроз системам обробки інформації з обмеженим доступом	73
2.3. Особливості реалізації атак та заходи послаблення їх деструктивного впливу	76
2.4. Система показників уразливості інформації і вимоги до первинних даних	86
Запитання для самоконтролю	88
РОЗДІЛ 3. ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ	90
3.1. Фізичний захист інформації з обмеженим доступом	91
3.2. Технічний захист інформації з обмеженим доступом	92
3.3. Криптографічні засоби захисту інформації з обмеженим доступом ...	100
3.4. Доопрацювання засобів захисту	104
Запитання для самоконтролю	115
РОЗДІЛ 4. ОСНОВНІ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	116
4.1. Основні складові інформаційної безпеки.....	119

4.2.	Важливість і складність проблеми інформаційної безпеки	121
4.3.	Модель подання системи інформаційної безпеки. Методи та засоби її забезпечення	123
	Запитання для самоконтролю	130
РОЗДІЛ 5. ФОРМУВАННЯ МНОЖИНИ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ		131
5.1.	Причини порушення цілісності інформації	132
5.2.	Канали несанкціонованого доступу інформації	134
5.3.	Методи визначення значень показників уразливості інформації	138
	Запитання для самоконтролю	144
РОЗДІЛ 6. ВИБІР ЗАСОБІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		145
6.1.	Використання базового і детального підходів вибору засобів безпеки в інформаційних системах	147
6.2.	Обґрунтування базових вимог до безпеки інформації в інформаційних системах	150
6.3.	Вибір базового набору регуляторів безпеки	154
	Запитання для самоконтролю	157
РОЗДІЛ 7. УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ		158
7.1.	Процес управління безпекою інформаційних технологій	158
7.1.1.	Стратегія та методи забезпечення інформаційної безпеки	161
7.1.2.	Функції управління безпекою інформаційних технологій	164
7.2.	Елементи безпеки інформаційних технологій	165
7.3.	Моделі управління безпекою інформаційних технологій	169
7.4.	Міжнародний стандарт ISO/IEC 17799:2005. Призначення та особливості	174
7.5.	Міжнародний стандарт ISO/IEC 27001. Призначення та особливості	187
	Запитання для самоконтролю	190
РОЗДІЛ 8. МОДЕЛІ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		192
8.1.	Дискреційна модель політики інформаційної безпеки	193
8.2.	Мандатна модель політики інформаційної безпеки	197
8.3.	Рольова модель політики інформаційної безпеки	200
	Запитання для самоконтролю	204
ПІСЛЯМОВА		206
ГЛОСАРІЙ		207
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ		218