

ЗМІСТ

Передмова	3
-----------------	---

Розділ 1. Інформаційна сфера – основне джерело

інцидентів інформаційної безпеки	11
1.1. Правові та соціальні проблеми інформації	11
1.2. Інформація та відображення матеріального світу	14
1.3. Правові принципи інформаційної безпеки	17
1.4. Правові принципи функціонування організацій	18
1.5. Інформаційна структура організації	20
1.5.1. Інформаційні характеристики організації та природи інцидентів інформаційної безпеки	25
1.6. Ідентифікація інформаційних активів організації	29
1.7. Класифікація інформаційних активів	30
1.8. Опис бізнес-процесів організації	32
1.8.1. Основні бізнес-процеси організації	33
1.8.2. Допоміжні бізнес-процеси організації	34
1.8.3. Механізм ідентифікації та опису бізнес-процесу організації	35
1.8.4. Реєстр інформаційних активів	39
1.9. Ідентифікація вимог безпеки інформаційних активів	41
1.9.1. Реєстр вимог інформаційної безпеки організації	43
1.9.2. Вимоги законодавства та нормативної бази	44
1.9.3. Контрактні зобов'язання	45
1.9.4. Вимоги бізнесу	47
1.10. Цінність інформаційних активів	48
1.10.1. Визначення цінності активів	50
1.11. Збитки та їх негативні наслідки для організації	52
1.11.1. Збитки як категорія класифікації інцидентів інформаційної безпеки	54
1.11.2. Критерії оцінювання збитку	55
Питання для самоконтролю	59

Розділ 2. Основні елементи аналізу та оброблення

інцидентів інформаційної безпеки	60
2.1. Загальні зауваження	60
2.2. Безпека через віру у необізнаність зловмисника	62
2.3. Підхід при запровадженні технології розслідування інцидентів інформаційної безпеки	63
2.4. Відповідальність за стан інформаційної безпеки	64
2.5. Основні принципи безпеки	67
2.6. Фактори виникнення інцидентів інформаційної безпеки	70
2.7. Ідентифікація подій ІБ, які породжують інциденти інформаційної безпеки	72

2.8. Аналіз загроз та вразливостей, які спричиняють інциденти інформаційної безпеки.....	76
2.8.1. Профіль та життєвий цикл загроз, які спричиняють інциденти ІБ.....	77
2.9. Способи класифікації загроз, які спричиняють інциденти інформаційної безпеки.....	80
2.9.1. Інциденти ІБ, що реалізуються за допомогою програмних засобів	84
2.9.2. Інциденти ІБ, що реалізуються при витоці інформації технічними каналами	84
2.9.3. Інциденти ІБ, що реалізуються програмними засобами.....	85
2.9.4. Інциденти ІБ, що реалізуються технічними засобами	85
2.9.5. Інциденти ІБ, пов'язані з персоналом	86
2.9.5.1. Моделювання інцидентів ІБ з боку персоналу	87
2.9.5.2. Приклади інцидентів ІБ, пов'язані з персоналом	91
2.9.5.2.1. <i>Шахрайство системного адміністратора Дурініо</i>	91
2.9.5.2.2. <i>Найбільший витік персональних даних в Японії</i>	93
2.9.5.2.3. <i>Безконтрольний трейдинг у банку Societe Generale</i>	93
2.10. Класифікація вразливостей інформаційних активів, які спричиняють інциденти ІБ.....	94
2.10.1. Ідентифікація вразливостей організаційного рівня	97
2.10.2. Ідентифікація технічних вразливостей	98
2.11. Загальні підходи до оцінювання загроз та вразливостей, які спричиняють інциденти інформаційної безпеки	99
2.12. Оцінювання ризиків ІБ як основа запобігання інцидентам інформаційної безпеки	104
2.13. Кількісний аналіз ризиків, які спричиняють інциденти ІБ.....	105
2.13.1. Кількісне оцінювання ризиків ІБ експертно-аналітичним методом на основі ранжування джерел загроз.....	108
2.13.2. Кількісне оцінювання вразливостей ІБ експертно-аналітичним методом, які спричиняють інциденти інформаційної безпеки	113
2.14. Якісне оцінювання ризиків ІБ, що спричиняють інциденти інформаційної безпеки	114
2.14.1. Калібрування шкали якісного оцінювання ризику ІБ.....	119
2.15. Процес оброблення ризиків ІБ	120
2.16. Способи оброблення ризиків настання інцидентів ІБ.....	124
2.16.1. Прийняття ризиків настання інцидентів ІБ.....	126
2.16.1.1. Критерії прийняття ризиків настання інцидентів ІБ	128
2.16.2. Зменшення значення ризику настання інциденту ІБ.....	129
2.16.3. Передавання ризику настання інциденту ІБ	132
2.16.4. Уникнення ризику настання інциденту ІБ	133
2.17. Механізм оцінювання повернення інвестицій в ІБ від інцидентів ІБ.....	133
Питання для самоконтролю.....	137

Розділ 3. Рекомендації з усунення інцидентів комп'ютерної безпеки

Національного інституту стандартів і технології США (NIST)	138
3.1. Організація служби реагування на інциденти комп'ютерної безпеки	142
3.1.1. Події та інциденти	143

3.1.2. Необхідність реагування на інцидент	143
3.1.3. Створення політики, плану та процедури реагування на інциденти.....	144
3.1.3.1. Політика	144
3.1.3.2. Елементи плану	144
3.1.3.3. Елементи процедури	145
3.1.3.4. Обмін інформацією із сторонніми особами.....	145
3.1.3.4.1. Засоби масової інформації (ЗМІ).....	146
3.1.3.4.2. Правоохоронна діяльність	147
3.1.3.4.3. Організації, які повідомляють про інциденти	148
3.1.3.4.4. Інші зовнішні сторони.....	148
3.1.4. Структура групи реагування на інциденти.....	149
3.1.4.1. Моделі групи	149
3.1.4.2. Вибір моделі групи (команди)	151
3.1.4.3. Персонал з реагування на інциденти.....	153
3.1.4.4. Залежності (підпорядкованості) всередині організацій.....	155
3.1.5. Послуги групи реагування на інциденти	156
3.1.6. Рекомендації.....	156
3.2. Подолання інциденту.....	158
3.2.1. Підготовка	159
3.2.1.1. Підготовка до врегулювання інцидентів	159
3.2.1.2. Запобігання інцидентам	161
3.2.2. Виявлення та аналіз.....	162
3.2.2.1. Категорії інцидентів	162
3.2.2.2. Ознаки інциденту	163
3.2.2.3. Передвісники та ознаки	164
3.2.2.4. Аналіз інциденту	166
3.2.2.5. Документування інциденту	169
3.2.2.6. Встановлення пріоритетності інцидентів.....	170
3.2.2.7. Повідомлення про інцидент	173
3.2.3. Стимування, ліквідація та відновлення	174
3.2.3.1. Обрання стратегії стимування.....	174
3.2.3.2. Збирання та оброблення доказів	175
3.2.3.3. Ідентифікація хостів атаки.....	176
3.2.3.4. Ліквідація та відновлення	177
3.2.4. Діяльність після інциденту	177
3.2.4.1. Отриманий досвід.....	177
3.2.4.2. Використання бази даних про інциденти	179
3.2.4.3. Зберігання доказів	182
3.2.5. Контрольний список для врегулювання інцидентів	182
3.2.6. Рекомендації.....	184
3.3. Додаток А. Сценарії вирішення інцидентів	186
3.3.1. Питання про сценарій.....	187
3.3.2. Сценарії.....	188
3.4. Додаток В. Елементи даних, пов'язані з інцидентом.....	193

3.4.1. Основні дані	194
3.4.2. Дані обробника інцидентів	194
3.5. Додаток С. Глосарій (Терміни)	195
3.6. Додаток D. Кроки врегулювання кризи	198

Розділ 4. Розроблення політики реагування

на інциденти інформаційної безпеки	200
4.1. Політика інформаційної безпеки	200
4.2. Визначення та види політики інформаційної безпеки.....	202
4.3. Види політик інформаційної безпеки.....	207
4.3.1. Дискреційна (розмежувальна) політика інформаційної безпеки.....	207
4.3.2. Мандатна політика інформаційної безпеки.....	209
4.3.3. Рольова політика інформаційної безпеки	213
4.4. Основні причини створення політик інформаційної безпеки	215
4.5. Розроблення політик інформаційної безпеки	218
4.5.1. Складнощі впровадження політик інформаційної безпеки.....	219
4.5.2. Склад групи з розроблення політик інформаційної безпеки	220
4.5.3. Процес розроблення політик інформаційної безпеки	220
4.5.4. Основні вимоги до політики інформаційної безпеки	222
4.6. Приклади політик інформаційної безпеки.....	223
4.7. Варіанти політик інформаційної безпеки організацій	226
4.7.1. Металургійна компанія	226
4.7.2. Комерційний банк.....	229
4.8. Політики, рекомендовані Інститутом SANS.....	232
4.8.1. Політика допустимого шифрування	232
4.8.2. Політика допустимого використання	233
4.8.3. Політика антивірусного захисту.....	237
4.8.4. Політика зберігання електронної пошти	238
4.8.5. Політика використання електронної пошти	239
4.8.6. Політика використання паролів.....	240
4.8.7. Політика оцінювання ризиків ІБ	244
4.8.8. Політика інформаційної безпеки маршрутизатора.....	244
4.8.9. Політика забезпечення інформаційної безпеки серверів	245
4.8.10. Політика віртуальних приватних мереж.....	247
4.8.11. Політика безпроводного доступу до мережі організації.....	249
4.8.12. Політика автоматичного переадресування електронної пошти	250
4.8.13. Політика класифікації інформації	250
4.8.14. Політика паролів доступу до баз даних	255
4.8.15. Політика інформаційної безпеки сегменту демілітаризованої зони	256
4.8.16. Політика інформаційної безпеки внутрішнього сегменту	260
4.8.17. Політика екстранету	263
4.8.18. Кодекс етики	264
4.8.19. Політика антивірусного захисту.....	266
Питання для самоконтролю	267

Розділ 5. Система управління інцидентами інформаційної безпеки як основа технології розслідування інцидентів ІБ	268
5.1. Алгоритм запровадження системи управління інцидентами ІБ	268
5.2. Процес розслідування інцидентів інформаційної безпеки	273
5.2.1. Оцінювання сфери розслідування	273
5.2.1.1. Ініціювання розслідування	273
5.2.1.2. Перевірка політики інформаційної безпеки та нормативних документів ІБ	274
5.2.1.3. Визначення інструментів для проведення розслідування	276
5.2.2. Збирання	277
5.2.2.1. Збирання, збереження і архівування доказів	277
5.2.3. Дослідження	277
5.2.4. Аналіз	278
5.2.5. Відображення (Систематизація даних і формування звіту)	279
5.3. Висновки	279
Питання для самоконтролю	280
Список використаної літератури	281
Додатки	283
Додаток 1. Перелік типових загроз інформаційної безпеки міжнародного стандарту ISO 27001: 2005	283
Додаток 2. Перелік типових вразливостей інформаційної безпеки міжнародного стандарту ISO 27001: 2005	288
Додаток 3. Метод оцінювання ризиків настання інцидентів ІБ CRAMM і листи опитування для оцінювання загроз та вразливостей, які спричиняють інциденти ІБ, та ступеня критичності систем	291
Д.3.1. Метод CRAMM для оцінювання ризиків настання інцидентів ІБ	291
Д.3.2. Лист-опитування для оцінювання загроз за методом CRAMM, що спричинили інциденти ІБ	292
Д.3.3. Лист-опитування для оцінювання вразливостей за методом CRAMM, використаних для реалізації інцидентів ІБ	307
Д.3.4. Базовий перелік питань для визначення методом CRAMM ступеня критичності систем при настанні інциденту ІБ	320
Додаток 4. Методичні вказівки для виконання комплексної лабораторної роботи «Розроблення технології розслідування інцидентів інформаційної безпеки підприємства «.....»	322
Додаток 5. Методичні вказівки для виконання комплексної лабораторної/практичної роботи «Аналіз ризиків та інцидентів інформаційної безпеки підприємства «.....»	327