ЗМІСТ

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 упровадження 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 Національної академії Служби безпеки України, а також досвід практичного впровадження системи управління інформаційною безпекою в Національному банку України.

Автори висловлюють щиру вдячність рецензентам: доктору технічних наук 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. $\Sigma\acute{\upsilon}\sigma\tau\eta\mu\alpha$ — 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):

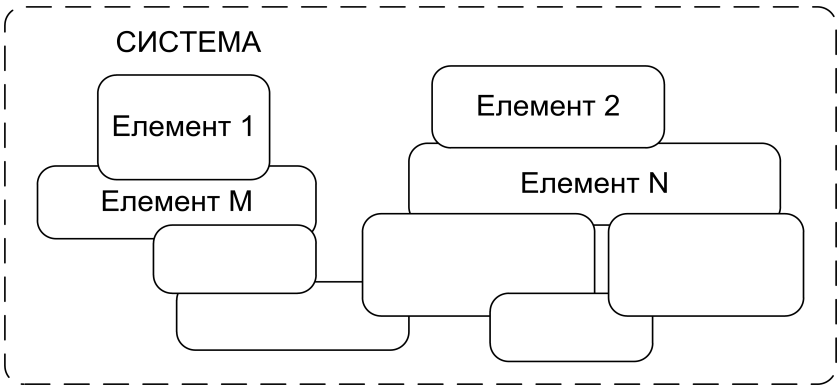

Рис. 1.1. До поняття система

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 мультиплікативности 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].