

ЗМІСТ

Вступ.....	3
Розділ 1. Міжнародні стандарти у сфері менеджменту інформаційної безпеки	7
1.1. Сімейство міжнародних стандартів у сфері менеджменту інформаційної безпеки та їх історія	7
1.2. Міжнародний стандарт ISO/IEC 27001 “Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Вимоги”	9
1.2.1. Характеристика стандарту.....	9
1.2.2. Процесний підхід до створення систем менеджменту інформаційної безпеки.....	10
1.2.3. Структура та сфера застосування стандарту ISO/IEC 27001.....	12
1.2.4. Система менеджменту інформаційної безпеки. Загальні вимоги	16
1.3. Впровадження сімейства міжнародних стандартів ISO/IEC 27000 в організаціях України.....	24
1.4. Алгоритм впровадження системи менеджменту інформаційної безпеки на відповідність вимогам міжнародного стандарту ISO/IEC 27001	28
1.5. Документація системи менеджменту інформаційної безпеки за вимогами стандарту ISO/IEC 27001	31
1.6. Коротка характеристика стандарту ISO/IEC 27002 “Інформаційні технології. Звід правил з управління захистом інформації”	35
1.6.1. Структура та сфера застосування стандарту.....	35
1.6.2. Основні категорії захисту інформації.....	36
1.6.3. Оцінювання та оброблення ризиків	36
1.6.4. Політика у сфері захисту інформації.....	38
Запитання для самоперевірки	40
Розділ 2. Організація захисту інформації.....	41
2.1. Організація внутрішнього захисту інформації.....	41
2.1.1. Зобов’язання керівництва щодо захисту інформації.....	41
2.1.2. Координація захисту інформації.....	42
2.1.3. Розмежування обов’язків щодо захисту інформації	42
2.1.4. Процес отримання дозволу для засобів оброблення інформації.....	43
2.1.5. Угоди про конфіденційність.....	43
2.1.6. Контакти зі спеціальними службами.....	44
2.1.7. Контакти зі спеціальними групами.....	45
2.1.8. Незалежний аналіз захисту інформації	45
2.1.9. Підтримання контакту із зовнішніми сторонами	46
2.2. Менеджмент засобів зв’язку та операцій.....	46
2.3. Менеджмент змін	47

2.3.1. Розмежування обов'язків	48
2.3.2. Розмежування засобів розроблення, випробування та експлуатацію	48
2.4. Менеджмент надання послуг третьої сторони	49
2.4.1. Надання послуг	50
2.4.2. Постійний контроль і аналіз послуг третьої сторони	50
2.4.3. Менеджмент змін у послугах третьої сторони	51
2.4.4. Планування реалізації та приймання системи	51
2.5. Менеджмент продуктивності	52
2.6. Приймання системи	52
2.7. Резервне копіювання інформації	53
2.8. Менеджмент захисту мереж зв'язку	54
2.8.1. Засоби керування мережею зв'язку	54
2.8.2. Захист мережевих послуг	55
2.9. Використання носіїв інформації	55
2.9.1. Менеджмент змінних носіїв інформації	56
2.9.2. Ліквідація носіїв інформації	56
2.9.3. Процедури використання інформації	57
2.9.4. Захист системної документації	57
2.10. Політика і процедури обміну інформацією	58
2.11. Угоди про обмін інформацією	60
2.11.1. Фізичні носії під час транспортування	61
2.11.2. Електронний обмін повідомленнями	61
2.11.3. Інформаційні системи для організацій	62
2.12. Послуги електронної торгівлі	63
2.12.1. Електронна торгівля	63
2.12.2. Он-лайн угоди	64
2.12.3. Загальнодоступна інформація	65
2.13. Постійний контроль	65
2.13.1. Ведення контрольного журналу	65
2.13.2. Постійний контроль використання систем	66
2.13.3. Захист даних системного журналу	67
2.13.4. Журнали оператора та адміністратора	68
2.13.5. Реєстрація відмов	68
2.14. Менеджмент інцидентів у системі захисту інформації	68
2.14.1. Складання звітів про події в системі захисту інформації	69
2.14.2. Складання звітів про недоліки захисту	70
2.15. Менеджмент інцидентів і вдосконалень системи захисту інформації	70
2.15.1. Обов'язки і процедури	70
2.15.2. Висновки з інцидентів в системі захисту інформації	72
Запитання для самоперевірки	72

Розділ 3. Ризик-менеджмент за вимогами міжнародного стандарту ISO/IEC 27001	73
3.1. Особливості впровадження ризик-менеджменту	73
3.1.1. ЕТАП 1. Опис активу	74
3.1.2. ЕТАП 2. Опис ризику	75
3.1.3. ЕТАП 3. Первісне оцінювання ризику	76
3.1.4. ЕТАП 4. Визначення цільового показника та заходів з оброблення ризику	78
3.1.5. ЕТАП 5. Повторне оцінювання ризику	80
3.1.6. ЕТАП 6. Перегляд усього процесу ризик-менеджменту	81
3.2. Визначення рівня відповідності систем менеджменту інформаційної безпеки міжнародному стандарту ISO/IEC 27001	82
Запитання для самоперевірки	89
Розділ 4. Структура і методика реалізації системи інцидент-менеджменту	91
4.1. Система менеджменту інцидентів	91
4.2. Переваги впровадження інцидент-менеджменту	93
4.3. Організація інцидент-менеджменту в організації	94
4.4. Етапи управління інцидентами	95
4.4.1. Виявлення інциденту	96
4.4.2. Інформування про виникнення інциденту	97
4.4.3. Реєстрація інциденту	99
4.4.4. Усунення наслідків інциденту	100
4.4.5. Розслідування інциденту	101
4.4.6. Реалізація дій, що унеможливають повторне виникнення інциденту	102
4.4.7. Аналіз інцидентів за певний період	103
4.4.8. Аналіз процесу інцидент-менеджменту	104
4.5. Взаємозв'язок інцидент-менеджменту та ризик-менеджменту	105
Запитання для самоперевірки	106
Розділ 5. Планування впровадження систем менеджменту інформаційної безпеки	107
5.1. Впровадження системи менеджменту інформаційної безпеки за вимогами стандарту ISO/IEC 27001	107
5.2. План робіт з доопрацювання СМІБ відповідно до вимог стандарту ISO/IEC 27001	109
5.3. Оптимізація оперативних планів	110
5.4. Виконання робіт за розділами стандарту	111
5.5. Виконання робіт відповідно до видів діяльності	111
5.6. Підготовка зведеного плану	112
5.7. Врахування підходу ДСТУ ISO/IEC TR 13335:2003	114
Запитання для самоперевірки	123

Розділ 6. Аудит систем менеджменту інформаційної безпеки	125
6.1. Становлення процесу аудиту систем менеджменту інформаційної безпеки....	125
6.2. Усвідомлення аудиту системи менеджменту інформаційної безпеки	129
6.3. Правові основи аудиту систем менеджменту інформаційної безпеки	135
6.4. Види аудиту систем менеджменту інформаційної безпеки	138
6.5. Модель об'єкта аудиту	146
6.6. Аудит систем менеджменту інформаційної безпеки згідно з міжнародним стандартом ISO 19011	149
6.6.1. Сфера застосування та принципи здійснення аудиту згідно з міжнародним стандартом ISO 19011	149
6.6.2. Управління програмою аудиту.....	150
6.6.3. Цілі та обсяг програми аудиту.....	152
6.6.4. Відповідальність за програму аудиту, ресурси та методики програми аудиту	154
6.7. Аудиторська діяльність	156
6.7.1. Початок аудиту	158
6.7.2. Аналіз документів.....	160
6.7.3. Підготовка до аудиторської діяльності на місцях	160
6.7.4. Здійснення аудиторської діяльності на місцях	162
6.7.5. Підготовка, схвалення та розсилання звіту про аудит	167
6.7.6. Завершення та виконання дій після аудиту.....	168
6.8. Компетентність та оцінювання аудиторів.....	168
6.9. Комплексний аудит системи менеджменту інформаційної безпеки	182
6.10. Сертифікаційний QSA-аудит за методикою PCI DSS.....	195
Запитання для самоперевірки	196
Терміни та визначення	198
Список літератури	202
Додаток А	205
Додаток Б.....	220
Додаток В	224