

## ЗМІСТ

<b>Вступ</b> .....	7
<b>Розділ 1. СОЦІАЛЬНІ, ЕКОНОМІЧНІ ТА ПРАВОВІ АСПЕКТИ МЕНЕДЖМЕНТУ ІБ</b> .....	11
1.1. Соціальні проблеми інформації .....	11
1.2. Інформація та відображення матеріального світу .....	12
1.3. Роль держави у сфері ІБ.....	15
1.4. Правові принципи ІБ .....	16
1.5. Класифікація інформації організації.....	17
1.6. Правові аспекти функціонування організацій .....	21
1.7. Загальна структура інформаційної сфери організації .....	23
1.8. Інформаційна сфера – головне джерело ризиків ІБ організації.....	28
1.9. Інформаційні характеристики організації та природи її ризиків .....	30
Запитання для самоконтролю .....	34
<b>Розділ 2. ОСНОВНІ ЕЛЕМЕНТИ МЕНЕДЖМЕНТУ ІБ</b> .....	35
2.1. Загальні зауваження .....	35
2.2. Безпека через віру в необізнаність зловмисника .....	36
2.3. Підхід «зверху–вниз» .....	37
2.4. Відповідальність за стан ІБ .....	38
2.5. Основні принципи безпеки .....	42
2.6. Визначення ІБ .....	43
2.7. Ідентифікація подій ІБ .....	46
2.8. Профіль та життєвий цикл загрози .....	49
2.9. Способи класифікації загроз .....	52
2.9.1. Загрози, що реалізуються за допомогою програмних засобів .....	56
2.9.2. Загрози витоку інформації технічними каналами .....	56
2.9.3. Загрози програмними засобами .....	57
2.9.4. Загрози технічними засобами .....	57
2.10. Ранжування джерел загроз .....	58
2.11. Класифікація вразливостей інформаційних активів .....	63
2.11.1. Ідентифікація вразливостей організаційного рівня .....	65
2.11.2. Ідентифікація технічних вразливостей .....	66
2.12. Ранжування вразливостей ІБ .....	66
2.13. Наслідки реалізації пари джерело загроз–уразливість .....	68
2.14. Збитки та їхні негативні наслідки для організації .....	69
2.14.1. Збитки як категорія класифікації загроз.....	71
Запитання для самоконтролю.....	72
<b>Розділ 3. ОСНОВНІ ЕЛЕМЕНТИ УПРАВЛІННЯ РИЗИКАМИ ІБ</b> .....	74
3.1. Поняття ризику ІБ .....	74
3.2. Оцінювання ризиків як основа корпоративного управління .....	75
3.3. Оцінювання ризику .....	76

3.3.1. Кількісний аналіз ризиків .....	77
3.3.2. Якісний аналіз ризиків .....	80
3.3.2.1. Метод DELPHI .....	84
3.4. Порівняння кількісного та якісного аналізу ризиків .....	85
3.5. Інформаційна складова бізнес-ризиків .....	86
3.6. Активи організації як ключовий фактор ризику .....	88
3.7. Аналіз факторів ризику .....	89
3.8. Попередній аналіз ризиків на основі системного ризик-орієнтованого підходу .....	92
3.9. Інтерпретація характеристик ризику для управління ІБ .....	93
3.10. Переваги системного підходу управління ризиками .....	95
3.11. Зміст процесу управління ризиками .....	98
3.12. Структура документації з управління ризиками .....	99
3.13. Політика управління інформаційними ризиками .....	101
3.14. Структура системи управління ризиками .....	104
3.14.1. Процесна модель управління ризиками .....	105
3.15. Неперервна діяльність з управління ризиками .....	108
3.15.1. Супровід та моніторинг механізмів ІБ .....	108
3.15.2. Аналіз процесу з боку керівництва .....	109
3.15.3. Перегляд та переоцінювання ризику .....	110
3.15.4. Взаємозв'язок процесів аудиту та управління ризиками .....	110
3.15.5. Управління документами та записами .....	111
3.15.6. Превентивні та коригуючі заходи .....	112
3.15.7. Комунікація ризиків .....	112
3.16. Аутсорсинг процесів управління ризиками .....	113
3.17. Розподіл відповідальності за управління ризиками .....	114
3.17.1. Вимоги до ризик-менеджера .....	116
3.17.2. Група аналізу ризиків .....	117
3.17.3. Вимоги до експерта з оцінювання ризиків1 .....	18
Запитання для самоконтролю .....	119
<b>Розділ 4. ОЦІНЮВАННЯ ТА ОБРОБЛЕННЯ РИЗИКІВ ІБ .....</b>	<b>120</b>
4.1. Формулювання проблеми оцінювання та оброблення ризиків .....	120
4.2. Ідентифікація активів .....	122
4.3. Опис бізнес-процесів .....	123
4.3.1. Основні бізнес-процеси організації .....	123
4.3.2. Допоміжні процеси організації .....	124
4.3.3. Механізм ідентифікації та опису бізнес-процесу організації .....	125
4.3.4. Реєстр інформаційних активів .....	129
4.4. Ідентифікація вимог ІБ .....	131
4.4.1. Реєстр вимог ІБ .....	132
4.4.2. Вимоги законодавства та нормативної бази .....	133
4.4.3. Контрактні зобов'язання .....	134
4.4.4. Вимоги бізнесу .....	136
4.5. Цінність інформації та активів .....	137

4.5.1. Визначення цінності активів .....	138
4.5.2. Критерії оцінювання збитку .....	140
4.5.3. Таблиця цінності активів організації .....	142
4.6. Оцінювання процесів СМІБ на відповідність ISO 27001 .....	143
4.7. Визначення пріоритетів аварійного відновлення .....	147
4.8. Визначення значення ризику .....	152
4.8.1. Калібрування шкали оцінювання ризику .....	154
4.8.2. Приклад оцінювання ризику .....	155
4.8.3. Звіт з оцінювання ризиків .....	157
4.9. Процес оброблення ризиків .....	158
4.10. Способи оброблення ризиків ІБ .....	160
4.10.1. Прийняття ризику .....	163
4.10.1.1. Критерій прийняття ризиків .....	164
4.10.2. Зменшення значення ризику .....	166
4.10.3. Передавання ризику .....	168
4.10.4. Уникнення ризику .....	169
4.11. Оцінювання повернення інвестицій в ІБ .....	170
4.12. Прийняття рішення про оброблення ризику .....	173
4.13. План оброблення ризиків .....	174
4.14. Положення про застосування контролів .....	177
4.15. Завершальні висновки-рекомендації .....	179
Запитання для самоконтролю .....	183

## **Розділ 5. РОЗРОБЛЕННЯ ПОЛІТИКИ ЗАПРОВАДЖЕННЯ ІБ .....**

5.1. Політика ІБ .....	185
5.2. Визначення та види політики ІБ .....	187
5.3. Основні причини створення політик ІБ .....	191
5.4. Моделі управління доступом на основі політик ІБ .....	194
5.4.1. Дискреційна (розмежувальна) політика ІБ .....	195
5.4.2. Мандатна політика ІБ .....	197
5.4.3. Рольова політика ІБ .....	200
5.5. Розроблення політик ІБ .....	202
5.5.1. Складнощі впровадження політик ІБ .....	202
5.5.2. Склад групи з розроблення політик ІБ .....	203
5.5.3. Процес розроблення політик ІБ .....	203
5.5.4. Основні вимоги до політики ІБ .....	205
5.6. Приклади політик ІБ .....	205
5.7. Варіанти політик ІБ організацій .....	209
5.7.1. Металургійна компанія .....	209
5.7.2. Комерційний банк .....	211
5.8. Політики, рекомендовані Інститутом SANS .....	214
5.8.1. Політика допустимого шифрування .....	215
5.8.2. Політика допустимого використання .....	215
5.8.3. Політика антивірусного захисту .....	219
5.8.4. Політика зберігання електронної пошти .....	220

5.8.5. Політика використання електронної пошти.....	221
5.8.6. Політика використання паролів.....	222
5.8.7. Політика оцінювання ризиків ІБ .....	226
5.8.8. Політика ІБ маршрутизатора .....	226
5.8.9. Політика забезпечення ІБ серверів.....	227
5.8.10. Політика віртуальних приватних мереж.....	229
5.8.11. Політика безпроводного доступу до мережі організації.....	230
5.8.12. Політика автоматичного переадресування електронної пошти .....	231
5.8.13. Політика класифікації інформації .....	232
5.8.14. Політика паролів доступу до баз даних .....	236
5.8.15. Політика ІБ сегменту демілітаризованої зони.....	238
5.8.16. Політика ІБ внутрішнього сегменту .....	241
5.8.17. Політика екстранету .....	244
5.8.18. Кодекс етики .....	245
5.8.19. Політика антивірусного захисту.....	247
Запитання для самоконтролю .....	248
<b>Розділ 6. ЗАГАЛЬНА МОДЕЛЬ ІБ ОРГАНІЗАЦІЇ.....</b>	<b>249</b>
6.1. Вступні зауваження .....	249
6.2. Організаційна модель ІБ .....	250
6.3. Компоненти програми ІБ .....	252
6.4. Управління ІБ на стратегічному рівні.....	253
6.4.1. Розроблення проектів ІБ.....	256
6.4.2. Розроблення програми ІБ.....	258
6.5. Захисні механізми .....	261
6.5.1. Критерій обрання заходів захисту.....	261
6.5.2. Функціональність та ефективність засобів захисту.....	263
6.6. Загальна модель забезпечення ІБ організації .....	264
6.6.1. Проблеми практичної реалізації моделі забезпечення ІБ організації .....	266
Запитання для самоконтролю .....	270
<b>СПИСОК ЛІТЕРАТУРИ.....</b>	<b>271</b>
<b>ДОДАТКИ.....</b>	<b>272</b>
<b>Додаток 1. ПЕРЕЛІК ТИПОВИХ ЗАГРОЗ ІБ</b>	
<b>МІЖНАРОДНОГО СТАНДАРТУ ISO 27001: 2005.....</b>	<b>272</b>
<b>Додаток 2. ПЕРЕЛІК ТИПОВИХ ВРАЗЛИВОСТЕЙ ІБ</b>	
<b>МІЖНАРОДНОГО СТАНДАРТУ ISO 27001: 2005.....</b>	<b>277</b>