

ЗМІСТ

ВСТУП	13
ПЕРЕЛІК АБРЕВІАТУР	15

I Основи управління інформаційною безпекою	19
---	-----------

Розділ 1. Теоретичні основи та підходи до побудови системи управління інформаційною безпекою організації	20
1.1. Визначення поняття система. Системний підхід	20
1.2. Визначення поняття процес. Процесний підхід	23
1.3. Визначення поняття управління. Менеджмент та управління . . .	26
1.4. Циклічна модель покращення процесів	27
1.5. Системний підхід до управління організацією	29
1.6. Процесний підхід до управління організацією	30
Висновки	31
Питання та практичні завдання до розділу 1	32

Розділ 2. Основні напрямки розвитку менеджменту у сфері інформаційної безпеки	33
--	-----------

2.1. Основи організаційної та управлінської роботи у сфері інформаційної безпеки	33
2.1.1. Мета, завдання, передумови та напрямки організаційної і управлінської роботи у сфері інформаційної безпеки	33
2.1.2. Основний зміст і особливості організаційної роботи на рівнях організації інформаційної безпеки	37
2.2. Основні напрямки розвитку менеджменту у сфері інформаційної безпеки на міжнародному рівні	38
2.2.1. Діяльність міжнародних організацій у сфері інформаційної безпеки	38
2.2.2. Діяльність спеціалізованих міжнародних організацій у сфері інформаційної безпеки	41
2.2.3. Управління інформаційною безпекою на рівні потужних постачальників інформаційних систем	41
Висновки	43
Питання та практичні завдання до розділу 1	45

Розділ 3. Управління інформаційною та кібербезпекою на державному рівні	46
3.1. Передумови розвитку державного управління у сфері інформаційної безпеки	46
3.2. Управління інформаційною безпекою в Україні	50
3.2.1. Роль Держспецзв'язку в управлінні інформаційною безпекою в Україні	50
3.2.2. Основні функції системи забезпечення інформаційної безпеки України	52
3.2.3. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України	53
3.2.4. Основні положення політики забезпечення інформаційної безпеки України	56
3.2.5. Національна система кібербезпеки	59
3.2.6. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA	66
3.2.7. Взаємодія у сфері кібербезпеки	67
Висновки	69
Питання та практичні завдання до розділу 3	69
Розділ 4. Основи управління інформаційною безпекою на рівні організації	70
4.1. Передумови розвитку управління у сфері інформаційної безпеки на рівні організацій	70
4.2. Формування політики інформаційної безпеки в організації	72
4.2.1. Загальні положення щодо формування політики інформаційної безпеки організації	72
4.2.2. Політика інформаційної безпеки верхнього рівня	74
4.2.3. Політики інформаційної безпеки середнього рівня	75
4.2.4. Основний зміст розділів політики безпеки за окремими напрямками захисту інформації	78
4.2.5. Організація режиму секретності в установах і організаціях	81
4.2.6. Політики використання Інтернет та локальних і корпоративних мереж	83
4.2.7. Політика інформаційної безпеки організації: нижній рівень	86
4.3. Організація роботи органу інформаційної безпеки	86
4.3.1. Функції, пов'язані з формуванням, підтримкою і документальним забезпеченням політики інформаційної безпеки	87
4.3.2. Функції, пов'язані з впровадженням засобів захисту інформації	88
4.3.3. Функції, пов'язані з адмініструванням інформаційних систем і систем захисту інформації	89
4.3.4. Функції, пов'язані з контролем виконання вимог політики інформаційної безпеки та проведенням аудитів	90
4.3.5. Функції, пов'язані з охороною організації	90
4.4. Життєвий цикл політики ІБ	91

4.4.1.	Розробка політики ІБ	92
4.4.2.	Впровадження політики ІБ	95
4.4.3.	Застосування політики ІБ	96
4.4.4.	Анулювання політики ІБ	99
4.5.	Відповідальність за політику ІБ	100
4.6.	Організаційна структура та персонал департаменту інформаційної безпеки	105
4.6.1.	Основні положення щодо організаційної структури департаменту інформаційної безпеки	105
4.6.2.	Робота з персоналом організації	106
4.6.3.	Реагування на виникаючі надзвичайні ситуації (інциденти), пов'язані з порушенням інформаційної безпеки	109
4.6.4.	Інциденти, причиною яких є навмисно здійснювані напади на інформаційні ресурси організації	110
4.6.5.	Аудит стану інформаційної безпеки в організації	116
	Висновки	124
	Питання та практичні завдання до розділу 4	125

Розділ 5. Стандартизація систем та процесів управління інформаційною безпекою організації **127**

5.1.	Основна модель стандартизації систем та процесів управління інформаційною безпекою організації	127
5.1.1.	Модель системи управління якістю, з основу якої покладено процес відповідно до ISO 9001	127
5.1.2.	Стандарти управління інформаційною безпекою серії ISO/IEC 27k Інформаційні технології. Методи захисту. Система управління інформаційною безпекою	131
5.2.	Основні моделі стандартизації процесів управління інформаційною безпекою та оцінки рівня безпеки	134
5.2.1.	Огляд систем управління інформаційної безпеки	135
5.2.1.1.	Загальні положення	135
5.2.1.2.	Сутність СУІБ	136
5.2.1.3.	Система управління	138
5.2.1.4.	Процесний підхід	138
5.2.1.5.	Важливість СУІБ	139
5.2.2.	Створення, моніторинг, підтримка та вдосконалення СУІБ	140
5.2.2.1.	Основні положення	140
5.2.2.2.	Визначення вимог до інформаційної безпеки	140
5.2.2.3.	Оцінка ризиків інформаційної безпеки	141
5.2.2.4.	Обробка ризиків інформаційної безпеки	142
5.2.2.5.	Вибір і впровадження елементів управління	142
5.2.2.6.	Моніторинг, підтримка та підвищення ефективності СУІБ	144
5.2.2.7.	Постійне вдосконалення	144
5.2.3.	Критичні чинники успішності СУІБ	144
5.2.4.	Переваги стандартів СУІБ	145

5.2.5.	Моделі сімейства стандартів СУІБ	146
5.2.5.1.	Загальна інформація	146
5.2.5.2.	Стандарт, що описує огляд і термінологію	146
5.2.5.3.	Стандарти, що визначають вимоги	147
5.2.5.4.	Стандарти, що описують загальні вказівки	149
5.2.5.5.	Стандарти, що описують специфічні для сектора принципи	154
5.2.5.6.	Стандарти з рекомендаціями для спеціальних засо- бів управління серії 2703x	159
5.2.5.7.	Стандарти з рекомендаціями для спеціальних засо- бів управління серії 2704x	172
5.2.5.8.	Інші стандарти з рекомендаціями для спеціальних засобів управління	175
5.3.	Взаємозв'язок стандартів при застосуванні для управління інфор- маційною безпекою в організаціях	189
5.3.1.	Загальні та основні нормовані вимоги до СУІБ	189
5.3.2.	Галузеве застосування ISO/IEC 27001	192
5.3.3.	Звід правил та основні розширення	194
5.3.4.	Управління ризиками	195
5.3.5.	Сертифікація та оцінка відповідності	196
	Висновки	198
	Питання та практичні завдання до розділу 5	198

II Основи побудови системи і основних підсистем управ- ління інформаційною безпекою та кібербезпекою органі- зації **200**

Розділ 6. Управління і система управління інформаційною безпе- кою організації **201**

6.1.	Основні вимоги щодо побудови системи управління інформаційною безпекою	201
6.1.1.	Загальні вимоги до системи управління інформаційною без- пекою відповідно до стандарту ДСТУ ISO/IEC 27001: 2023	201
6.1.2.	Зміст основних елементів структури стандарту ДСТУ ISO/IEC 27001:2023	202
6.1.2.1.	Контекст організації [context of the organization]	202
6.1.2.2.	Лідерство [leadership]	203
6.1.2.3.	Планування [planning]	205
6.1.2.4.	Підтримка [support]	207
6.1.2.5.	Функціонування [operation]	209
6.1.2.6.	Оцінка результатів діяльності [performance evaluation]	209
6.1.2.7.	Покращення [improvement]	211
6.2.	Завдання і елементи управління інформаційною безпекою	211
6.2.1.	Організаційні елементи управління [organizational controls]	212

6.2.2.	Елементи управління персоналом [People controls]	216
6.2.3.	Фізичні елементи управління [Physical controls]	218
6.2.4.	Технологічні елементи управління [Technological controls]	219
6.3.	Рекомендації щодо вибору елементів управління інформаційною безпекою	222
6.3.1.	Загальні положення стандарту ДСТУ ISO/IEC 27002:2023	222
6.3.2.	Передумови та контекст [background and context]	223
6.3.3.	Вимоги до безпеки інформації [information security requirements]	224
6.3.4.	Елементи управління [controls]	224
6.3.5.	Визначення елементів управління [determining controls]	225
6.3.6.	Розробка інструкцій для конкретної організації [developing organization-specific guidelines]	225
6.3.7.	Розгляд життєвого циклу [life cycle considerations]	226
6.3.8.	Відповідні міжнародні стандарти [related International Standards]	226
6.4.	Зміст основних елементів структури стандарту ДСТУ ISO/IEC 27002:2023	227
6.4.1.	Пункти [clauses]	227
6.4.2.	Теми і атрибути [themes and attributes]	228
6.4.3.	Схема елемента управління [control layout]	233
6.5.	Загальні рекомендації щодо побудови системи управління інформаційною безпекою	234
6.5.1.	Визначення структури системи процесів управління інформаційною безпекою	234
6.5.2.	Основні напрями автоматизації процесів управління інформаційною безпекою організації	238
6.5.3.	Автоматизація процесів управління інформаційною безпекою на довільній платформі	240
	Висновки	241
	Питання та практичні завдання до розділу 6	242
Розділ 7.	Упровадження процесного підходу для побудови системи управління інформаційною безпекою організації	244
7.1.	Основи ідентифікації та опису бізнес процесів	244
7.1.1.	Загальні положення щодо ідентифікації інформаційних активів/ресурсів	244
7.1.2.	Особливості опису типових основних і допоміжних бізнес-процесів	245
7.1.2.1.	Основні бізнес-процеси організації	245
7.1.2.2.	Допоміжні процеси організації	246
7.1.3.	Ідентифікація і опис бізнес-процесів	247
7.1.3.1.	Основні характеристики бізнес-процесів	247
7.1.3.2.	Перелік питань та оформлення результатів опитування	249
7.1.3.3.	Реєстр інформаційних активів	251

7.2. Порядок та процедури інвентаризації, класифікації та оцінки критичності інформаційних активів/ресурсів організації	253
7.2.1. Процедури інвентаризації інформаційних активів/ресурсів	253
7.2.1.1. Загальні рекомендації щодо реалізації процедур інвентаризації інформаційних активів/ресурсів	253
7.2.1.2. Процедура реалізації підготовчого етапу інвентаризації інформаційних активів/ресурсів	254
7.2.1.3. Процедура реалізації етапу збирання відомостей щодо інформаційних активів/ресурсів	255
7.2.1.4. Процедура формування відомості інформаційних активів/ресурсів у частині опису процесу діяльності організації та встановлення власника процесу	255
7.2.1.5. Процедура формування відомості інформаційних активів/ресурсів у частині опису інформаційних активів/ресурсів	257
7.2.1.6. Процедура формування відомості інформаційних активів/ресурсів у частині встановлення власника інформаційного активу/ресурсу	257
7.2.1.7. Рекомендації щодо реалізації процедури детальної інвентаризації за допомогою автоматизованих програм	258
7.2.2. Процедури класифікації інформаційних активів/ресурсів	258
7.2.2.1. Процедура загальної класифікації інформаційних активів/ресурсів	258
7.2.2.2. Процедура детальної класифікації інформаційних активів/ресурсів	259
7.2.3. Процедура оцінки критичності інформаційних активів/ресурсів	261
Висновки	263
Питання та практичні завдання до розділу 7	264
Розділ 8. Підсистема управління ризиками інформаційної безпеки	265
8.1. Нормативне забезпечення управління ризиками інформаційної безпеки	265
8.1.1. Основні стандарти	265
8.1.2. Основні стандартизовані визначення необхідні для створення підсистеми управління ризиком	270
8.2. Управління ризиками інформаційної безпеки СУІБ	276
8.2.1. Складові процесу управління ризиками інформаційної безпеки	276
8.2.2. Цикли управління ризиками інформаційної безпеки	277
8.3. Встановлення контексту управління ризиками інформаційної безпеки організації	278
8.3.1. Міркування щодо значення організації	278
8.3.2. Визначення основних вимог зацікавлених сторін	278
8.3.3. Застосування оцінки ризику	279

8.3.4.	Встановлення та підтримка критеріїв ризику інформаційної безпеки	280
8.3.4.1.	Загальні положення	280
8.3.4.2.	Критерії прийнятності ризику	280
8.3.5.	Критерії для виконання оцінки ризиків інформаційної безпеки	283
8.3.5.1.	Загальні положення	283
8.3.5.2.	Критерії наслідків	283
8.3.5.3.	Критерії правдоподібності	285
8.3.5.4.	Критерії визначення рівня ризику	286
8.3.6.	Вибір відповідного методу	287
8.4.	Аналіз ризиків інформаційної безпеки	288
8.4.1.	Загальні положення	288
8.4.2.	Оцінка потенційних наслідків	288
8.4.3.	Оцінка ймовірності	289
8.4.4.	Визначення рівнів ризику	292
8.5.	Оцінка ризиків інформаційної безпеки	292
8.5.1.	Порівняння результатів аналізу ризику з критеріями ризику	292
8.5.2.	Пріоритезація проаналізованих ризиків для обробки ризиків	293
8.6.	Процес обробки ризиків інформаційної безпеки	294
8.6.1.	Загальні положення	294
8.6.2.	Вибір відповідних варіантів	295
8.6.3.	Визначення всіх заходів управління, необхідних для впро- вадження варіантів обробки ризиків інформаційної безпеки	296
8.6.4.	Порівняння засобів управління, визначених у ISO/IEC 27001:2022, додаток А	300
8.6.5.	Підготовка заяви про застосовність	301
8.7.	План обробки ризиків інформаційної безпеки	302
8.7.1.	Формулювання плану обробки ризиків	302
8.7.2.	Схвалення власниками ризиків	304
8.7.3.	Прийняття залишкових ризиків інформаційної безпеки . . .	305
8.8.	Робота	306
8.8.1.	Виконання процесу оцінки ризиків інформаційної безпеки .	306
8.8.2.	Виконання процесу обробки ризиків інформаційної безпеки	307
8.9.	Використання пов'язаних процесів СУІБ	307
8.9.1.	Контекст організації	307
8.9.2.	Лідерство та відданість справі	309
8.9.3.	Спілкування та консультації	309
8.9.4.	Задokumentована інформація	312
8.9.4.1.	Загальні положення	312
8.9.4.2.	Документована інформація про процеси	312
8.9.4.3.	Задokumentована інформація про результати	313
8.9.5.	Моніторинг та огляд	314
8.9.5.1.	Загальні положення	314
8.9.5.2.	Моніторинг та аналіз факторів, що впливають на ризик	315
8.9.6.	Аналіз керівництвом	316

8.9.7. Коригувальні дії	317
8.9.8. Постійне вдосконалення	317
Висновки	319
Питання та практичні завдання до розділу 8	320

Розділ 9. Управління інцидентами інформаційної безпеки та неперервністю бізнесу 322

9.1. Нормативна база щодо управління інцидентами інформаційної безпеки та неперервністю бізнесу	323
9.1.1. Перелік основних стандартів	323
9.1.2. ISO/IEC 27035:2020–2023 — управління інцидентами інформаційної безпеки	324
9.1.3. ISO/IEC 27037 — посібник з ідентифікації, збору та/або отримання та забезпечення безпеки свідочств, поданих в електронній формі	330
9.1.4. ISO/IEC 27031:2011 — посібник з готовності інформаційних та телекомунікаційних технологій для забезпечення неперервності бізнесу	333
9.1.5. ISO 22300 — менеджмент неперервності бізнесу	336
9.2. Управління інцидентами інформаційної безпеки	338
9.2.1. Подія та інцидент інформаційної безпеки	340
9.2.2. Цілі і завдання управління інцидентами інформаційної безпеки	343
9.2.3. Діяльність в рамках управління інцидентами інформаційної безпеки	345
9.2.4. Етапи процесу управління інцидентами ІБ	348
9.2.4.1. Планування і підготовка процесу управління інцидентами ІБ	350
9.2.4.2. Використання системи управління інцидентами ІБ	351
9.2.4.3. Аналіз процесу управління інцидентами ІБ	353
9.2.4.4. Покращення процесу управління інцидентами ІБ	355
9.2.5. Виявлення подій ІБ та інцидентів ІБ та оповіщення про них	356
9.2.6. Обробка подій ІБ та інцидентів ІБ	358
9.2.6.1. Перша оцінка і попереднє рішення з подій ІБ	359
9.2.6.2. Друга оцінка і підтвердження інциденту ІБ	363
9.2.7. Реагування на інциденти ІБ	364
9.2.8. Негайне реагування на інциденти	365
9.2.9. Управління реагуванням на інцидент ІБ	369
9.2.10. Наступне реагування на інцидент	369
9.2.11. Антикризовані дії	370
9.2.12. Правова експертиза інцидентів ІБ	371
9.2.13. Розширення області прийняття рішень	376
9.2.14. Реєстрація діяльності і управління внесенням змін	376
9.2.15. Технічна підтримка реагування на інциденти ІБ	376
9.2.16. Документація системи управління інцидентами ІБ	378
9.2.16.1. Політика управління інцидентами ІБ	380

9.2.16.2.	Програма управління інцидентами ІБ	381
9.2.17.	Група реагування на інциденти ІБ	386
9.2.18.	Забезпечення обізнаності та навчання в галузі інцидентів ІБ	392
9.2.19.	Збереження доказів інциденту ІБ	393
9.2.20.	Засоби управління подіями ІБ	398
9.3.	Підсистема управління неперервністю діяльності організації	401
9.3.1.	Основні визначення щодо неперервності діяльності організації	404
9.3.2.	Основні положення щодо підсистеми управління неперервністю бізнесу	405
9.3.3.	Життєвий цикл управління неперервністю бізнесу	407
9.3.3.1.	Управління програмою УНБ	408
9.3.3.2.	Аналіз неперервності бізнесу організації	412
9.3.3.3.	Визначення стратегії УНБ	417
9.3.3.4.	Розробка та впровадження в УНБ заходів і відповідей на інциденти	423
9.3.3.5.	Заходи зі застосування, підтримки та аналізу УНБ	427
9.3.3.6.	Упровадження УНБ в культуру організації	436
9.3.4.	Документація і записи у галузі неперервності бізнесу	438
9.3.4.1.	Політика УНБ	439
9.3.4.2.	Плани управління інцидентом, забезпеченням неперервності бізнесу і відновленням бізнесу	441
9.3.5.	Засоби управління неперервністю бізнесу	453
	Висновки	453
	Питання та практичні завдання до розділу 9	455

Розділ 10.Перевірка й оцінка системи управління інформаційною безпекою організації	457
10.1. Основні поняття та нормативно-правове забезпечення аудиту	457
10.2. Процес аудиту	459
10.2.1. Загальні положення	459
10.2.2. Принципи проведення аудиту	460
10.2.3. Управління програмою аудиту	463
10.2.3.1. Загальні положення	463
10.2.3.2. Встановлення цілей програми аудиту	464
10.2.3.3. Визначення та оцінювання ризиків і можливостей програми аудиту	466
10.2.3.4. Формування програми аудиту	467
10.2.3.5. Виконання програми аудиту	470
10.2.3.6. Моніторинг програми аудиту	473
10.2.3.7. Аналіз та поліпшення програми аудиту	474
10.2.4. Проведення аудиту	475
10.2.4.1. Загальні положення	475
10.2.4.2. Розпочинання аудиту	475
10.2.4.3. Підготування до аудиторської діяльності	476
10.2.4.4. Виконання аудиторської діяльності	480

10.2.4.5. Підготовка та подання звіту про аудит	487
10.2.4.6. Завершення аудиту	488
10.2.4.7. Виконання подальших дій за результатами аудиту	489
10.2.5. Компетентність та оцінювання аудиторів	489
10.2.5.1. Загальні положення	489
10.2.5.2. Визначення компетентності аудиторів	490
10.2.5.3. Особисті якості	490
10.2.5.4. Знання та навички	491
10.2.5.5. Набуття аудиторської компетентності	495
10.2.5.6. Набуття компетентності керівника групи аудиту	495
10.2.5.7. Установлення критеріїв оцінювання аудитора	496
10.2.5.8. Вибірання належного методу оцінювання аудитора	496
10.2.5.9. Оцінювання аудитора	497
10.2.5.10. Підтримування та поліпшення компетентності аудиторів	497
10.3. Оцінювання інформаційної безпеки	497
10.3.1. Передумови оцінювання	499
10.3.2. Огляд оцінок елементів управління інформаційної безпеки	500
10.3.2.1. Процес оцінювання	500
10.3.2.2. Ресурси та компетентність	504
10.3.3. Методи огляду	506
10.3.3.1. Огляд	506
10.3.3.2. Аналіз процесу	507
10.3.3.3. Техніка обстеження	508
10.3.3.4. Тестування методів перевірки	509
10.3.3.5. Техніка відбору проб	512
10.3.4. Особливості підготовки до контрольного оцінювання	512
Висновки	514
Питання та практичні завдання до розділу 10	515
СЛОВНИК БАЗОВИХ ТА ДОДАТКОВИХ ТЕРМІНІВ І ПО- НЯТЬ	516
ПРЕДМЕТНИЙ ПОКАЖЧИК	531
ЛІТЕРАТУРА	537

Додатки до посібника за посиланням



ВСТУП

У навчальному посібнику наведена систематизована сукупність відомостей про стан і перспективи розвитку широкого кола методологічних, наукових і технічних основ управління інформаційною безпекою та кібербезпекою, процесів створення й функціонування системи управління інформаційною безпекою та кібербезпекою організації, її основних підсистем, методів, засобів і елементів управління інформаційною безпекою.

Навчальний посібник створений за результатами детального аналітичного вивчення та практичного застосування сучасної міжнародної та національної нормативно-правової бази щодо управління інформаційною безпекою та кібербезпекою на міжнародному, державному рівні та на рівні організації.

Посібник складається з двох частин і десяти розділів. У першій частині посібника сформульовані теоретичні основи та підходи до побудови систем управління інформаційною безпекою організації, здійснений аналіз основних напрямів розвитку менеджменту у сфері інформаційної безпеки на міжнародному рівні. Сформульовані загальні підходи щодо управління інформаційною безпекою та кібербезпекою на рівні організацій. Показано, що ефективне забезпечення кіберзахисту здійснюється в організаціях, де створена система управління інформаційною безпекою.

Теоретичні основи до побудови системи управління інформаційною безпекою засновуються на системному та процесному підходах, що призводить до застосування циклічної моделі покращення процесів, на основі якої запропонована основна модель стандартизації систем та процесів управління інформаційною безпекою та кібербезпекою, яка ґрунтується на ризик-орієнтованому підході.

У посібнику наведений опис основних моделей стандартизації процесів управління безпекою та оцінки рівня безпеки, які реалізовані у стандартах управління інформаційною безпекою серії ISO/IEC 27k Інформаційна безпека, кібербезпека та захист конфіденційності (раніше — інформаційні технології). Система управління інформаційною безпекою.

У другій частині посібника викладені методологічні основи побудови системи і основних підсистем управління інформаційною безпекою та кібербезпекою організації. Детально розглянуті загальні вимоги до сис-

теми управління інформаційною безпекою відповідно до стандарту ДСТУ ISO/IEC 27001: 2023 [45] та сформульовані загальні рекомендації щодо побудови системи управління інформаційною безпекою, у тому числі щодо автоматизації процесів управління інформаційною безпекою організації.

Наведені основні підходи щодо впровадження процесного підходу для побудови системи управління інформаційною безпекою організації, що, насамперед, передбачають ідентифікацію та опис бізнес-процесів, а також інвентаризацію, класифікацію та оцінку критичності інформаційних активів/ресурсів організації.

Визначені загальні підходи до побудови наступних підсистем системи управління інформаційною безпекою: підсистеми управління ризиками, підсистеми управління інцидентами, підсистеми управління неперервністю діяльності організації, а також підсистеми перевірки й оцінки системи управління інформаційною безпекою організації, що включає у себе порядок і процеси аудиту інформаційної безпеки та підходи до оцінювання інформаційної безпеки організації.

Завдяки словнику базових та додаткових термінів і понять та системі посилань на терміни і поняття посібник можна використати як тлумачний словник.

Навчальні матеріали, що стосуються опису елементів управління інформаційною безпекою, прикладів методів підтримки процесу оцінки ризиків, вимог щодо забезпечення готовності інформаційно-комунікаційних технологій до забезпечення неперервності бізнесу, вимог до органів, що здійснюють аудит та сертифікацію систем управління інформаційною безпекою, а також словник базових та додаткових термінів і понять додаються до навчального посібника окремо.

При написанні навчального посібника реалізований досвід авторів, здобутий при викладанні відповідних навчальних дисциплін у Державному університеті інформаційно-комунікаційних технологій, Національному авіаційному університеті та Національній академії Служби безпеки України, а також досвід практичного впровадження системи управління інформаційною безпекою в Національному банку України.

Автори висловлюють щирю вдячність рецензентам: доктору технічних наук, професору Г. М. Гулаку та доктору технічних наук, професору В. О. Хорошку за змістовні зауваження та рекомендації, які безумовно сприяли покращенню книги.

Розділ 1

Теоретичні основи та підходи до побудови системи управління інформаційною безпекою організації

Визначені теоретичні основи та підходи до побудови системи управління інформаційною безпекою організації.

На основі визначення поняття система формулюється поняття системний підхід, а на основі визначення поняття процес формулюється поняття процесний підхід.

На основі циклічної моделі покращення процесів формулюються перелік понять щодо системного та процесного підходів до управління організацією.

1.1. Визначення поняття система. Системний підхід

Формальне визначення системи [system] (від грец. *Σύστημα* — складений) — це сукупність взаємопов'язаних і взаємодіючих елементів.

Система являє множину, яка складається з двох або більше елементів та задовольняє наступним трьом умовам (рис. 1.1):

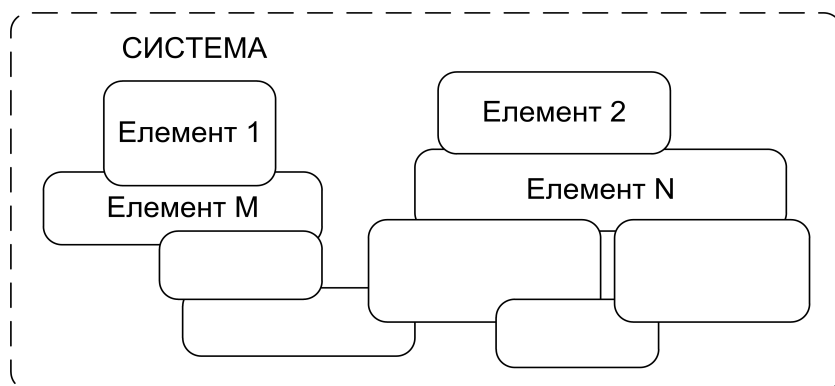


Рис. 1.1. До поняття система

1. Поведінка кожного елемента впливає на поведінку цілого, (наприклад, організм людини). Кожна його частина: серце, легені, шлунок тощо впливає на функціонування організму в цілому.

2. Поведінка елементів та їх вплив на ціле взаємозалежні. Дана умова означає, що поведінка кожного елемента і його вплив на ціле залежить від

того, як веде себе принаймні ще один інший елемент. Жоден елемент не має самостійного впливу на систему в цілому.

3. Які б підгрупи елементів ні утворилися, кожен елемент впливає на поведінку цілого, і жоден з них не впливає на них самостійно. Іншими словами, елементи системи з'єднані таким чином, що утворення ними незалежних підгруп неможливо.

Систему можна визначити як множину (сукупність) елементів (об'єктів) будь-якої природи, що взаємодіють між собою для досягнення загальної мети і володіють системними властивостями (цих властивостей не має жоден з елементів і жодне з підмножин елементів при будь-якому способі розподілу на складові) [2]. Властивостями системи є:

- цілісність — первинність цілого по відношенню до елементів;
- адитивність — принципова незвідність властивостей системи до суми властивостей складових її елементів;
- синергетичність — односпрямованість (або цілеспрямованість) дій сукупності елементів системи посилює ефективність функціонування системи;
- емерджентність — наявність нових властивостей і якостей у безлічі елементів системи, яких не було до їх об'єднання в систему; елемент системи має властивості, які він втрачає в разі відокремлення від системи;
- мультиплікативність — ефекти функціонування елементів в системі володіють властивістю множення, а не додавання;
- взаємодія і взаємозалежність системи і зовнішнього середовища;
- структурність — можливі декомпозиція системи на частини і встановлення зв'язків між ними;
- ієрархічність — кожна частина системи може розглядатися як система (підсистема) більш широкої глобальної системи;
- безперервність (неперервність) функціонування;
- цілеспрямованість — система завжди розглядається відносно деякої/деяких цілі/цілей;
- адаптивність — система прагне до стану стійкої рівноваги, яке передбачає адаптацію параметрів системи до мінливих параметрами зовнішнього середовища;
- альтернативність шляхів функціонування і розвитку — в залежності від конкретних параметрів, що виникають при функціонуванні системи, можуть існувати кілька альтернативних шляхів досягнення конкретної мети;
- спадковість — передача переважаючих (найбільш сильних) ознак на певних етапах розвитку (еволюції) системи від її старого версії до

нової;

- пріоритет інтересів системи більш глобального рівня перед інтересами її частин або підсистем.

Будь-яка система має внутрішній і зовнішній опис.

До внутрішнього опису системи відносяться її внутрішній стан і внутрішній механізм перетворення вхідних даних у вихідні. Цей опис дає інформацію про поведінку системи, про відповідність або невідповідність внутрішньої структури системи заданим цілям, підсистемам (елементам) і її ресурсам.

Зовнішній опис включає зовнішні прояви системи і містить інформацію про взаємодію з іншими системами, з цілями і ресурсами інших систем.

Системний підхід — це методологічний напрям дослідження об'єкта як системи з різних сторін, комплексно, в сукупності відносин і зв'язків між його елементами, на відміну від підходів, що застосовувалися раніше (фізичних, структурних і т. ін.) [2].

Системний підхід орієнтований на розкриття цілісності об'єкта, на виявлення різноманітних типів зв'язків і відносин, що мають місце як усередині досліджуваного об'єкта, так і в його взаєминах із зовнішнім середовищем, і зведення їх в єдину теоретичну картину. Його основне завдання полягає в розробці методів дослідження і конструювання складних об'єктів, що розвиваються — систем різних типів і класів, спираючись на вивчення об'єктивних закономірностей розвитку систем.

Системний аналіз. Встановленням структурних зв'язків між елементами досліджуваної системи, спирається на комплекс загальнонаукових, експериментальних, природничо-наукових, статистичних, математичних методів, займається системний аналіз. Він являє собою сукупність методів і засобів дослідження та побудови складних об'єктів за рахунок обґрунтування рішень при створенні та управлінні технічними, економічними та соціальними системами.

Системний аналіз використовується як один з найважливіших методів в системному підході, як ефективний засіб вирішення складних, зазвичай недостатньо чітко сформульованих проблем, до яких відносяться і проблеми управління різними об'єктами. Системний аналіз дозволяє уточнити проблеми і структурувати їх в серію завдань, що вирішуються за допомогою різних методів, знайти критерії їх вирішення, деталізувати цілі.

Моделювання систем. При системному підході в рамках моделювання систем необхідно, перш за все, чітко визначити мету моделювання системи. Важливо пам'ятати, що неможливо повністю змоделювати реально функціонуючу систему, а необхідно створити модель (систему-модель) під поставлену проблему при вирішенні конкретної задачі. Зрештою моделю-

вання повинно адекватно відображати реальні процеси поведінки досліджуваних систем. Однією з цілей моделювання є її пізнавальна спрямованість. Виконанню цієї мети сприяє правильний відбір в створювану модель елементів системи, структури і зв'язків між ними, критерію оцінки адекватності моделі. При такому підході спрощується класифікація реальних систем та їх моделей.

Основними цілями при системному підході є наступні:

- підвищення синергетичності;
- зниження емерджентності;
- забезпечення позитивної мультиплікативності в організації;
- забезпечення стійкості функціонування організації;
- забезпечення адаптивності роботи організації;
- забезпечення сумісності роботи різних підсистем організації;
- забезпечення ефективної роботи зворотних зв'язків в організації як всередині підсистем, так і між підсистемами.

Системний підхід припускає наступні етапи вирішення проблеми:

- 1) вивчення предметної області (якісний аналіз);
- 2) виявлення і формулювання проблеми;
- 3) математична (кількісна) постановка проблеми;
- 4) натурне та/або математичне моделювання досліджуваних об'єктів і процесів;
- 5) статистичне оброблення результатів моделювання;
- 6) пошук і оцінка альтернативних рішень;
- 7) формулювання висновків і пропозицій щодо вирішення проблеми.

1.2. Визначення поняття процес. Процесний підхід

Процес [process] (від лат. processus — просування) — це сукупність взаємопов'язаних або взаємодіючих видів діяльності, яка перетворює входи на виходи і вимагає для цього певних ресурсів і керуючих впливів (управління) (рис. 1.2) [2; 120].

Входами до процесу звичайно є виходи інших процесів. Входами можуть бути специфічні вимоги, включаючи ресурси — підмножина активів організації, що використовуються або споживаються у процесі здійснення деякої діяльності. На виході маємо в тій чи іншій мірі задоволені вимоги і сам безпосередній результат процесу.

Входи і виходи процесу можуть бути відчутними (обладнання, матеріали, продукція, інформація на різних носіях тощо) і невідчутними (специфіковані вимоги, послуга і т. ін.). Будь-який процес має зацікавлені сторони — споживача, внутрішнього або зовнішнього, і діє відповідно до встановлених цілей [119; 120].