ЗМІСТ

Вступ ... 7

Розділ 1. Основні елементи аудиту ІБ організації ... 15
1.1. Загальні зауваження ... 15
1.2. Відповідальність за стан ІБ ... 17
1.3. Основні принципи безпеки ... 19
1.4. Визначення ІБ ... 22
1.5. Особливості аудиту ІБ при ідентифікації подій ІБ ... 25
1.6. Способи класифікації загроз при проведенні аудиту ІБ ... 28
1.6.1. Загрози, що реалізуються за допомогою програмних засобів ... 32
1.6.2. Загрози витоку інформації технічними каналами ... 33
1.6.3. Загрози програмними засобами ... 33
1.6.4. Загрози технічними засобами ... 34
1.7. Побудова профілю та життєвого циклу загрози при проведенні аудиту ІБ ... 35
1.8. Уразливості інформаційних активів ... 37
1.8.1. Ідентифікація уразливостей організаційного рівня при проведенні аудиту ІБ організації ... 39
1.8.2. Ідентифікація технічних уразливостей при проведенні аудиту ІБ організації ... 40
Запитання для самоконтролю ... 41

Розділ 2. Аудит ІБ. Основні поняття, визначення, етапи, види та напрями діяльності ... 42
2.1. Поняття аудиту ІБ, його мета та завдання ... 42
2.2. Програма аудиту ІБ ... 48
2.3. Планування процедури аудиту ІБ ... 49
2.4. Види аудиту ... 54
2.4.1. Активний аудит ... 54
2.4.2. Експертний аудит ... 56
2.4.3. Аудит на відповідність стандартам ... 58
2.5. Поняття комплексного аудиту безпеки інформаційних систем ... 60
2.6. Основні напрями аудиту ІБ ... 64
2.7. Контроль та аналіз аудиторських груп, вимоги до аудиторів ... 65
Запитання для самоконтролю ... 67

Розділ 3. Правові основи аудиту ІБ ... 68
3.1. Загальні зауваження ... 68
3.2. Стандарт «Критерії оцінювання надійності комп'ютерних систем» (Помаранчева книга) ... 72

3.3. Гармонізовані критерії європейських країн ... 80
3.3.1. Основні поняття Загальних критеріїв ... 82
3.3.2. Методологія оцінювання інформаційних технологій за Загальними критеріями ... 90
3.3.3. Оцінювання рівня довіри функціональної безпеки інформаційної технології ... 93
3.3.4. Огляд класів та сімейств Загальних критеріїв ... 97
3.4. Німецький стандарт BSI ... 101
3.5. Британський стандарт BS 7799 ... 103
3.6. Міжнародний стандарт ISO 17799 ... 105
3.7. Стандарт COBIT ... 107
3.8. Стандарти та керівництва, розроблені у межах проєкту SCORE ... 113
3.9. Національні стандарти та керівництва з аудиту ІБ ... 114
3.10. Вплив законодавчих актів та регулятивних норм на розвиток аудиту ІБ ... 115
Запитання для самоконтролю ... 127

Розділ 4. Моделі оцінювання процесів аудиту ІБ ... 128
4.1. Модель оцінювання процесів об'єкта аудиту ... 128
4.2. Точність оцінювання процесів об'єкта аудиту ... 130
4.3. Моделі (алгоритми) обчислення показників ІБ ... 133
4.4. Модель зрілості процесів забезпечення ІБ CMM ... 135
4.5. Модель оцінювання зрілості SSE-CMM ... 139
4.6. Модель оцінювання зрілості COBIT ... 142
4.7. Модель зрілості рейтингової системи URSIT ... 146
4.8. Опис моделі зрілості ... 151
Запитання для самоконтролю ... 155

Розділ 5. Практичний аудит ІБ ... 156
5.1. Аудит ІБ на відповідність міжнародним стандартам ... 156
5.1.1. Аудит ІБ на відповідність міжнародному стандарту ISO/IEC 17799:2000 (BS 7799-1:2000) ... 156
5.1.2. Аудит ІБ на відповідність вимогам Асоціації аудиту та управління інформаційними системами (вимогам стандарту COBIT) ... 164
5.1.2.1. Приклад проведення аудиту ІБ підсистеми розрахунку та видачі заробітної плати ... 168
5.1.3. «Керівництво з аудиту засобів управління федеральних інформаційних систем» GAO/AIMD-12.19.6 ... 176
5.1.3.1. Планування аудиту при застосуванні положень FISCAM ... 178
5.1.3.2. Оцінювання та тестування при застосуванні положень FISCAM ... 182
5.1.3.4. Підсумковий документ аудиту при застосуванні положень FISCAM ... 184

5.1.4. «Керівництво з власного оцінювання безпеки для систем інформаційних технологій» NIST 800-26 ... 185
5.1.5. «Керівництво з метрик безпеки для систем інформаційних технологій» NIST 800-55 ... 190
5.1.6. Схема проведення аудиту ІБ на відповідність вимогам стандарту SysTrust ... 201
5.2. Практичний аудит ІБ. Дослідження (аудит) ІБ та оцінювання результатів аудиту ... 206
5.2.1. Завдання та зміст робіт при проведенні аудиту ІБ корпоративної системи ... 207
5.2.2. Етапи аудиту ІБ ... 211
5.2.2.1. Ініціювання процедури аудиту ... 211
5.2.2.2. Збирання інформації аудиту ... 212
5.2.3. Перелік даних, необхідних для проведення аудиту ІБ ... 218
5.2.4. Алгоритм проведення аудиту ІБ організації ... 222
5.2.5. Аналіз даних аудиту ... 224
5.2.6. Рекомендації з підготовлення звітних документів ... 229
5.2.6.1. Структура звіту за результатами аудиту безпеки інформаційної системи та аналізу ризиків ... 229
5.2.7. Інтерпретація результатів проведення аудиту або власного оцінювання стану ІБ організації ... 236
Запитання для самоконтролю ... 240

Розділ 6. Аудит ІБ корпоративної системи ... 242
6.1. Аудит безпеки зовнішнього периметру корпоративної мережі ... 242
6.1.1. Дослідження зовнішнього периметру мережі на предмет захищеності ... 245
6.2. Аудит виділених приміщень ... 245
6.2.1. Підготовчий етап аудиту виділених приміщень ... 245
6.2.2. Етап безпосереднього проведення аудиту виділених приміщень ... 248
6.2.3. Завершальний етап проведення аудиту виділених приміщень ... 251
6.3. Аудит безпеки окремих об’єктів ІТ-інфраструктури ... 253
6.4. Технічна експертиза продуктів та рішень із забезпечення ІБ ... 253
6.5. Особливості аудиту ІБ організацій, які використовують аутсорсинг ... 254
6.6. Особливості аудиту ІБ у банківській системі ... 260
6.7. Методичні рекомендації НБУ щодо впровадження системи управління ІБ та методики оцінювання ризиків ... 269
Запитання для самоконтролю ... 270

Розділ 7. Програмні продукти для проведення аудиту ІБ ... 271
7.1. Аналіз програмних продуктів для проведення аудиту ІБ ... 271
7.2. Мережеві сканери ... 274

7.3. Метод CRAMM 281
7.4. Система COBRA 287
7.5. Метод RiskWatch 288
Запитання для самоконтролю 289

Розділ 8. Економічне оцінювання забезпечення ІБ 290
8.1. Загальні зауваження 290
8.2. Методика сукупної вартості володіння 291
8.2.1. Основні положення методики 293
Запитання для самоконтролю 300

Список літератури 301

Додатки 302

Додаток 1. Перелік типових загроз інформаційної безпеки міжнародного стандарту ISO 27001: 2005 302

Додаток 2. Перелік типових уразливостей інформаційної безпеки міжнародного стандарту ISO 27001: 2005 308

Додаток 3. Терміни та визначення 311

Додаток 4. Керівництво для проведення аудиту системи менеджменту інформаційної безпеки 324

Додаток 5. Метод CRAMM для проведення аудиту інформаційної безпеки 362