

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Київський університет імені Бориса Грінченка



Гулак Г. М., Жильцов О. Б., Киричок Р. В.,
Коршун Н. В., Складанний П. М.

ІНФОРМАЦІЙНА та КІБЕРНЕТИЧНА БЕЗПЕКА ПІДПРИЄМСТВА

Підручник



Львів
Видавець Марченко Т. В.
2024

*Рекомендовано до друку Вченою радою
Київського університету імені Бориса Грінченка
(протокол №10 від 30.11.2023 р.)*

Автори:

Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М.

Рецензенти:

Смірнов О. А. – завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, доктор технічних наук, професор;

Опірський І. Р. – завідувач кафедри захисту інформації Національного університету «Львівська політехніка», доктор технічних наук, професор;

Ковальчук Л. В. – провідний науковий співробітник Інституту проблем моделювання в енергетиці Національної академії наук України, доктор технічних наук, професор.

Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М.

I-74 **Інформаційна та кібернетична безпека підприємства** : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2024. – 370 с.

ISBN 978-617-7937-91-2

Широке використання в процесі інформатизації суспільства сучасних технологій автоматизованої обробки інформації та управління технологічними процесами створило не тільки об'єктивні передумови підвищення ефективності всіх видів діяльності особи, суспільства та держави, але і ряд проблем захисту інформації. Складність вирішення цих проблем обумовлена необхідністю створення систем захисту інформації в умовах обмежених фінансових, матеріальних, людських та часових ресурсів.

В цих умовах розуміння потенціалу різних методів та технологій захисту, їх взаємного зв'язку та взаємного доповнення, глибоке знання принципів та методів управління організаційно-технічними системами створюють надійне підґрунтя ефективного розв'язання згаданих проблем керівниками та виконавцями служб захисту інформації, практиками та дослідниками протягом всього життєвого циклу автоматизованих систем обробки даних.

Для студентів, що навчаються за спеціальністю 125 – Кібербезпека, аспірантів, науковців та практиків.

УДК 004.056

ISBN 978-617-7937-91-2

© Гулак Г. М., Жильцов О. Б., Киричок Р. В.,
Коршун Н. В., Складанний П. М., 2024
© Київський університет ім. Б. Грінченка, 2024
© Видавець Марченко Т. В., 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	8
ВСТУП.....	12

РОЗДІЛ 1

Актуальні проблеми захисту інформації в кіберпросторі та методичні засади забезпечення інформаційної безпеки.....	14
--------------------------------------------------------------------------------------------------------------------------	-----------

1.1. Методологія захисту інформації як організація продуктивної діяльності людини.....	14
1.2. Понятійний апарат інформаційної безпеки та кібербезпеки	21
1.3. Складові забезпечення інформаційної безпеки та кібербезпеки	26

РОЗДІЛ 2

Елементи загальної теорії захисту інформації	30
2.1. Характеристика інформації як об'єкта захисту	30
2.2. Інформація як об'єкт права власності	36
2.3. Поняття, сутність, цілі захисту інформації.....	37

РОЗДІЛ 3

Інформаційно-технологічна складова підприємництва	43
3.1. Особливості сучасної системи електронного підприємництва	43
3.2. Структура інформаційної сфери підприємництва.....	46
3.3. Загальна характеристика системи бізнес-процесів підприємства	49
3.4. Технологічна основа підприємництва	52

РОЗДІЛ 4

Загрози інформації та основні принципи побудови моделей загроз і порушника інформаційної безпеки.....	58
4.1. Сутність потенційних та реальних загроз інформації.....	58
4.2. Класифікація загроз інформації, джерел їхнього виникнення та шляхи реалізації	60
4.3. Основні аспекти побудови моделей загроз інформаційної безпеки	74

4.4. Особливості формування моделі порушника інформаційної безпеки.....	77
----------------------------------------------------------------------------	----

РОЗДІЛ 5

Основні напрями забезпечення інформаційної та кібернетичної безпеки підприємства.....	84
--------------------------------------------------------------------------------------------------	-----------

5.1. Загальна модель інформаційної та кібернетичної безпеки організації.....	84
5.2. Базові принципи побудови системи захисту інформації	96

РОЗДІЛ 6

Основа адміністративного рівня забезпечення інформаційної безпеки: політика, аналіз та оцінка ризиків	102
------------------------------------------------------------------------------------------------------------------------	------------

6.1. Основні підстави та цілі створення політики безпеки	102
6.2. Загальні принципи формування політики інформаційної безпеки підприємства.....	106
6.3. Базові аспекти та методологія аналізу й оцінки ризиків інформаційної безпеки	111

РОЗДІЛ 7

Сучасні методи забезпечення надійності персоналу як складова процедурного рівня забезпечення інформаційної безпеки	125
-----------------------------------------------------------------------------------------------------------------------------------------	------------

7.1. Психологічний стан на різних етапах розвитку підприємства	125
7.2. Кадрова складова інформаційної безпеки.....	132
7.3. Методи підвищення ефективності дій персоналу щодо забезпечення інформаційної безпеки.....	134

РОЗДІЛ 8

Методи технічного захисту інформації на об'єктах інформаційної діяльності	137
--------------------------------------------------------------------------------------------	------------

8.1. Основні положення та нормативні визначення щодо технічного захисту інформації.....	137
8.2. Поняття та характеристика технічних каналів витоку інформації	139
8.3. Захист інформації від витоку електричними та електромагнітними каналами	142
8.4. Методи захисту від витоку інформації за рахунок акустичних та оптичних каналів.....	145
8.5. Спеціальні дослідження технічних засобів.....	149

РОЗДІЛ 9

Інженерно-технічні методи забезпечення об'єктів інформаційної діяльності	151
9.1. Методи й засоби контролю, сигналізації, розмежування доступу на об'єкти інформаційної діяльності.....	152
9.2. Методи мінімізації збитків від аварій і стихійних лих.....	156

РОЗДІЛ 10

Основні аспекти підтримки працездатності, керування інцидентами інформаційної безпеки та відновлення іт-інфраструктури	159
10.1. Методи підтримки працездатності технічних систем та підвищення їхньої надійності	159
10.2. Керування інцидентами інформаційної безпеки.....	162
10.2.1. Процес реагування на інциденти інформаційної безпеки	169
10.3. Процедури відновлення ІТ-інфраструктури	175

РОЗДІЛ 11

Механізми забезпечення інформаційної безпеки програмно-технічного рівня	180
11.1. Методи захисту інформації від НСД в автоматизованих системах.....	180
11.1.1. Системи ідентифікації та аутентифікації користувачів	182
11.1.2. Системи розмежування доступу до інформації	193
11.1.3. Засоби захисту від НСД через мережу	197
11.2. Особливості антивірусних технологій захисту інформації.....	200
11.3. Основні технології захисту від DDoS-атак	206
11.4. Системи виявлення та запобігання вторгненням (IDS / IPS).....	213
11.5. Технологія керування інформацією та подіями безпеки (SIEM)	216

РОЗДІЛ 12

Технології криптографічного захисту інформації.....	219
12.1. Базові поняття криптографічного захисту інформації.....	220
12.2. Симетричні криптографічні системи.....	224
12.3. Асиметричні криптографічні системи	228
12.4. Механізми забезпечення цілісності та аутентичності інформації	233
12.5. Забезпечення безпеки та керування криптографічними ключами.....	239

12.6. Типові вимоги до побудови та застосування сучасних криптосистем	243
12.7. Порядок формування та застосування на підприємстві системи спеціального зв'язку.....	250
12.7.1. Проблематика вибору засобів криптографічного захисту інформації.....	258
12.8. Основи застосування технології блокчейн	260

РОЗДІЛ 13

Методи та моделі стеганографії.....	263
13.1. Комп'ютерна і цифрова стеганографія, цифрові водяні знаки.....	264
13.2. Модель комп'ютерної стеганографічної системи	267
13.3. Вразливості стеганографічних систем	269

РОЗДІЛ 14

Методи відновлення та гарантованого знищення інформації	271
14.1. Проблеми й технології відновлення доступу до даних, збережених на машинних носіях	271
14.2. Гарантоване знищення інформації в комп'ютерних системах	278

РОЗДІЛ 15

Методика побудови комплексної системи захисту інформації в інформаційно-комунікаційних системах.....	286
15.1. Класифікація автоматизованих систем згідно з НД ТЗІ	288
15.2. Етапи створення комплексної системи захисту інформації	289
15.3. Вимоги до організаційних заходів	293
15.4. Склад проектної та експлуатаційної документації.....	295

РОЗДІЛ 16

Особливості захисту різних видів інформації з обмеженим доступом	298
16.1. Сутність критеріїв оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.....	298
16.2. Основні заходи щодо захисту державної таємниці.....	303
16.3. Особливості захисту службової інформації	305
16.4. Особливості захисту персональних даних	306
16.5. Особливості раціонального вибору засобів захисту інформації.....	309

РОЗДІЛ 17

Концепція створення системи управління інформаційною безпекою	312
17.1. Методологічні аспекти побудови системи управління інформаційною безпекою	312
17.2. Процесний підхід як основа побудови системи управління інформаційною безпекою підприємства.....	314
17.3. Створення системи управління інформаційною безпекою	316
17.4. Переваги впровадження системи управління інформаційною безпекою	320

РОЗДІЛ 18

Методика аудиту безпеки інформаційної інфраструктури підприємства.....	324
18.1. Загальні положення аудиту інформаційної безпеки на підприємстві	325
18.2. Методичні аспекти внутрішнього аудиту інформаційної безпеки.....	327
18.3. Основні аспекти організації зовнішнього аудиту інформаційної безпеки.....	333

РОЗДІЛ 19

Кібернетична розвідка як інструмент підтримання безпеки інформаційних систем	344
19.1. Роль кіберрозвідки в протистоянні сучасним загрозам кібербезпеки	345
19.2. Технологія Threat Intelligence	348
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	362

Навчальне видання

ГУЛАК Геннадій Миколайович,
ЖИЛЬЦОВ Олексій Борисович,
КИРИЧОК Роман Васильович,
КОРШУН Наталія Володимирівна,
СКЛАДАННИЙ Павло Миколайович

ІНФОРМАЦІЙНА та КІБЕРНЕТИЧНА БЕЗПЕКА ПІДПРИЄМСТВА

Підручник

Підп. до друку 30.11.2023 р.
Формат 70x100/16. Папір друк. №2. Гарнітура PT Serif.
Умовн. друк. арк. 30,06. Наклад 300 прим.

Видавець Марченко Т. В.
м. Львів-53, 79053, Україна, тел.: +38 (050) 370-19-57
e-mail: magnol06@ukr.net
<https://magnolia.lviv.ua>

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників і розповсюджувачів видавничої
продукції: серія ДК № 6784 від 30.05.2019 року,
видане Державним комітетом інформаційної політики,
телебачення та радіомовлення України.

Надруковано у друкарні видавця Марченко Т. В.