ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ю.М. Якименко, В.А. Савченко, С.В. Легомінова

СИСТЕМНИЙ АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: СУЧАСНІ МЕТОДИ УПРАВЛІННЯ

Підручник

Київ – 2022

УДК. 303.732.4:004.056

Я 45

Рекомендований до друку

Вченою радою Державного університету телекомунікацій

(Протокол № 17 від 20 травня 2021року)

Рецензенти:

Богданович В.Ю., доктор технічних наук, професор, головний науковий співробітник Центрального науково-дослідного інститут ЗСУ.
Наконечний В.С., доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.
Гайдур Г.І., доктор технічних наук, професор, завідувач кафедри інформаційної та кібербезпеки Державного університету телекомунікацій.

Я 45 Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с.

Підручник відображає основні аспекти вивчення дисципліни «Системний аналіз інформаційної безпеки»: висвітлення теоретичних основ системного аналізу у сфері інформаційної безпеки , застосування методологічних підходів до створення систем управління інформаційною безпекою, з особливостями створення систем управління інцидентами і управління ризиками інформаційної безпеки та їх впровадження; розкриття застосування методів в системному аналізі інформаційної безпеки: аналіз інформаційних систем, аналіз та синтез у дослідженні і проектуванні організацій, метод аналізу ієрархій і метод мережевого планування; порядок оцінки стану інформаційної безпеки організації: оцінка економічної безпеки підприємства, моніторинг і аудит інформаційної безпеки організації, SIEM в системі управління подіями.

Підручник може бути корисний студентам, які навчаються за освітніми програмами за спеціальністю 125 Кібербезпека, науково-педагогічним працівникам, фахівцям в галузі інформаційної безпеки державних та комерційних організацій.

УДК. 303.732.4:004.056

ЗМІСТ

ПЕРЕДМОВА

Забезпечення управлінської діяльності у сфері інформаційної безпеки є складною багатогранною сферою, що регламентується численними як міжнародними так і національними нормативними документами.

Наявність значної кількості попередньо написаних підручників та посібників з питань інформаційної безпеки, що базуються на класичних схемах викладання матеріалу, не в повній мірі задовольняють запити студентства та викладачів, а саме в практичному дослідженні процесів забезпечення інформаційної безпеки завдяки використанню методичних інструментів системного аналізу. Тому підготовка кваліфікованого фахівця з управління інформаційною безпекою в Україні має включати вивчення системного підходу та сучасних методів системного аналізу, що використовуються для підготовки та обґрунтування рішень при дослідженні складних проблем, об'єктів, процесів та явищ, які розглядаються у вигляді систем і функціонують в умовах неповної інформації та у сфері інформаційної безпеки.

У підручнику розглянуто теоретичні основи системного аналізу у сфері інформаційної безпеки: стан розвитку теорії систем, побудова організаційних структур підприємств, інформаційно-аналітичні системи, оцінка ефективності управління організацією. Розкрито застосування методологічних підходів до створення систем управління інформаційною безпекою: захисту інформації, управління інформаційною безпекою, управління інцидентами інформаційної безпеки, управління ризиками інформаційної безпеки. Показано практика проходження перевірки системи управління інформаційною безпекою на відповідність вимогам міжнародних та національних стандартів. Також висвітлено застосування методів в системному аналізі інформаційної безпеки: аналіз інформаційних систем, аналіз та синтез у дослідженні організацій, метод аналізу ієрархій і метод мережевого планування. Показано порядок оцінки стану інформаційної безпеки організації: оцінка економічної безпеки підприємства, моніторинг і аудит інформаційної безпеки організації, SIEM в системі управління подіями інформаційної безпеки організації.

ТЕМА 1. Основні положення теорії систем у сфері інформаційної безпеки

1.1. Стан розвитку теорії систем та її елементи

Правомірно розглядати системний аналіз як одну з дисциплін, що сприяють розвитку загальної теорії систем.

Теорія систем традиційно завжди була тісно пов'язана із проектуванням і розробкою складних систем (перша розробка в цій області почата для телефонії), тоді як системний аналіз забезпечував математичний опис процесів функціонування й керування. Системний аналіз орієнтований на розв'язок завдань, для яких можна побудувати математичні моделі, що дозволяють одержувати оптимальні розв'язки. Що стосується теорії систем, то вона, використовуючи формальні побудови, має справа з більш складними завданнями і її методи є більш глобальними й абстрактними.

Існує дуже велика безліч визначень поняття «система» і різні підходи до їх класифікації. Безліч визначень цього поняття говорить про те, що по суті дотепер немає досить однозначного його визначення. Теоретики системності вважають, що «системизм» – це новий погляд на мир, сформований в XX столітті, але який до кінця ще не завершений. Отже, дотепер немає завершеної загальної теорії систем (ЗТС). Як видно, усі існуючі визначення поняття «система» і системності по своїй суті є визначеннями наслідків, які випливають із визначення самого поняття «система».

1.1.1. Визначення системи та її основні властивості

Система — слово грецьке, буквально означає ціле, складене із частин. В іншому значенні — порядок, певний правильним розташуванням частин і їх взаємозв'язками. Система є сукупністю динамічно взаємозалежних елементів, змістом еволюції якої є досягнення деякої мети. Теорія систем займається насамперед виявленням механізму досягнення цієї мети, а також механізмів саморегулювання й переходу в стан рівноваги.

«Система – це набір взаємодіючих елементів», приводить Берталанфі, один із засновників сучасної ЗТС підкреслюючи, що система – це структура, у якої елементи якимось образом діють один на одного (взаємодіють).

«Система – це комплекс вибірково залучених елементів, взаємодіючих компонентів по досягненню заданого корисного результату, який ухвалюється основним системно утворюючим фактором»- Анохін В.А.

Система – ця безліч об'єктів разом з відносинами між об'єктами й між їхніми атрибутами. Це визначення припускає, що система має властивості, функції й мети, відмінні від властивостей, функцій і цілей складових її об'єктів, відносин і атрибутів.

Об'єкти – це частини системи. Більшість систем складається з фізичних частин, але в систему можуть входити й абстрактні об'єкти: математичні змінні, рівняння, закони й т. п. Атрибути – це властивості об'єктів.

Властивості систем- загальні для всіх систем:

- Цілісність — система є абстрактна сутність, що володіє цілісністю й певна у своїх границях. Цілісність системи має на увазі, що в деякому істотному аспекті «сила» або «цінність» зв'язків елементів усередині системи вище, чим сила або цінність зв'язків елементів системи з елементами зовнішніх систем або середовища.
- Ієрархічність — кожний компонент системи може розглядатися як система; сама система також може розглядатися як елемент якоїсь над- або під-системи (суперсистеми).

“Система” має також і двома протилежними властивостями: обмеженістю й цілісністю. Перше — це зовнішня властивість системи, а друге — внутрішнє, що здобувається в процесі розвитку. Система може бути відмежованої, але не цілісної.

Обмеженість системи являє собою перша й споконвічна її властивість. Це необхідне, але не достатня властивість. Якщо сукупність об'єктів обмежена від зовнішнього миру, то вона може бути системної, а може й не бути нею.

Сукупність стає системою тільки тоді, коли вона знаходить цілісність, тобто здобуває структурність, ієрархічність, взаємозв'язок із середовищем.

Найважливіші властивості системи: структурність, взаємозалежність із середовищем, ієрархічність, множинність описів (табл. 1.1).

Цілісність, що не зводиться до своїх складових частин. Тут завжди спостерігається втрата якості. Оскільки науковий опис об'єкта припускає процедури уявного розчленовування цілісності, то цілісність являє собою безліч описів. Звідси різноманіття визначень системи: структурована безліч; безліч, взаємодіюче з оточенням; упорядкована цілісність і т. д.

Структурність — це впорядкованість системи, певний набір і розташування елементів зі зв'язками між ними. Між функцією й структурою системи існує взаємозв'язок, як між філософськими категоріями змістом і формою. Зміна змісту (функцій) спричиняє зміна форми (структури), але й навпаки.

Таблиця 1.1.

Характеристика основних властивостей системи

Властивість системи	Характеристика
Обмеженість	Система відокремлена межами від навколишнього середовища
Цілісність	Її властивість цілого принципово не зводиться до суми властивостей окремих складових елементів
Структурність	Поведінку системи зумовлено не стільки особливостями окремих елементів, а скільки властивостями її структури
Взаємозалежність із середовищем	Система формує і проявляє властивості в процесі взаємодії із середовищем
Ієрархічність	Підпорядкованість елементів
Множинність описів	Через складність пізнання системи вимагає множинності її описів

Ієрархічність системи. Елементи системи перебувають у різних відносинах між собою й місце кожного з них є місцем на ієрархічній градації системи. Система хоча й проявляє себе як одиничний і цілісний об'єкт, але складається з елементів (підсистем, частин), тобто, систем більш низького порядку. У той же час вона сама може бути системою (підсистемою, частиною), що входить до складу системи більш високого порядку.

Усі елементи нашого миру взаємозалежні тією чи іншою мірою.

Процес цілеспрямованої зміни в часі стану системи називається **поведінкою**. На відміну від керування, коли зміна стану системи досягається за рахунок зовнішніх впливів, поведінка реалізується винятково самою системою, виходячи із власних цілей.

Фундаментальною властивістю систем є **стійкість**, тобто здатність системи протистояти зовнішнім впливам, що обурюють. Від неї залежить тривалість життя системи. **Прості системи** мають пасивні форми стійкості: міцність, збалансованість, регульованість. А **для складних** визначальними є активні форми: надійність, живучість і адаптованість. Якщо перераховані форми стійкості простих систем (крім міцності) стосується ***їхньої поведінки***, то визначальна форма стійкості складних систем носять в основному ***структурний характер***.

Надійність — властивість збереження структури систем, незважаючи на загибель окремих її елементів за допомогою їх заміни або дублювання.

Живучість — як активне придушення шкідливих якостей. Таким чином, надійність є більш пасивною формою, чому живучість.

Адаптованість — властивість змінювати поведінку або структуру з метою збереження, поліпшення або придбання нових якостей в умовах зміни зовнішнього середовища. Обов'язковою умовою можливості адаптації є наявність зворотних зв'язків.

Усяка реальна система існує в середовищі. Зв'язок між ними буває настільки тісної, що визначати границю між ними стає складно. Можна виділити два аспекти взаємодії:

- ухвалює характер обміну між системою й середовищем (інформацією);
- середовище звичайно є джерелом невизначеності для систем.

Вплив середовища може бути пасивним або активним.

Відношення – одна з форм загального взаємозв'язку всіх предметів, явищ, процесів у природі, суспільстві, мисленні.

Відносини предметів друг до друга винятково різноманітні: ***причина й наслідок, частина й ціле, підпорядкування й супідрядність, аргумент і функція***, ***проходження в часі***, і т. д. У математику й логіку використовують такі види відносин, як «… більше чому…», «…включене в…», «…тягне за…» і т.п.

У визначенні системи відзначене, що для всіх систем характерна наявність відносин між об'єктами й між їхніми атрибутами.

З появою необхідності розв'язку завдань широкого класу, що виникають у всіляких сферах людської діяльності, і які мають, незважаючи на їхню якісну відмінність, одне загальне – вони *зводяться до вибору способу дії, варіанта плану, параметрів конструкції,* тобто **до прийняття рішень.**

У цих умовах виникли термін **«операція»** і наукова дисципліна, називана **«Дослідження операцій».**

Операція означає будь-яку цілеспрямовану дію. Ціль операції вважається заданою. Завдання дослідника операції полягає в тому, щоб знайти оптимальний спосіб використання ресурсів сторони, що оперує, забезпечує досягнення заданої мети.

Наукова дисципліна **«Дослідження операцій»**, спостерігає реальні явища, пов'язані з функціональними системами, розробляє моделі, призначені для пояснення цих явищ, використовує ці моделі для вивчення того, що відбудеться при зміні умов, і перевіряє пророкування новими спостереженнями. Одержання рішень при цьому щонайкраще відповідають цілям усієї організації. У дослідженні операцій уживає спроба врахувати всі істотні фактори, установити між ними зв'язок і оцінити їх у цілому.

Складна система — збірна назва систем, що полягають із великої кількості взаємозалежних елементів. Слід підкреслити неформальність цього

поняття, оскільки на сучасному етапі розвитку науки немає його строгого математичного визначення. *(Математична енциклопедія).*

Складна система — складений об'єкт, частини якого можна розглядати як системи, закономірно об'єднані в єдине ціле відповідно до певних принципів або зв'язані між собою заданими відносинами.(*Більша радянська енциклопедія*)

До деяких рис складної системи (як об'єкта управління) ставляться:

- Відсутність математичного опису або алгоритму,
- «Зашумленість», яка виражається в скруті спостереження і управління.
- Обумовлена більшим числом другорядних (для цілей управління) процесів і ін.

1.1.2. Сутність і основні характеристики системності

Загальним поняттям, яке позначає всі можливі прояви систем, є “системність”. Системність — досить складне й різноманітне явище, що проявляється в трьох аспектах (рис.1.1).

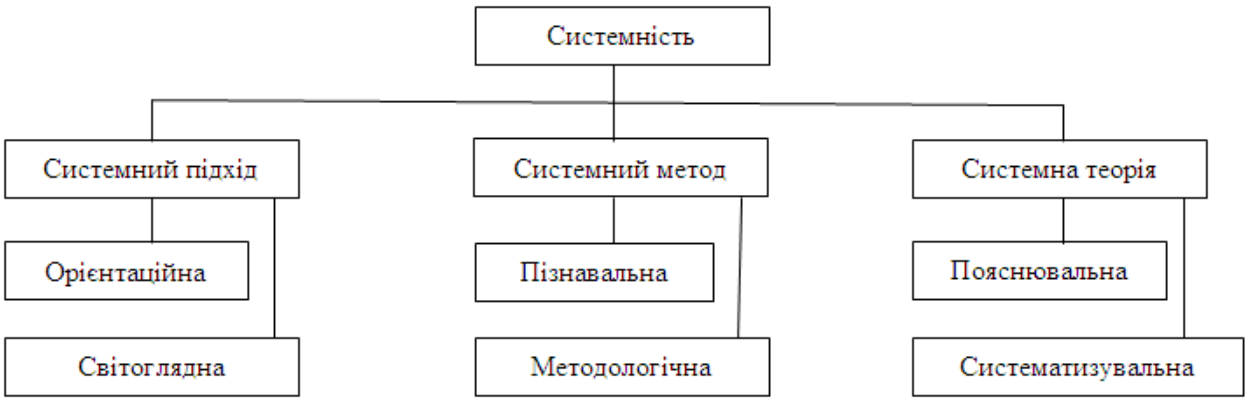


Рис.1.1. Структура системності і складові її функції

Складові системності реалізують специфічні функції.

У **системному підході** термін “підхід” означає сукупність прийманъ, способів впливу на кого-небудь, у вивченні чого-небудь… У цьому змісті підхід

— скоріше не детальний алгоритм дії людину, а безліч деяких узагальнених правил.

Системний підхід можна розглядати *як принцип діяльності*. Адже під принципом розуміється *найбільш загальне правило діяльності*, яке забезпечує його правильність, але не *гарантує однозначність і успіх*.

Системний підхід слід розглядати як деякий *методологічний підхід людини до дійсності*, що представляє собою деяку спільність принципів. Це по суті справи *системна парадигма, системний світогляд*.

Призначення *системного підходу* полягає в тому, що він *направляє людину на системне бачення дійсності.* Він *змушує розглядати мир із системних позицій*, точніше — *з позицій його системного обладнання*. *Системний підхід* будучи принципом пізнання, виконує орієнтаційну й світоглядну функції.

Принцип системності припускає вистава досліджуваного об'єкта як:

- елементним складом;
- структурою як формою взаємозв'язку елементів;
- функціями елементів і цілого;
- єдністю внутрішнього й зовнішнього середовища системи;
- законами розвитку системи і її складових.

Системний метод виступає як деяка інтегральна сукупність щодо простих методів і приймань пізнання, а також перетворення дійсності.

Системний метод реалізує пізнавальну й методологічну функції, а системна теорія — пояснюючу, що й систематизує.

Таким чином, системність виступає як інструмент пізнавальної діяльності, значного арсеналу конкретних методів пізнання всього сущого.

Системна теорія як знання про системи накопичує їх, упорядковує й використовує для пояснення систем різної природи.

Існує також ще два принципово різні підходи до визначення системи: дескриптивний і конструктивний.

Дескриптивний підхід ґрунтується на визнанні того, що системність властива дійсності. Дескриптивний підхід до системи полягає в тому, що

характер функціонування системи пояснюють її структурою, елементами. Будь-який об'єкт виступає як система - властивість і функція задаються її внутрішнім обладнанням (відношенням, структурою, взаємозв'язками). Дескриптивний підхід лежить в основі системного аналізу, який полягає в побудові структури системи, з якої виводяться її функції.

Схема дескриптивного підходу може бути такою:

- виділення елементів, що мають деяку просторово-тимчасову визначеність;
- визначення зв'язків між елементами;
- визначення системотворчих властивостей, зв'язків і відносин; визначення структур, тобто законів композиції;
- аналіз функцій системи.

Конструктивний підхід носить зворотний характер. У ньому *по заданій функції конструюється відповідна їй структура.* При цьому використовується не просто функціональний, але й функціонально-цільовий підхід, тому що система повинна відповідати деяким цілям конструювання.

Виділення й побудова системи здійснюється так:

- ставиться мета, яку повинна забезпечувати система;
- визначається функція (або функції), що забезпечує(ие) досягнення цієї мети;
- підшукується або створюється структура, що забезпечує виконання функції.

Мета являє собою *стан, до якого спрямована тенденція руху об'єкта*.

Ціль звичайно виникає із проблемної ситуації, яка не може бути дозволена наявними засобами. І система певної структури й за допомогою своїх функцій виступає засобом дозволу проблеми (рис.1.2).

Рис.1.2. Конструювання системи

Системологія як прикладна інженерна дисципліна є під впливом техніки, моделювання, проектування й конструювання, тобто **технічної**, **інформаційної** й соціальної **інженерії** (рис.1.3).

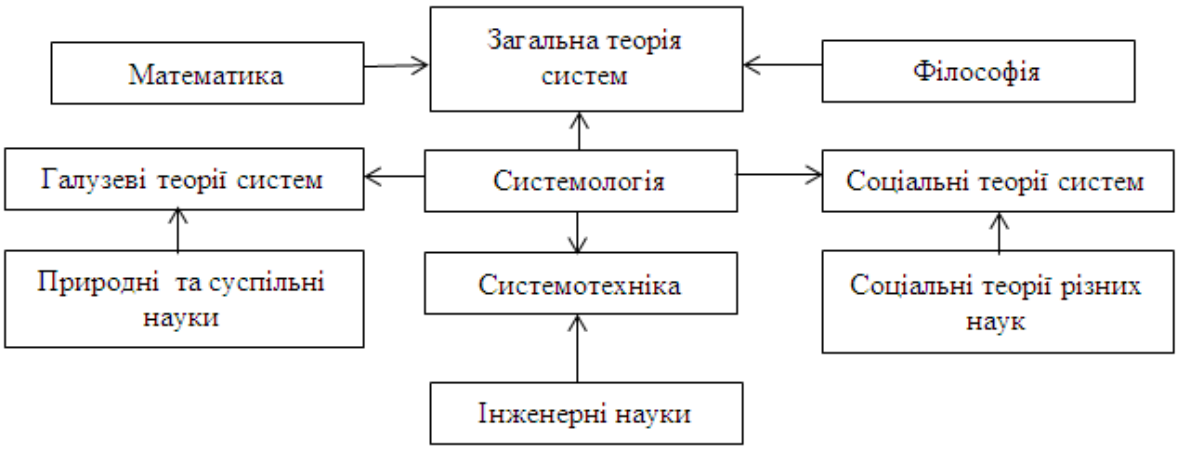


Рис.1.3. Структура системології

Величезну роль у розвитку загальної теорії систем відіграють **науки (логіка, теорія множин, кібернетика й ін.).** ***Галузеві теорії систем*** розкривають специфіку систем різної природи. ***Спеціальні теорії систем*** спрямовані на відбиття їх окремих сторін, аспектів, зрізів, етапів. Наприклад, теорія перехідних систем, теорія еволюції систем і т. п.

В останній чверті XX ст. разом з видатними успіхами системності проявляються **кризові процеси**. Системність у ряді випадків перестає відповідати на зростаючі потреби сучасності. **Системний підхід став усе**

частіше давати збої. Внаслідок постійної зміни нововведень людство виявилося в постійно перехідному суспільстві, що полягає з підсистем, що безупинно обновляються. Суспільство потребує принципового відновлення системної методології. У цьому напрямку продовжують працювати вчені, наприклад: І. І. Пригожин (лауреат Нобелівської премії 1977 р.), Г. Хаген і ін. Мультиплікаційний підхід, висунутий ними на перший план серед інших методологічних принципів, дозволив пояснити перехідні, нестаціонарні процеси, що забезпечує подолання кризи системності.

1.1.3. Класифікація систем

Класифікацією називається розбивка на класи по найбільш істотних ознаках. Під **класом** розуміється сукупність об'єктів, що володіють деякими ознаками спільності.

Ознака (або сукупність ознак) є підставою (критерієм) класифікації.

Система може бути охарактеризована одним або декількома ознаками і відповідно їй може бути знайдене місце в різних класифікаціях, кожна з яких може бути корисної при виборі методології дослідження. Звичайно ціль класифікації обмежити вибір підходів до відображення систем, виробити мова опису, що підходить для відповідного класу.

По змісту розрізняють **реальні** (матеріальні), які **об'єктивно існують** і **абстрактні** (концептуальні, ідеальні) системи, які є продуктом мислення (рис.1.4).

Реальні системи діляться на **природні** (природні системи) і **штучні** (антропогенні).

Природні системи: системи неживий (фізичні, хімічні) і живий (біологічні) природи.

Штучні системи: створюються людством для своїх потреб або утворюються в результаті цілеспрямованих зусиль.

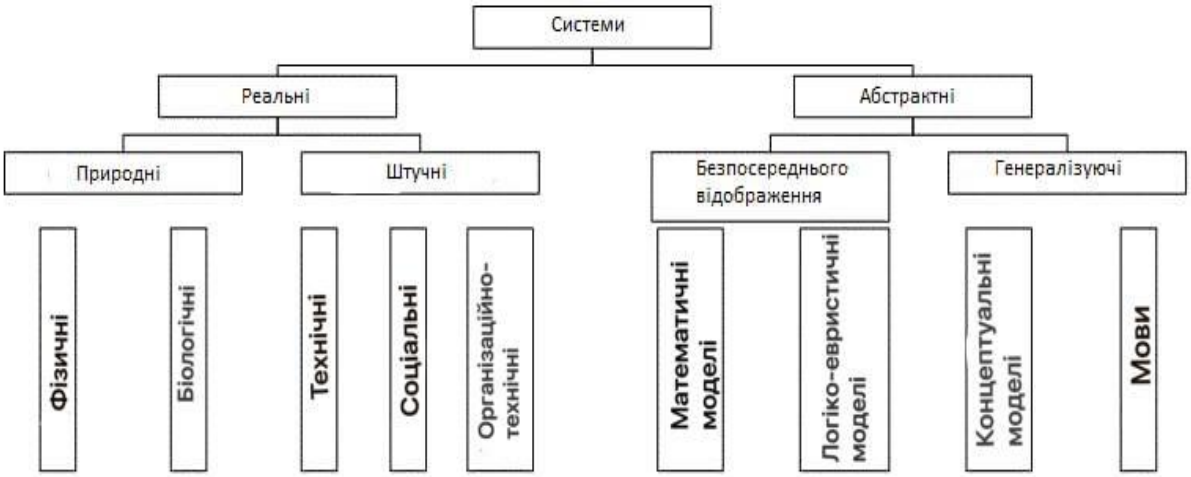


Рис.1.4. Класифікація систем

Абстрактні системи є **результатом відбиття дійсності (реальних систем) у мозку людини.**

Абстрактні системи розділяють на **системи безпосереднього відображення** (що відбивають певні аспекти реальних систем) і **системи генералізуючого (узагальнюючого) відображення** До перших ставляться **математичні й евристичні моделі**, а до других — **концептуальні системи** (теорії методологічної побудови) і **мови**.

Існує також **класифікація систем за критеріями** - виду й ступені функціонально-виконуваних завдань (табл.1.2).

Таблиця 1.2.

Класифікація систем за критеріями

№ п.п.	Підстава (критерій) класифікації	Класи систем
1	По взаємодії із зовнішнім середовищем	Відкриті Закриті Комбіновані
2	За структурою	Прості Складні Більші

Продовження табл.1.2.

3	По характеру функцій	Спеціалізовані Багатофункціональні (універсальні)
4	По характеру розвитку	Стабільні, Які розвиваються
5	По ступеню організованості	Добре організовані Погано організовані (дифузійні)

По взаємодії із зовнішнім середовищем. На основі поняття зовнішнього середовища системи розділяються на: **відкриті, закриті** (замкнені, ізольовані) і **комбіновані**. Розподіл систем на відкриті й закриті пов'язане з їхніми характерними ознаками: можливість збереження властивостей при наявності зовнішніх впливів. Якщо система нечутлива до зовнішніх впливів її можна вважати закритої. А якщо ні, то — відкритої.

Відкритою називається система, яка взаємодіє з навколишнім середовищем. Усі реальні системи є відкритими. Відкрита система є частиною більш загальної системи або декількох систем.

Закритою називається система, яка не взаємодіє із середовищем або взаємодіє із середовищем строго певним чином. Закриті системи являють собою деяку абстракцію реальної ситуації, тому що, строго говорячи, ізольованих систем не існує.

Комбіновані системи містять *відкриті й закриті підсистеми*. Наявність комбінованих систем свідчить про складну комбінацію відкритої й закритої підсистем.

Залежно від структури й просторово-тимчасових властивостей системи діляться на **прості, складні й великі**.

Прості — системи, що не мають розгалужених структур, що полягають із невеликої кількості взаємозв'язків і невеликої кількості елементів. Такі елементи

служать для виконання найпростіших функцій, у них не можна виділити ієрархічні рівні.

Складні — характеризуються більшим числом елементів і внутрішніх зв'язків, їх неоднорідністю й різним по якості, структурною різноманітністю, виконанням складної функції або рядом функцій.

Компоненти складних систем можуть розглядатися **як підсистеми**, кожна з яких може бути деталізована ще більш простими підсистемами.

Систему називають **складною** якщо в реальній дійсності суттєво проявляються **ознаки її складності (** усі ознаки у взаємозв'язку):

1. **структурна складність** — визначається по числу елементів системи, числу й різноманітності типів зв'язків між ними, кількості ієрархічних рівнів і загальному числу підсистем системи. Основними типами вважаються наступні види зв'язків: структурні (у тому числі, ієрархічні), функціональні, каузальні (причинно-наслідкові), інформаційні, просторово-тимчасові;

2. **складність функціонування (поведінки)** — визначається характеристиками безлічі станів, правилами переходу зі стану в стан, вплив системи на середовище й середовища на систему, ступенем невизначеності перерахованих характеристик і правил;

3. **складність вибору поведінки** — у багато альтернативних ситуаціях, коли вибір поведінки визначається метою системи, гнучкістю реакцій на заздалегідь невідомі впливи середовища;

4. **складність розвитку** — обумовлена характеристиками еволюційних або стрибкоподібних процесів.

Складні системи можна підрозділити на **факторні підсистеми**:

1. вирішальну, яка ухвалює глобальні розв'язки у взаємодії із зовнішнім середовищем і розподіляє локальні завдання між усіма іншим підсистемами;

2. інформаційну, яка забезпечує збір, переробку й передачу інформації, необхідної для прийняття глобальних рішень і виконання локальні завдань;

3. керуючу для реалізації глобальних рішень;

4. гомеостазну, що підтримує динамічна рівновага усередині систем і регулюючу потоки в підсистемах;

5. адаптивну, яка накопичує досвід у процесі навчання для поліпшення структури й функцій системи.

Великою системою називають систему, неспостережувану одночасно з позиції одного спостерігача в часі або в просторі, для якої істотний просторовий фактор, **число підсистем якої дуже велике**, а **склад різнорідний**.

Система **може бути й великою і складною одночасно**. Складні системи поєднують більш велику групу більших систем, тобто ***великі — це підклас складних систем.***

Основними ***при аналізі й синтезі*** великих і складних систем є ***процедури декомпозиції й агрегування***.

Декомпозиція (потужний інструмент дослідження систем) — поділ систем на частині, з наступним самостійним розглядом окремих частин.

Агрегування протилежне декомпозиції - об'єднання елементів системи з метою розглянути її з більш загальних позицій.

З погляду характеру функцій різняться **спеціальні, багатофункціональні і універсальні системи.**

Для **спеціальних систем** характерна одиничність призначення й вузька професійна спеціалізація обслуговуючого персоналу (порівняно нескладна).

Багатофункціональні системи дозволяють реалізувати на одній і тій же структурі кілька функцій. Приклад: виробнича система, що забезпечує випуск різної продукції в межах певної номенклатури.

Для **універсальних систем**: реалізується безліч дій на одній і тій же структурі, однак склад функцій по виду й кількості менш однорідний (менш визначений).

По характеру розвитку систем: **стабільні, що розвиваються**.

У **стабільної системи** структура й функції практично не змінюються протягом усього періоду її існування й, як правило, якість функціонування

стабільних систем у міру зношування їх елементів тільки погіршується. Відбудовні заходи звичайно можуть лише знизити темп погіршення.

Відмінною особливістю **систем, що розвиваються**, є те, що із часом їх структура й функції здобувають істотні зміни. Функції системи більш постійні, хоча часто й вони видозмінюються. Практично незмінними залишається лише їх призначення. системи, що розбудовуються, мають більш високу складність.

По ступеню організованості: **добре організовані, погано організовані** (дифузійні).

Розв'язок завдання при виставі її у вигляді **добре організованої системи** здійснюється аналітичними методами формалізованого вистави системи. Застосовується в тих випадках, коли можна запропонувати детермінований опис і експериментально довести правомірність його застосування, адекватність моделі реальному процесу.

Погано організовані системи. При виставі об'єкта у вигляді погано організованої або дифузійної системи не ставиться завдання визначити всі компоненти, що враховуються, їх властивості і зв'язки між ними та цілями системи.

Продовження табл. 1.2.

Класифікація систем за критеріями

№	Підстава (критерій) класифікації	Класи систем
6	По складності поведінки	Автоматичні Вирішальні Самоорганізовані
7	По характеру зв'язку між елементами	Детерміновані Стохастичні
8	По характеру структури управління	Централізовані Децентралізовані
9	По призначенню	Виробляючі Керуючі Обслуговуючі

<u>В порядку ускладнення поведінки: автоматичні, вирішальні, самоорганізовані, передбачувальні, перетворювальні.</u>

Автоматичні: однозначно реагують на обмежений набір зовнішніх впливів, внутрішня їхня організація пристосована до переходу в рівноважний стан при висновку з нього (гомеостаз).

Вирішальні: мають постійні критерії розрізнення їх постійної реакції на широкі класи зовнішніх впливів. Сталість внутрішньої структури підтримується заміною елементів, що вийшли з ладу .

Самоорганізовані: мають гнучкі критерії розрізнення і гнучкі реакції на зовнішні впливи, що пристосовуються до різних типів впливу. Стійкість внутрішньої структури вищих форм таких систем забезпечується постійним самовідтворенням.

Самоорганізовані системи володіють ознаками дифузних систем: стохастичністю поведінки, нестаціонарністю окремих параметрів До цього додаються такі ознаки, як непередбачуваність поведінки; здатність адаптуватися до мінливих умов середовища, змінювати структуру при взаємодії системи із середовищем, зберігаючи при цьому властивості цілісності; здатність формувати можливі варіанти поведінки й вибирати з них найкращий і ін.

Приклади: організація управління на рівні підприємства, галузі, держави в цілому, тобто в тих системах де обов'язково є людський фактор.

Якщо стійкість системи по своїй складності починає перевершувати складні впливи —, що це **передбачувальні** системи, які може передбачити подальший хід взаємодії.

Перетворювальні — це уявлювані складні системи на вищому рівні складності, не зв'язані сталістю існуючих носіїв. Науці приклади таких систем поки не відомі.

<u>По характеру зв'язків між елементами</u>

Системи, для яких стан системи однозначно визначається початковими значеннями й може бути передвіщене для будь-якого наступного моменту часу, називаються **детермінованими.**

Стохастичні системи — системи, зміни в яких носять випадковий характер.

За ознаками структури побудови систем і значимості тієї ролі, яку відіграють у них окремі складові частини в порівняння з ролями інших. Однієї із частин системи може належати домінуюча роль .Такий компонент — буде виступати як центральний, що визначає функціонування всієї системи. Ці системи називають **централізованими.** Якщо всі складові систем приблизно однаково значимі й взаємозалежні послідовно або паралельно й мають приблизно однакові значення для функціонування, то такі системи - **децентралізовані**.

По призначенню. Серед технічних і організаційних систем виділяють: **виробляючи, управляючи, обслуговуючи.**

У виробляючих системах реалізуються процеси одержання деяких продуктів або послуг. Інформаційні системи — **для збору, передачі й перетворення інформації й надання** інформаційних послуг.

Призначення **управляючих систем** — організація й управління матеріально-енергетичними й інформаційними процесами.

Обслуговуючі системи займаються підтримкою заданих меж працездатності виробляючих і управляючих систем.

Мають місце й **інші підходи до класифікації систем**.

Так по формах руху системи підрозділяються **на механічні, фізичні, хімічні, біологічні й соціальні.**

Питання для самоконтролю

1. Що таке системний принцип?
2. Яку дисципліну стало прийнято називати системним аналізом?
3. Що таке теорія систем?
4. Що називають системою?
5. Що таке об'єкт системи? Приведіть приклади.
6. Що таке атрибут об'єкта системи? Приведіть приклади.

7. Що таке відношення? Приведіть приклади.
8. Яка система називається цілісної?
9. Яка система називається відособленої?
10. Аналіз основних визначень поняття “система”.
11. Принципи загальної теорії систем.
12. Чим різняться між собою конструктивний і дескриптивний підходи у визначенні системи?
13. Дайте конструктивне визначення системи.
14. Розкрийте структуру системності й складові її функції.
15. Як класифікуються системи?
16. Перелічите ознаки складності системи.

1.2. Побудова організаційних структур підприємств

Сучасний системний аналіз є прикладною наукою, націленої на з'ясування причин реальних складнощів, що виникли перед «володарем проблеми» (зазвичай це конкретна організація, установа, підприємство, колектив), і на вироблення варіантів їх усунення.

Поява проблеми - ознака недостатньої системності; рішення проблеми - результат підвищення системності.

Успіх в сучасному бізнесі та менеджменті багато в чому спирається на оперативний аналіз економічної ситуації і вибір оптимального рішення. Під управлінням розуміються найзагальніші принципи, на основі яких будується структура управління організацією.

Для виконання практичної задачі з побудови функціональних структур підприємств необхідно спиратися на основних поняттях з теорії систем і методи прикладного системного аналізу.

Практично виконана робота спрямовується на засвоєнні аспектів з теорії системного аналізу - класифікації систем і основних типах структур управління підприємством.

Пропонується виконати завдання з побудовою організаційних структур управління підприємством з підрозділами забезпечення інформаційної безпеки і з морфологічним, інформаційним і функціональним їх описами.

1.2 1. Організаційний процес побудови структур підприємств

При побудові структури підприємства завжди розглядають його як систему. За ступенем складності розрізняють прості, складні і дуже складні системи. **Прості системи** характеризуються невеликим числом елементів, зв'язку між якими легко піддаються опису (засоби механізації, найпростіші організми). **Складні системи** складаються з великої кількості елементів і характеризуються розгалуженою структурою, виконують більш складні функції. Зміни окремих елементів і (або) зв'язків тягне за собою зміну багатьох інших елементів. Але все ж окремі конкретні стану системи можуть бути описані (автомати, ЕОМ). Дуже складні системи характеризуються великою кількістю різних елементів, мають безліч структур, не можуть бути повністю описані (мозок, господарство). за різним призначенням і переліком різноманітних виконуючих задач системи розпізнають як одно- або багатофункціональні, з постійним або змінним складом функцій.

Система завжди має цілі, для яких вона функціонує і існує. Тобто система це сукупність (безліч) окремих об'єктів з неминучими зв'язками між ними. Під об'єктом (елементом) прийнято розуміти найпростішу неподільну частину системи. У загальному вигляді є необмежене безліч таких частин, спосіб виділення яких залежить від формулювання цілей аналізу і побудови самої системи.

Створення реальної системи означає, що вона синтезується з деяких компонентів в наступному порядку: задум системи, аналіз і виділення компонентів, конструювання, компоненти, об'єднання компонентів в єдине ціле. Система може бути розчленована на елементи не відразу, а шляхом послідовного поділу на підсистеми. Підсистеми самі є системами і до них, отже, відноситься

все, що сказано про систему, в тому числі і про її цілісності. Тобто підсистема - це частина загальної системи з деякими її зв'язками і відносинами.

Структура відбиває найбільш суттєві взаємозв'язки між елементами і їх групами. Дані взаємозв'язку забезпечують існування системи та її основних властивостей. Структура - все те, що вносить порядок в безліч об'єктів, тобто сукупність зв'язків і відносин між частинами цілого, необхідних для досягнення цілі.

Приклад системи "Інформаційний центр". Вхідні, вихідна і внутрісистемна інформація може надаватися документами, графічними, аудіо- та відеофайлами, програмами і т.д. ***Системні функції***: надання машинного часу, обробка даних, пошук інформації, створення і обробка архівів і баз даних. ***Системні цілі***: впровадження нових інформаційних технологій, впровадження нових методів навчання персоналу і користувачів, підвищення ефективності пошуку, отримання, обробки та зберігання інформації. ***Опис системи*** враховує ефективність методів роботи з інформацією в момент часу, коефіцієнт комп'ютерної неграмотності користувачів, коефіцієнт, що показує ступінь впровадження нових апаратно-програмних засобів.

Приклад. Банк є система. Зовнішнє середовище банку - система інвестицій, фінансування, трудових ресурсів, нормативів і т.д. Вхідні впливу - *характеристики (параметри) цієї системи*. Внутрішні стану системи - *характеристики фінансового стану*. Вихідні впливу - потоки кредитів, послуг, вкладень і т.д. *Функції системи* - банківські операції, наприклад, кредитування. Функції системи також залежать від характеру взаємодій системи і зовнішнього середовища. Безліч виконуваних банком функцій залежать від зовнішніх і внутрішніх функцій, які можуть бути описані (представлені) деякими числовими і / або нечисловими, наприклад, якісними, характеристиками або характеристиками змішаного, якісно-кількісного характеру.

Морфологічне (структурний або топологічний) опис системи - це опис будови або структури системи або опис сукупності елементів цієї системи і

необхідного для досягнення мети набору відносин між цими елементами системи.

Функціональне опис системи - це опис законів функціонування, еволюції системи, алгоритмів її поведінки, "роботи".

Інформаційне (інформаційно-логічне або інфологічне) опис системи - це опис інформаційних зв'язків як системи з навколишнім середовищем, так і підсистем системи.

Організаційний процес - це процес створення організаційної структури підприємства. Розробка структури зазвичай здійснюється зверху вниз.

Етапи організаційного проектування:

- розділіть організацію по горизонталі на широкі блоки;
- встановіть співвідношення повноважень для посад;
- визначте посадові обов'язки.

Розглядаючи організаційну структуру управління підприємством, враховуються рівні взаємодії: організації з зовнішнім середовищем; підрозділів організації; організації з людьми.

Важливу роль тут відіграє структура організації, за допомогою якої і через яку ця взаємодія здійснюється. Структура фірми - це склад і співвідношення її внутрішніх ланок, відділів.

Організаційна структура підприємства - це сукупність ланок (структурних підрозділів) і зв'язків між ними.

Вибір організаційної структури залежить від таких факторів, як:

- організаційно-правова форма підприємства;
- сфера діяльності (тип продукції, що випускається, її номенклатура і асортимент);
- масштаби підприємства (обсяг виробництва, чисельність персоналу);
- ринки, на які виходить підприємство в процесі господарської діяльності;
- використовувані технології;
- інформаційні потоки усередині і поза фірмою;
- ступінь відносної забезпеченості ресурсами і ін.

Структури управління на багатьох сучасних підприємствах були побудовані відповідно до принципів управління, сформульованими ще на початку XX століття. Найбільш повне формулювання цих принципів дав німецький соціолог Макс Вебер в концепції раціональної бюрократії.

Фахівці виділяють наступні основні типи організаційних структур підприємства (рис.1.5):

- лінійна-а; функціональна-б; лінійно-функціональна-в;
  лінійно-штабна-д; матрична-г.

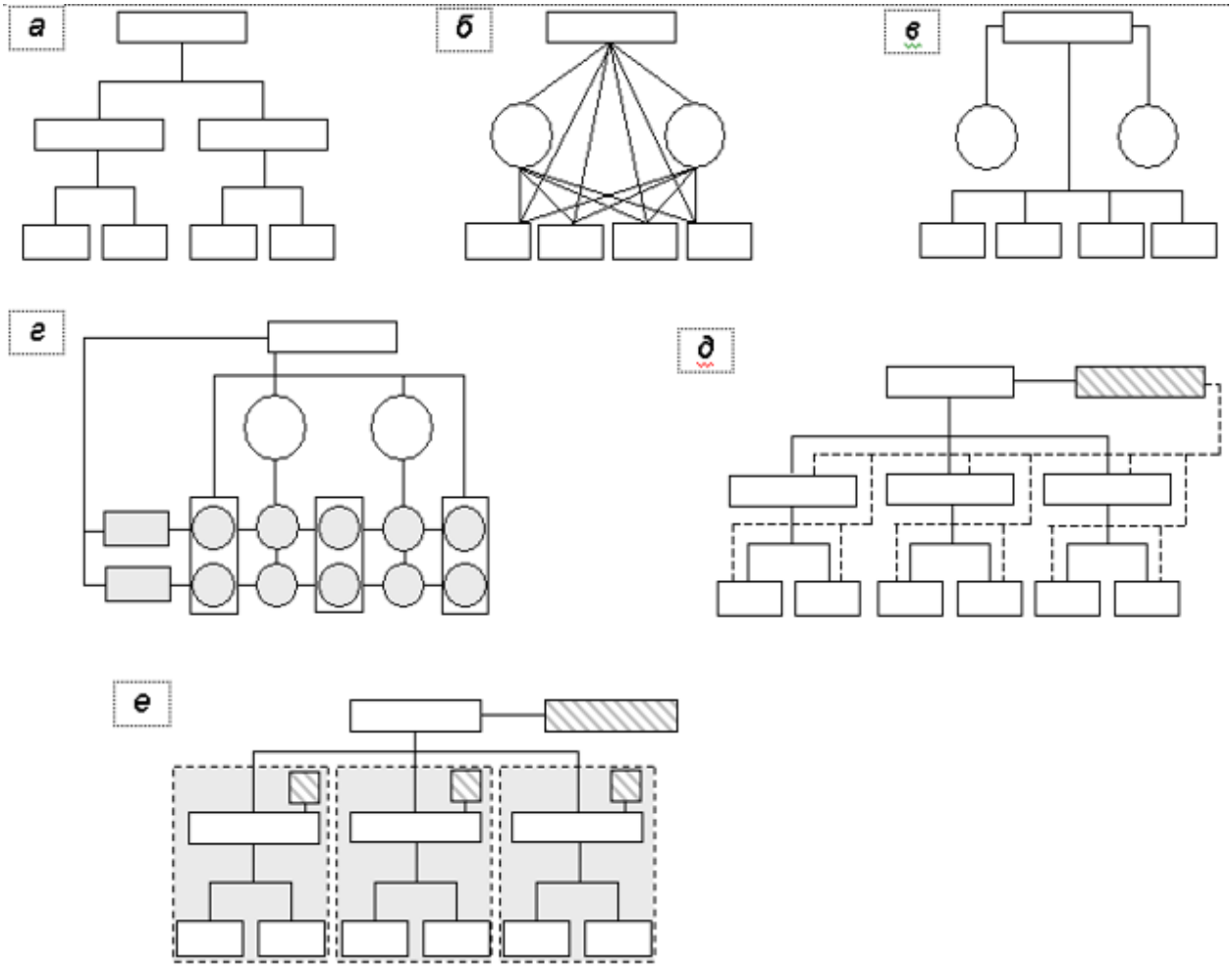


Рис.1.5. Основні типи організаційних структур підприємства

Приклади основних типів організаційних структур підприємств показані нижче на рис. 1.6-1.9.

Лінійна організаційна структура підприємства являє собою схему, що описує вертикальні зв'язку підпорядкування різних підрозділів організації. Так, виділяють керівника організації, його заступника і штат співробітників, їм

підлеглих. Цю організаційну структуру доцільно застосовувати при невеликому штаті організації і відносно стабільному зовнішньому і внутрішньому середовищу. Лінійна структура проста і може бути ефективною, якщо число розглянутих питань невелике і по них можуть бути дані рішення в найближчих підрозділах.

Переваги: простота, конкретність завдань і виконавців.

Недоліки: високі вимоги до кваліфікації керівників і високе завантаження керівника. Лінійна структура застосовується і ефективна на

невеликих підприємствах з нескладною технологією і мінімальної спеціалізацією.

Даний тип організаційної структури застосовується в умовах функціонування дрібних підприємств з нескладним виробництвом при відсутності розгалужених зв'язків з постачальниками, споживачами, науковими і проектними організаціями ...

В даний час лінійна структура використовується в управлінні невеликими фірмами, цехами, ділянками.

При **функціональній організаційній структурі** підприємство підрозділяється на елементи, кожен з яких має свої завдання і обов'язки.

Характеристики та особливості того чи іншого підрозділу відповідають за найбільш важливі напрямки діяльності підприємства. Традиційні функціональні блоки підприємства - відділи виробництва, маркетингу, фінансів. Це широкі області діяльності, або функції, які є на кожному підприємстві для забезпечення досягнення цілей.

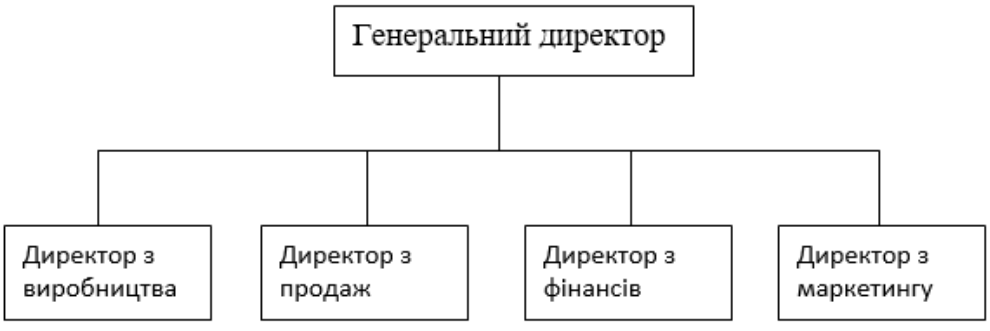


Рис.1.6. Функціональна організаційна структура підприємства

Переваги: поглиблення спеціалізації, підвищення якості управлінських рішень; можливість управляти багатоцільовий і багатопрофільною діяльністю.

Недоліки: недостатня гнучкість; погана координація дій функціональних підрозділів; низька швидкість прийняття управлінських рішень; відсутність відповідальності функціональних керівників за кінцевий результат роботи підприємства.

Функціональна організаційна структура, на відміну від лінійної, використовується на більш великих підприємствах з серійним виробництвом.

Структура змішаного типу - лінійно - функціональна (на практиці застосовується частіше)

В основі цієї організаційної структури лежать принципи двох попередніх типів: створення при основних ланках вертикальної лінійної структури також і функціональних підрозділів. Основна роль цих підрозділів полягає у підготовці проектів рішень, які вступають в силу після затвердження відповідними лінійними керівниками. Така структура зберігає цілеспрямованість лінійної структури і дає можливість спеціалізувати виконання окремих функцій і тим самим підвищити ефективність управління організацією.

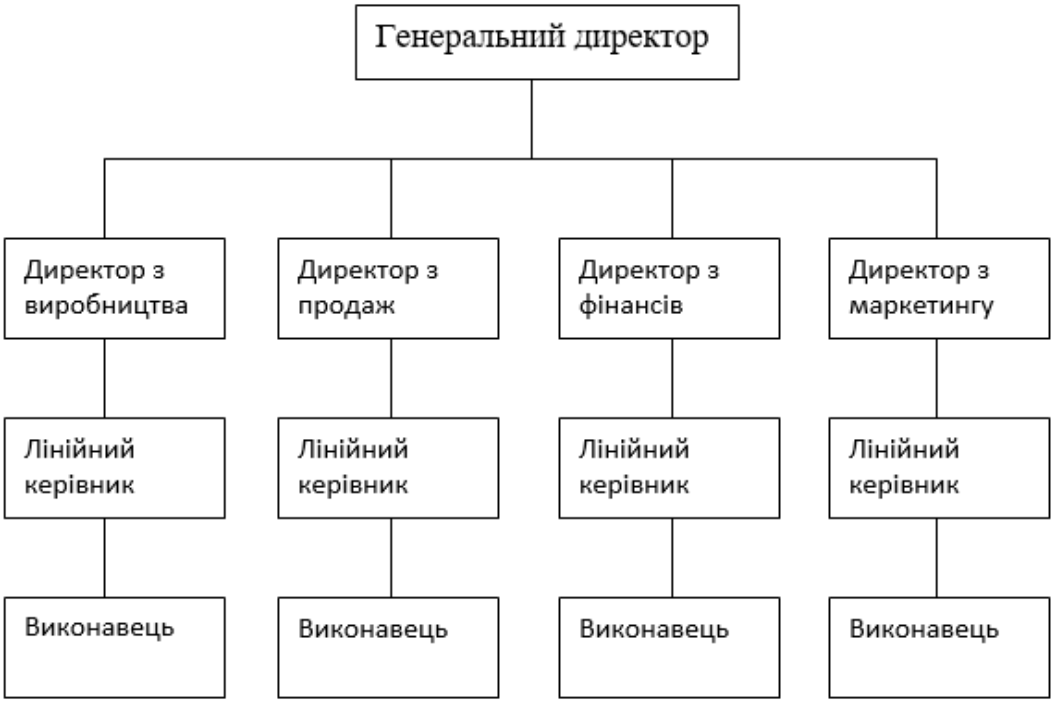


Рис.1.7. Структура підприємства змішаного типу: лінійно - функціональна

Лінійно-штабна організаційна структура багато в чому схожа з лінійно-функціональної, але її особливістю є те, що в ній виділяється деякий штабний координуючий орган. Він займається координацією питань, спрямованих в усі відділення (філії) та підрозділи підприємства.

Такий вид організаційної структури, як правило, зустрічається і в великих організаціях (холдинги, транснаціональні корпорації), коли необхідно забезпечити злагоджену роботу.

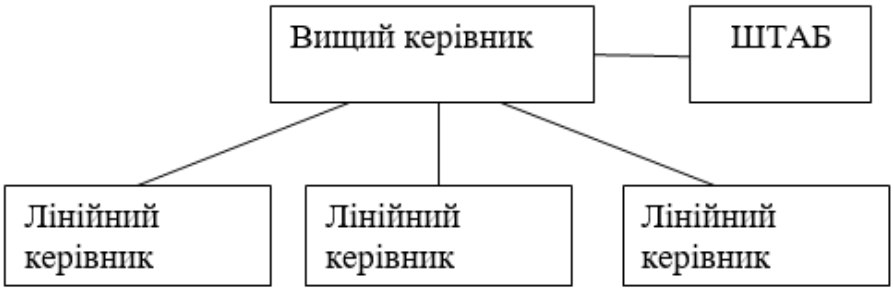


Рис.1.8. Лінейно - штабна організаційна структура підприємства

Для великих підприємств, що випускають велику кількість різноманітної продукції, а також для підприємств, що працюють в широких міжнародних масштабах, більше підходить матрична організаційна структура.

Ця структура являє собою систему, побудовану за принципом подвійного підпорядкування виконавців. **З одного** боку, вони підпорядковані безпосередньому керівнику функціональної служби, що надає персонал і технічну допомогу керівнику проекту, **з іншого** - керівнику проекту (цільовий програми), який наділений необхідними повноваженнями відповідно до запланованих термінів, ресурсами і якістю.

Матрична структура використовується в багатьох галузях промисловості, особливо в наукоємних виробництвах (наприклад, у виробництві електронної техніки), а також в деяких організаціях невиробничої сфери.

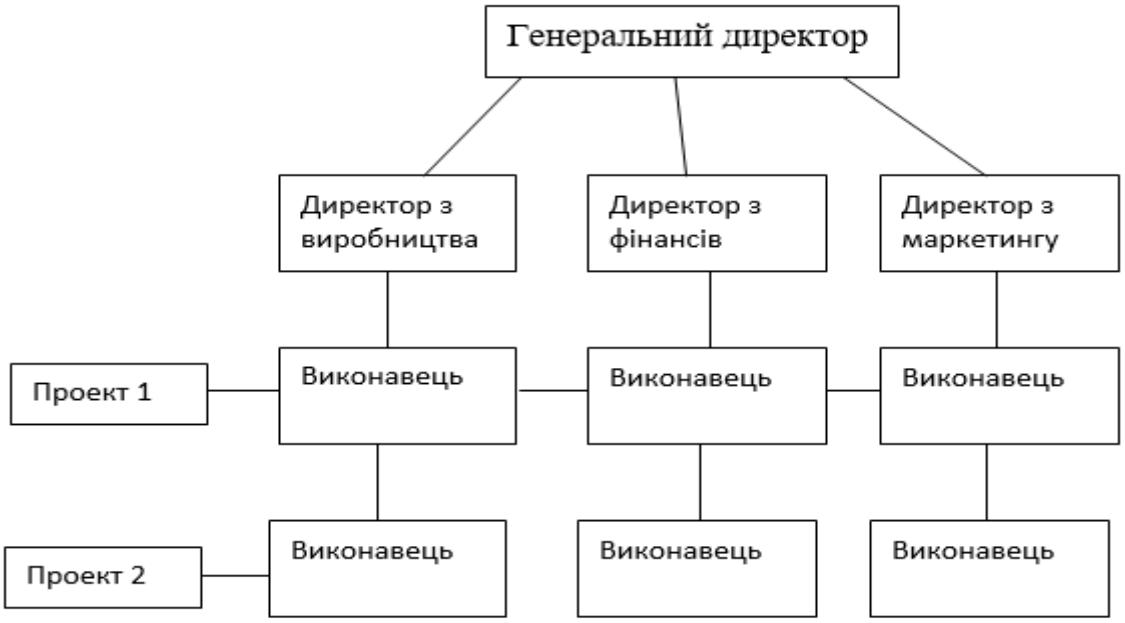


Рис.1.9. Матрична організаційна структура підприємства

Переваги: гнучкість, прискорення впровадження інновацій, персональна відповідальність керівника проекту за результати роботи.

Недоліки: наявність подвійного підпорядкування, конфлікти через подвійне підпорядкування, складність інформаційних зв'язків.

Наведені організаційні структури складають основу для розробки структур управління (моделей, систем) підприємств при проведенні наукових досліджень.

1.2.2. Методика побудови функціональної структури підприємств з підрозділами забезпечення інформаційної безпеки

Методику побудови функціональної структури будь-якого підприємства пропонується відпрацювати на прикладі вищого навчального закладу (ВНЗ) відповідно до завдань:

1. Треба почати з відповіді на питання: Які **підсистеми створені в системі "ВНЗ**"? Які зв'язки між ними існують? Описати їх зовнішню і внутрішню середу, структуру. Класифікувати (з поясненнями) ці підсистеми. Описати вхід, вихід, мету, зв'язки зазначеної системи та її підсистем. Намалювати топологію системи (на прикладі університету).

2. Привести приклад деякої системи будь-якого підприємства (на самостійний вибір студентом), вказати її зв'язку з навколишнім середовищем, вхідні і вихідні параметри, можливі стану системи, підсистеми. Пояснити на цьому прикладі (тобто на прикладі однієї із завдань), що виникають в даній системі конкретного змісту понять "вирішити задачу" і "рішення задачі". Після аналізу визначити можливі недоліки і проблеми для цієї системи. Провести морфологічний, інформаційний і функціональний опис однієї-двох систем. Треба відповісти на питання: чи є ці системи погано структуровані і чи погано формалізуються з іншими системами? Як можна поліпшити їх структурованість і формалізованість?

Приклади організаційних структур систем "ВНЗ" (рис.1.10-1.11) і компанії (рис.1.12):

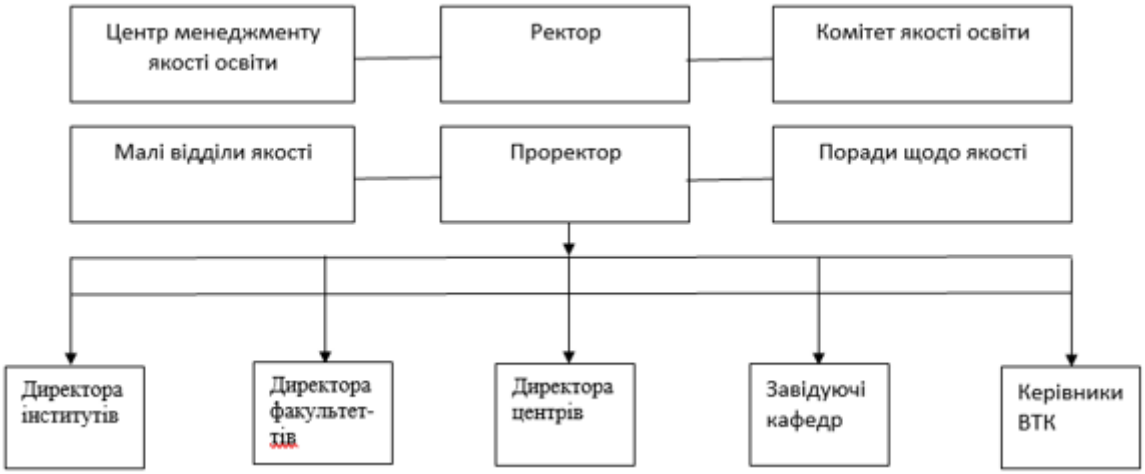


Рис.1.10. Спрощена структура університету (приклад)

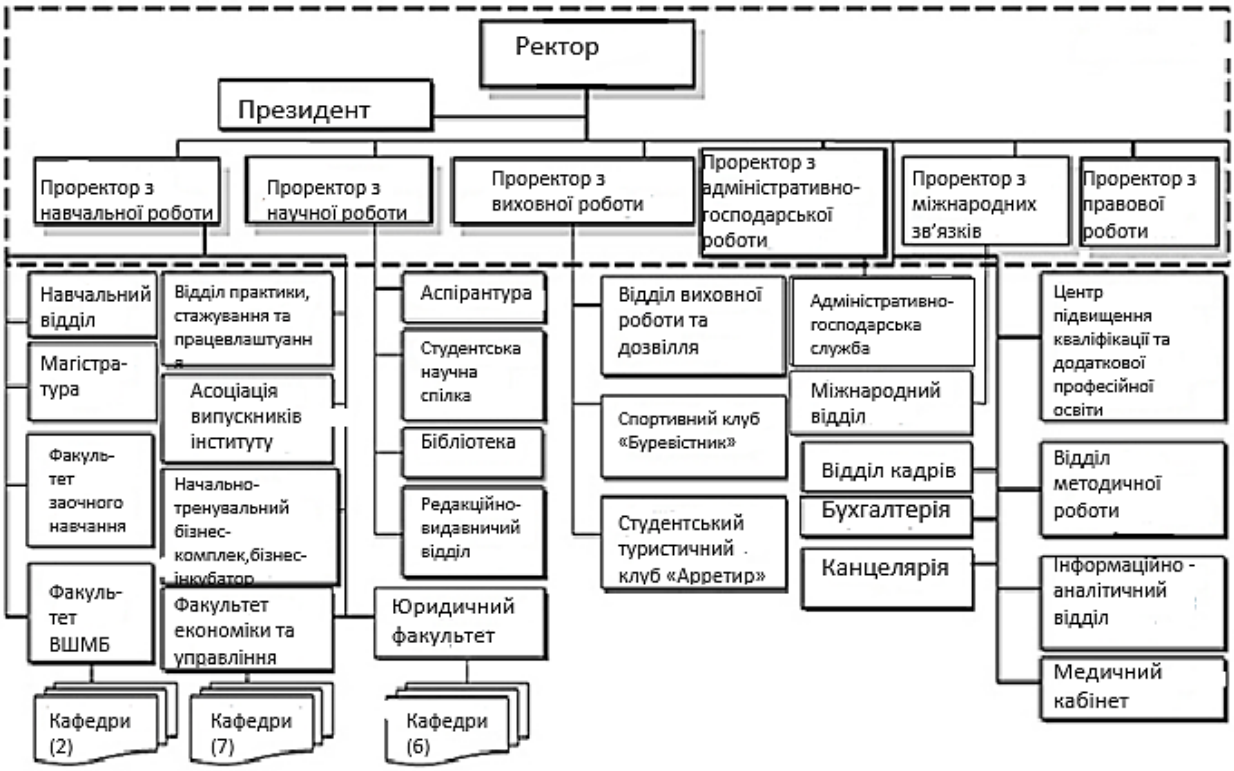


Рис.1.11. Ускладнена структура університету (приклад)

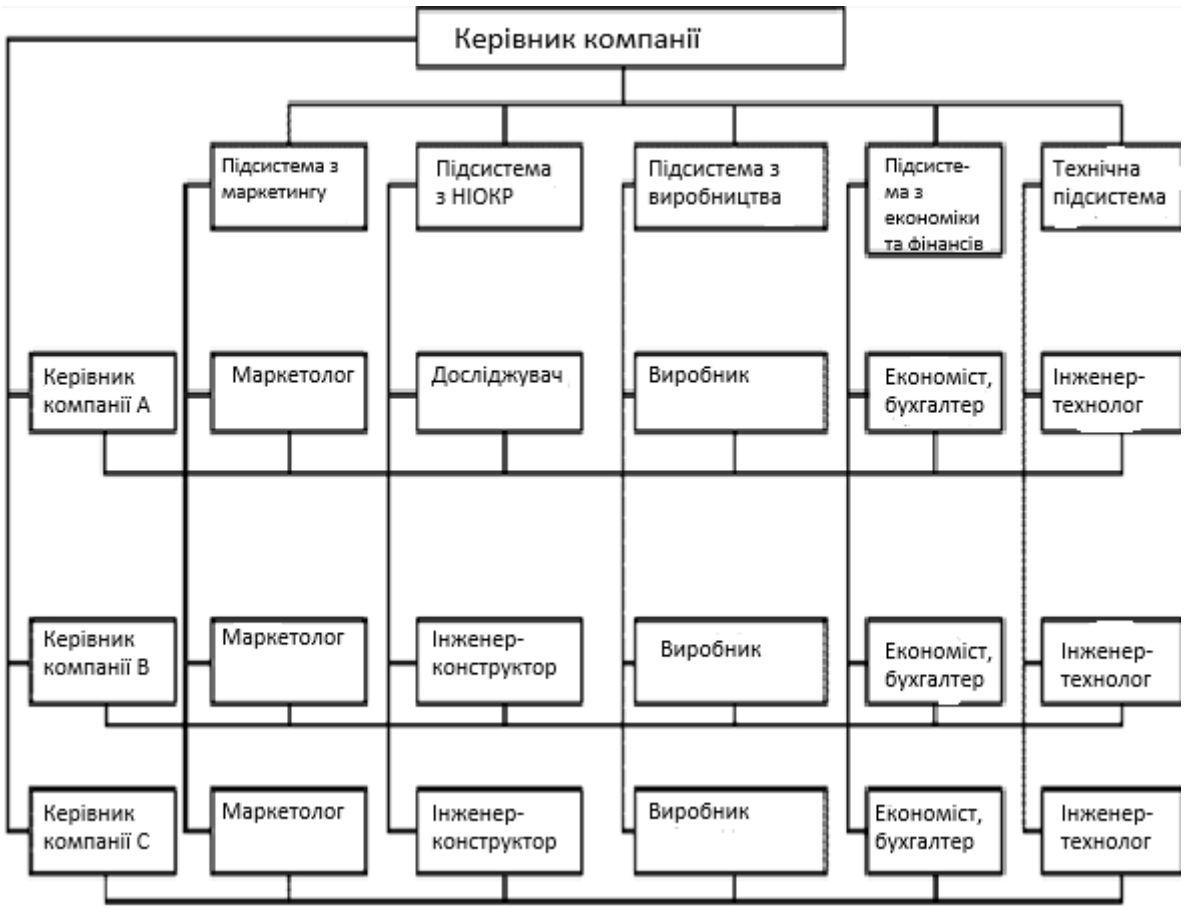


Рис.1.12. Реальна структура компанії

4. Після побудови функціональної структури підприємства треба виконати:

- визначити підрозділи або служби, які будуть виконувати функціональні обов'язки по забезпеченню інформаційної безпеки, їх місце і зв'язки – показати в структурній схемі;

- показати схему побудови функціональної системи управління інформаційною безпекою (СУІБ) з підсистемами управління ризиками і інцидентами інформаційної безпеки, а також систем, які забезпечують готовність до безперервності процесів, спрямованих на виконання виробничих і інших професійних задач на підприємстві;

- перелічіть обладнання для забезпечення інформаційної безпеки

Питання для самоконтролю

1. Що таке система і підсистема?
2. Для чого необхідна класифікація систем?
3. За якими ознаками здійснюється класифікація систем?
4. Які системи називають замкнутими?
5. Дайте визначення великої системи.
6. Яку систему можна назвати добре організованою?
7. Що розуміється під підсистемою?
8. Що розуміється під метою системи?
9. Що розуміється під класифікаційною ознакою системи?
10. Визначте додатковий класифікаційний ознак та типізуйте види систем за цією ознакою.
11. Що таке мета, структура, завдання, вирішення завдання, проблема?
12. Які основні ознаки і топології систем?
13. Приведіть схеми основних типів організаційних структур підприємства.
14. Приведіть схеми СУІБ з підсистемами управління ризиками і інцидентами інформаційної безпеки, а також систем, які забезпечують готовність до безперервності процесів на підприємстві.

1.3 Інформаційно-аналітичні системи

Проблема аналізу вихідної інформації для прийняття рішень виявилася настільки серйозною, що з'явився окремий напрямок у якісній розробці аналітичної частини у складі інформаційних систем. Це дозволить підняти рівень керівників у прийнятті стратегічних, тактичних та оперативних управлінських рішень.

1.3 1. Організація як предмет дослідження ІАС на базі OLAP-технологій

Головне завдання, розв'язуване IAC,- зробити накопичену в компанії інформацію більш доступною, інтерпретованою і своєчасною.

IAC на базі OLAP -Технологій (OLAP -Система, Система бізнес-аналітики-(BI) призначені *для аналізу більших обсягів інформації, дозволяють подолати обмеження традиційних IC.*

Споживачі інформації повинні бути забезпечені механізмами інтерактивного *складання звітів*, можливістю *перевірки гіпотез*, *виявлення закономірностей* у накопичених даних. Особи, що ухвалюють стратегічні рішення повинні мати механізми *моніторингу і оповіщення про всі важливі для бізнесу процеси й тенденції*. Це завдання стає транзакційно інтерпретованим, важко реалізованим, в умовах історичної неоднорідності й суперечливості, яка склалася в IC, використовуваних у компаніях (організаціях). Проблема аналізу вихідної інформації для прийняття рішень виявилася настільки серйозної, що з'явився окремий напрямок або вид IC: IAC.

Для ефективного рішення описаних задач перед організацією встає завдання проектування й побудови єдиного сховища даних (Data Warehouse)-(рис.1.13) і системи багатовимірного аналітичного зберігання і доступу до інформації (OLAP) – збору, обробки даних і створення звітів (рис.1.14).

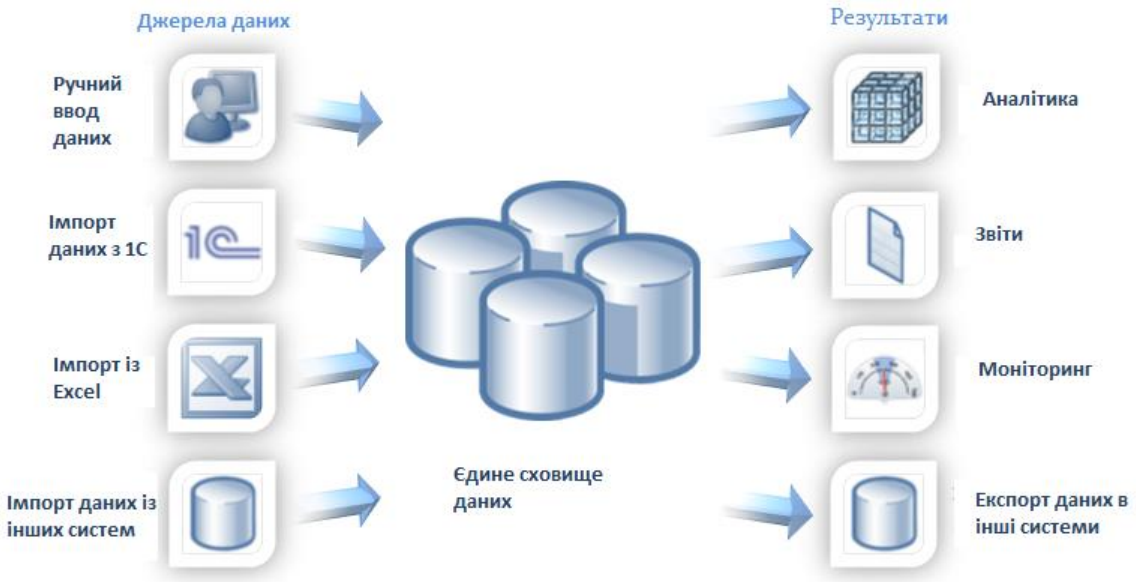


Рис.1.13. Місце єдиного сховища даних при обробці даних

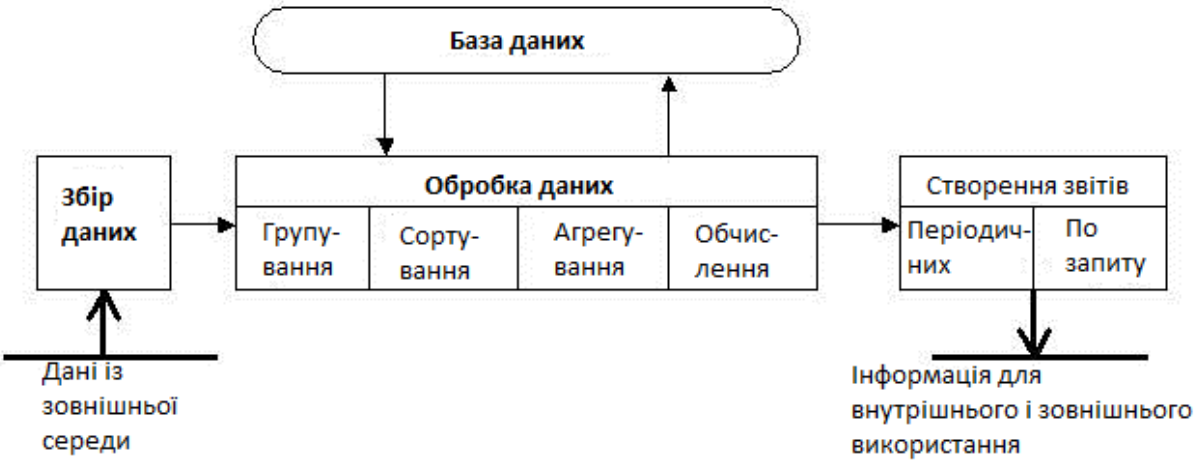


Рис.1.14. Основні компоненти інформаційної технології обробки даних

Інформаційна технологія - це сукупність об'єднаних у технологічний ланцюжок методів, виробничих процесів і програмно-технічних засобів, що забезпечують зберігання, пошук, обробку й поширення інформації.

Побудова сховища даних призначено вирішувати наступні завдання:

• **Забезпечення єдиної версії надаваної інформації**, що може бути критично для підтримки прийняття рішень. Досить часто різні ІС компаній, можуть надавати суперечну один одному інформацію із критичних для бізнесу питань. Це пов'язане з різним ступенем надійності, повноти й детальності збереженої в них інформації. Використання єдиного сховища ***гарантує, що всі споживачі інформації одержать на свої запити несуперечливі відповіді.***

• **Поліпшення якості збережених даних**. ***У процесі заповнення сховища, дані очищаються, приводяться до єдиного формату***, перевіряються на несуперечність і відповідність бізнес-правилам. Також

використовуються різні статистичні тести на виявлення аномалій, можливих помилок уведення і т. д. Побудова сховища неминуче приводить до стандартизації довідників, процедур уведення первинних даних, а також до оптимізації інформаційної політики компанії.

• **Зберігання даних у термінології бізнесу**, що поліпшує їх зрозумілість і доступність кінцевим користувачам.

• **Оптимізація зберігання даних** з погляду швидкості ***виконання аналітичних запитів.*** Для прискорення відгуку системи використовуються підходи, неможливі у транзакційній системі (звичайна база даних), тому що остання призначена для оптимізації введення й зберігання інформації.

• **Значне прискорення циклу розробки аналітичних звітів** у зв'язку з централізованим зберіганням усієї необхідної інформації. Розробникам не треба розбиратися в структурі даних у вихідних транзакційних системах, усе що їм потрібно ***зберігається в єдиній структурі даних, оптимізованої під їхні запити.***

• **Можливість інтерактивного складання складних аналітичних звітів** ***без участі програмістів***. Такі звіти повинні забезпечувати можливість аналізу операцій за різними показниками у всіх значимих аналітичних розрізах.

• **Безпека.** Централізація даних означає ***кращий контроль над доступом*** до них.

• **Можливість зберігання історії операцій.**.

• **Визначення і моніторинг ключових показників ефективності** функціонування підприємства ***в різних розрізах***.

• **Виявлення закономірностей у накопичених даних**. Вистава виявлених закономірностей у наочному виді. Можливість швидко ***побудувати модель і прогноз по виявлених закономірностях.***

Повноцінна **аналітична система в складі ІАС** повинна забезпечувати виконання наступних процесів - п**о-перше, одержання, перетворення й завантаження даних.**

Завдання по одержанню, перетворенні й завантаженню даних у сховище даних містить у собі:

• Об'єднання інформації з різних інформаційних систем, використовуваних у компанії.

• Фільтрація, очищення, валідація, агрегація даних, виявлення аномалій і протиріч. Перетворення всіх даних у єдиний формат.

• Створення єдиного інформаційного сховища, що поєднує інформацію з безлічі використовуваних систем. Дані в сховище організовані в термінах бізнесу й оптимізовані для побудови звітності.

• Створення вітрин даних - розрізів даних у загальному сховищі з фокусуванням на певних процесах. Вітрини даних забезпечують також рольовий підхід до доступу даних зі сховища.

• Створення періодичних завдань по відновленню сховища. Розробка системи оповіщення про помилки, протиріччя і неприступності вихідних даних та інші події при наповненні сховища.

По-друге, багатомірний аналіз даних у реальному часі.

Система онлайнової аналітичної обробки даних OLAP створюється на основі багатомірного сховища даних і призначена, у першу чергу, для створення в режимі «онлайн» аналітичних звітів і вистав.

1.3.2. Функції та сфери застосування ІАС

Таким чином, **основне призначення ІАС**— динамічна **вистава і багатомірний аналіз** історичних і поточних даних, **аналіз тенденцій, моделювання і прогнозування** результатів рішень.

Основними **функціями ІАС** є:

• Витяг даних з різних джерел, їх перетворення і завантаження в сховище;

• Зберігання даних;

• Аналіз даних, у тому числі оперативний і інтелектуальний;

• Підготовка результатів оперативного і інтелектуального аналізу для ефективного їхнього сприйняття споживачами.

Результатом застосування засобів ІАС є з однієї сторони - **регламентні аналітичні звіти**, орієнтовані на потреби користувачів різних категорій, з іншого боку - **засобу інтерактивного аналізу інформації й швидкої побудови звітів**

користувачами-непрограмістами з використанням звичних понять предметної області.

З технічної точки зору ІАС– це набір процедур, методів і регламентів, що приводять до регулярного планового збору, зберігання, аналізу й наданню інформації, використовуваної для прийняття управлінських рішень.

ІАС є надбудовою над уже функціонуючими на підприємстві інформаційними додатками і не вимагають їхньої заміни.

ІАС верхнього рівня служать для прийняття стратегічних рішень. Вони дозволяють керівникові вирішувати наступні завдання:

- **складання консолідованої звітності і**

надання зведеної інформації про діяльність підприємства(фінансові, виробничі й інші показники, динаміка їх змін і тенденції),

- **аналіз діяльності дочірніх підприємств, філій і підрозділів компанії** (аналіз прибутковості, витрат, виконання плану),
- **аналіз фінансової діяльності** (основні фінансові показники, тенденції, взаєморозрахунки), оптимізація фінансових потоків, реальна оцінка собівартості продукції,
- **проведення комплексної оцінки діяльності підприємства**, заснованої на постійному контролі чотирьох найбільш істотні її аспектів (фінанси, відносини із зовнішнім миром, внутрішній стан компанії, інновації),
- **аналіз організаційних процесів** (складання плану, контроль виконання розпоряджень, розрахунки за відвантажену продукцію, прогноз вступу засобів, прогноз попиту).

ІАС підрозділів – припускають більшу деталізацію й більш складну аналітичну обробку. Ці системи допомагають підготувати інформацію для

прийняття рішень (в області збуту, продуктової пропозиції, фінансового планування й ін.).

Розрізняють **два види інформаційно-аналітичних систем по режиму й темпу аналізу:**

- **статичні** - мають заздалегідь розроблений сценарій

обробки даних при досить обмежених можливостях варіацій запитів;

- **динамічні** - забезпечують обробку нерегламентованих запитів і гнучку систему підготовки звітів.

Виділяють наступні **принципи побудови ІАС на підприємстві**:

- **об'єднання всіх інформаційних процесів** підприємства;
- **вбудовування системи** у вже сформовану організаційну структуру підприємства;
- **координація зусиль усіх підрозділів підприємства** при виконанні поставлених задач;
- **відкритість системи для подальшого розвитку**;
- **комплексне використання всіх доступних методів аналізу**.

Повна структура ІАС, побудованої на основі сховища даних показана на рис.1.15.

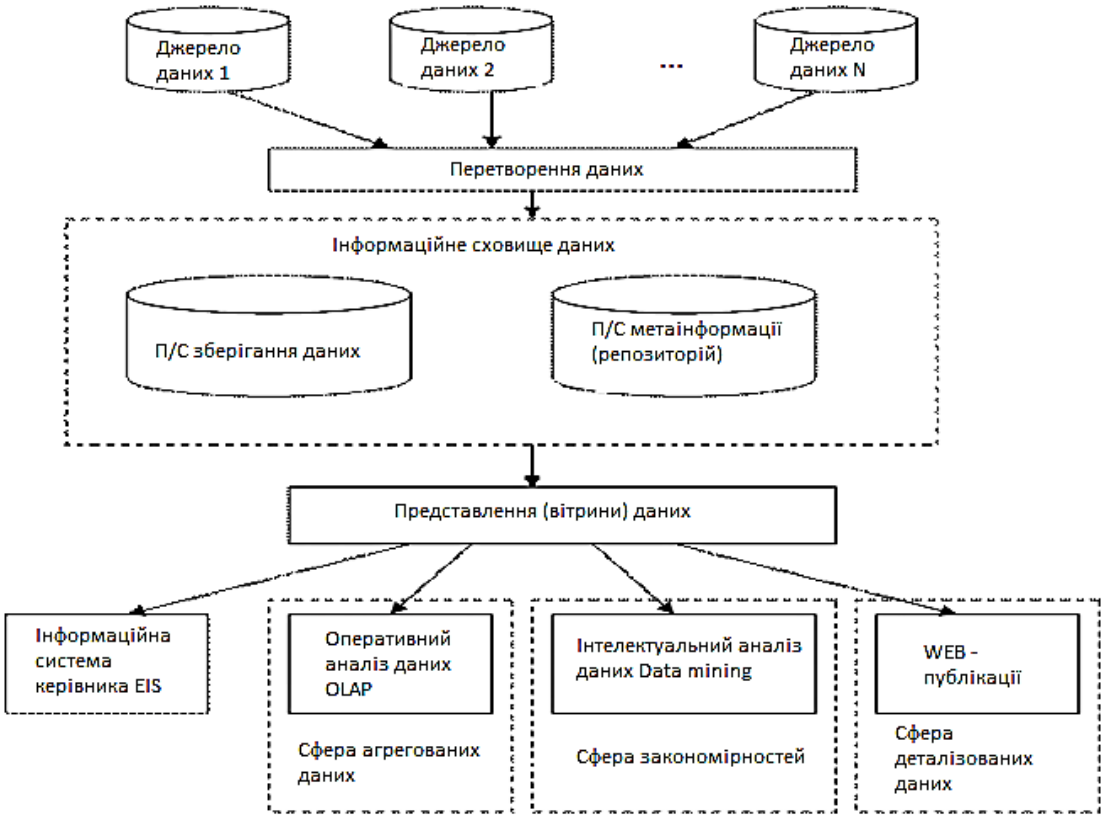


Рис.1.15. Повна структура ІАС

Підсистема зберігання даних (інформаційного сховища-ІХ)

Багатовимірне сховище даних може бути організовано у вигляді однієї з наступних структур:

1. **фізичної структури,** названої **MOLAP,** у яку з певною періодичністю завантажуються дані з файлів – джерел, що належать базам оперативних даних;
2. **віртуальної структури,** названої **ROLAP,** яка динамічно використовується при запитах. ROLAP – система розглядається просто як надбудова над реляційними базами даних, що забезпечує зручний інтерфейс користувача. Типовими інструментальними засобами, що підтримують ROLAP, є Business Objects**;**
3. **гібридної структури,** названою **HOLAP,** яка використовується при побудові багаторівневих інформаційних сховищ, застосовуваних на різних рівнях керування більших корпорацій.

Аналіз параметрів використання ROLAP і MOLAP інформаційних сховищ показує, що впровадження й експлуатація ROLAP - систем є більш простим і дешевим у порівнянні з MOLAP – системами, але уступають останнім в ефективності оперативного аналізу даних.

Підсистема метаінформації

Репозиторій являє собою опис структури інформаційного сховища: ***складу показників, ієрархії агрегацій вимірів, форматів даних, використовуваних функцій, фізичного розміщення на сервері, прав доступу користувачів, частоти відновлення.***

У репозиторії задається ***схема відображення структури файлів-джерел даних на структурі ІХ***, а також ***схема відображення структури ІХ*** **на вітринах даних**. Через репозиторій здійснюється ***інтерпретація запитів до ІХ на проведення оперативного аналізу даних.***

Підсистема перетворення даних (завантаження сховища)

Підсистема завантаження ІХ створюється тільки для MOLAP – систем. Для ROLAP – систем у процесі виконання запитів здійснюється **перетворення даних з файлів – джерел**. У тому й іншому випадках потрібне виконання наступних основних функцій:

- збір даних -передбачає передачу даних з джерел в ІХ відповідно до схеми відображення, представленої в репозиторії.

- очищення даних-здійснюється перевірка цілісності, виключення дублювання даних, відбраковування випадкових даних, відновлення відсутніх даних, приведення даних до єдиного формату.

- агрегування даних-(в разі необхідності агрегування даних) здійснюється підсумовування підсумків по заданим в репозиторії ознакам.

Підсистема вистави даних (організація вітрин даних-ВД)

Під **ВД** розуміється предметно-орієнтоване **сховище даних**, як правило, на **агреговану інформацію**, призначене для використання групою користувачів **у рамках конкретного виду діяльності підприємства**. Як правило, ВД є підмножинами загального сховища даних компанії, яке служить для них джерелом. Звичайно загальне ІХ і ВД розробляються паралельно.

Підсистема оперативного аналізу даних

Підсистема оперативного аналізу даних, як правило, використовується особами, що підготовляють інформацію **для прийняття рішень**, **шляхом виконання різних статистичних угруповань вихідних даних**.

У рамках користувацького інтерфейсу для оперативного аналізу даних використовуються наступні **базові операції**:

Поворот. Додавання нового ознаки аналізу.

Проекція. Вибірка підмножини, яка задається сукупністю вимірювань. При цьому значення, що лежать на осі проекції, підсумовуються.

Розкриття. Здійснюється декомпозиція ознаки агрегації на компоненти, наприклад, ознака року розбивається на квартали. При цьому автоматично деталізуються числові показники.

Згортка. Операція зворотна розкриттю. При цьому значення детальних показників підсумовуються в агрегований показник.

Перетин або зріз. Виділення підмножини даних за конкретним значенням одного або декількох вимірювань.

Підсистема інтелектуального аналізу даних

Підсистема інтелектуального аналізу даних **використовується** спеціальною категорією **користувачів – аналітиків**, які на основі їх **виявляють закономірності в діяльності підприємства і на ринку**, **використовувані надалі для обґрунтування стратегічних і тактичних рішень**.

Інтелектуальний аналіз вимагає **більш складні методи аналізу в порівнянні зі статичними угрупованнями** й виконується шляхом проведення безлічі сеансів.

Типовими завданнями інтелектуального аналізу даних є:

- ***Встановлення кореляцій, причинно-наслідкових зв'язків і тимчасових зв'язків подій***, наприклад визначення місця розташування прибуткових підприємств.
- ***Класифікація ситуацій, що дозволяє узагальнювати*** конкретні події в класи, наприклад визначення типового профілю покупця конкретних видів продукції.
- ***Прогнозування розвитку ситуацій***, наприклад прогнозування цін, обсягів продажів, виробництва.

До **основних методів інтелектуального аналізу даних** ставляться:

- Методи багатовимірного статистичного аналізу,
- **Індуктивні методи побудови дерева рішень**,
- Нейронні мережі.

Підсистема «Інформаційна система керівника»

Інформаційна система керівника призначена **для осіб, що безпосередньо ухвалюють рішення**. Тому інтерфейс таких систем повинен бути найбільшою мірою спрощеним. Звичайно в якості інтерфейсу керівникам підприємства пропонується **набір стандартних звітів і графіків**, які настроюються на потреби керівника через систему меню. Часто у якості інтерфейс пропонується **діаграма Ісікава**, яка представляє собою дерево показників , яке само розвивається, а листя його гілок розфарбовуються в різні кольори і символізують характер стану показника (нормальний, тривожний).Аркуш будь-якої галузі дерева може також бути розгорнутий у таблицю значень показника або графіка.

Підсистема WEB – публікації

Підсистема WEB – публікації припускає перетворення отриманої з їхньої інформації в HTML – вид, доступний для її перегляду вилученими клієнтами за допомогою браузерів Інтернету.

1.3.3. Архітектури сховищ даних в інформаційно-аналітичній системі

Концепції єдиного інтегрованого сховища й багатьох вітрин даних

В 1994 році M. Demarset запропонував об'єднати дві концепції: ***єдиного інтегрованого сховища*** і пов'язаних з ним ***вітрин, які*** одержують із нього інформацію, даних. У такому варіанті є велике інформаційне сховище агрегованої і переробленої інформації, яке може задовольнити потенційні запити по окремих напрямках діяльності.

Перевагою є: дані заздалегідь агрегуються і забезпечується їх єдина хронологія, погоджені різні формати, усуваються суперечливість і неоднозначність даних; інформація здобуває необхідну перевагу для швидкого й досить повного задоволення безлічі запитів.

Недоліком є необхідність застосування високопродуктивних апаратних засобів і спеціалізованих багатомірних або гібридних програмних інструментальних засобів.

У такому варіанті **ІАС здобуває ієрархічну багаторівневу структуру, що містить наступні рівні**:

- загально корпоративне централізоване сховище-ЦХД;
- вітрини даних по напрямках діяльності;
- локальні або регіональні бази і сховища -ХД;
- операційні бази даних, автоматизовані робочі місця (АРМ) користувачів автономних програм і ІС.

В останні роки у світі сформувався **ряд нових концепцій зберігання й аналізу корпоративних даних:**

1) **Сховища даних**, або Склади даних (Data Warehouse);

2) **Оперативна аналітична обробка** (On-Line Analytical Processing, **OLAP**);

3) **Інтелектуальний аналіз даних -ІАД** (Data Mining).

Технології OLAP тісно пов'язані з технологіями побудови Data Warehouse і методами інтелектуальної обробки - **Data Mining**. Тому найкращим варіантом є комплексний підхід до їх впровадження.

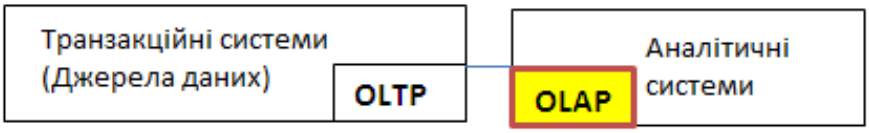
Пунктам концентрації інформації відповідають **ієрархічні рівні використання даних при підготовці, прийнятті й реалізації рішень**, які супроводжують функціонування підприємства (компанії).

Розрізняють:

-**рівень осіб, що ухвалюють рішення, який може бути сполучений з рівнем вітрин даних**;

-**рівень робочих місць аналітиків і інших зацікавлених користувачів**.

Достаток різних підходів, методів і рекомендацій приводять до деякої плутанини понять, достоїнств, недоліків і границь застосовності тих або інших архітектурних рішень. Необхідне розуміння **місця OLAP**, компонентів архітектури **сховищ даних (ХД), віртуальнихсховищ ХД** і **незалежних вітрин даних**, які широко використовуються в ІАС.



Місце OLAP в архітектурі: *посередник між* ***транзакцій ними системами- джерелами даних*** *і* ***клієнтськими додатками!?***

Транзакційна система -це система обробки транзакцій у реальномучасі**. транзакційна система**, як правило, містить **два типи таблиць**.

Один тип ***відповідає за швидкі транзакції (швидку обробку інформації)***. **Інший тип таблиць** ***використовується в основному аналітиками.*** *Наприклад,* ***фінансовими фахівцями*** *- раз на місяць, наприкінці року, або коли необхідно підвести підсумки діяльності організації.* **Обсяги** ***даних,*** *необхідних для аналізу,* ***перевищують розмір середньої транзакції при швидкій обробці інформації на кілька порядків величини***, тобто **під час виконання аналітичних робіт** ***час відгуку системи на запит*** значно ***збільшується.***

Створення систем OLAP (з резервом обчислювальної потужності) *зменшив негативний вплив аналітичного навантаження на транзакційну активність і* ***привело до значного подорожчання комплексу****, при тому, що* ***надлишкова потужність більшу частину часу залишається незатребуваної. Тому підтверджувалася необхідність поділу аналітичних і транзакційних систем при обробці інформації.***

Однак незабаром з'ясувалося, що ***OLAP - системи дуже погано справляються з роллю посередника між різними транзакційними системами - джерелами даних і клієнтськими додатками.***

Виникла необхідність створення середовища зберігання аналітичних даних (рис.1.16), тому що не забезпечувалася єдність бази даних**.** Так з'явилися **сховища даних**, призначені для надійного зберігання інформації, і **системи**

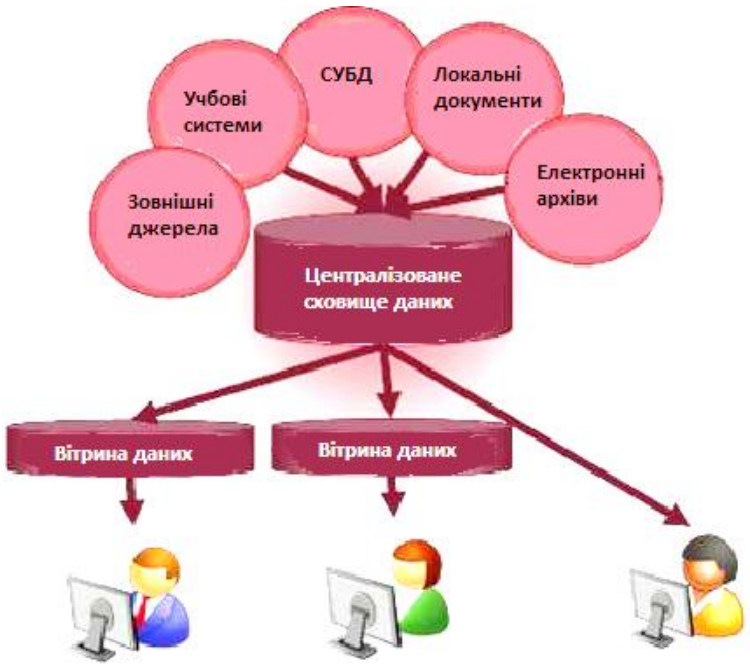


Рис.1.16. Схема ХД із вітринами даних

витягу, очищення й завантаження даних - ETL. А **OLAP -** системи вже працювали після сховищ даних (рис.1.17).

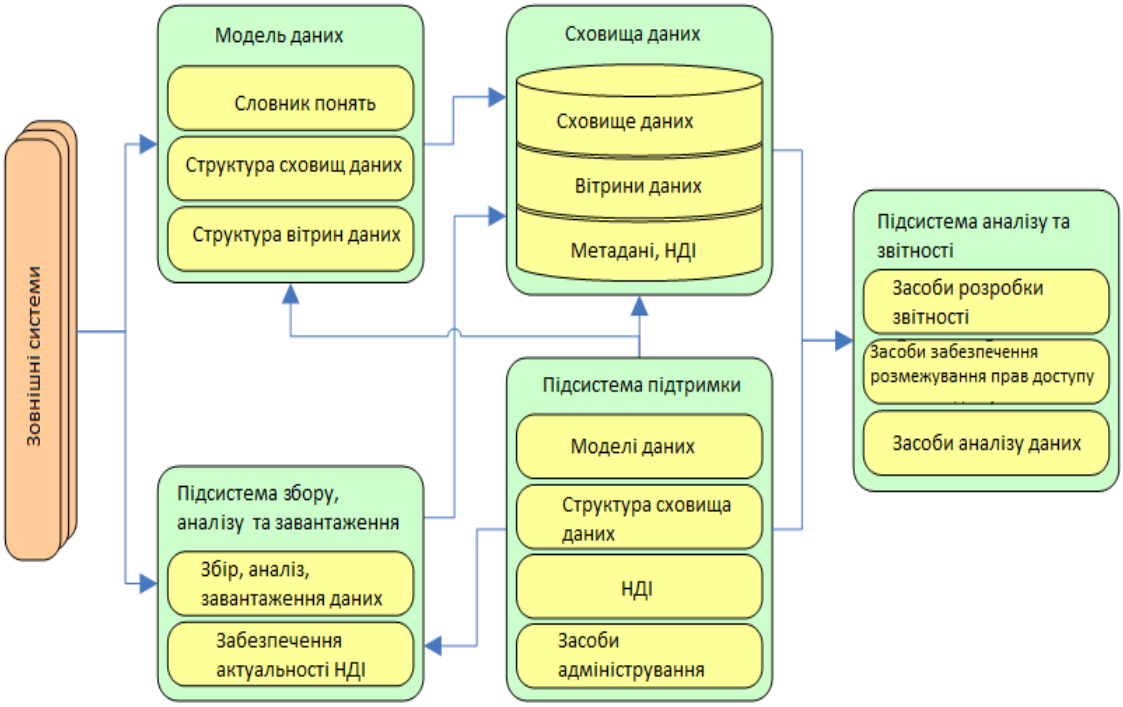


Рис.1.17. Дані в ІАС

З метою виключення втрат через несанкційний доступ і забезпечення комбінації надійності зберігання і *вимог по швидкому інформаційному обслуговуванню в сховище- були розроблені ще* **вітрини даних (ВД).**

Наповнення вітрин зі сховища може відбуватися під час спаду активності користувачів. У випадку збою інформація може бути легко відновлена з мінімальними втратами. **Поява ВД**- як вихід з положення, коли різні користувацькі додатки потребують ***різних форматів даних: багатомірні масиви даних, двовимірні масиви, реляційні таблиці, файли у форматі MS Excel...***

У той же час вітрини даних можуть також ***обслуговувати завдання звітності, статистичного аналізу, планування, сценарних розрахунків, і, у тому числі, багатомірного аналізу (OLAP).***

Еволюція розуміння місця OLAP в архітектурі обробки даних з 1993р. по теперішній час представлена на рис.1.18.

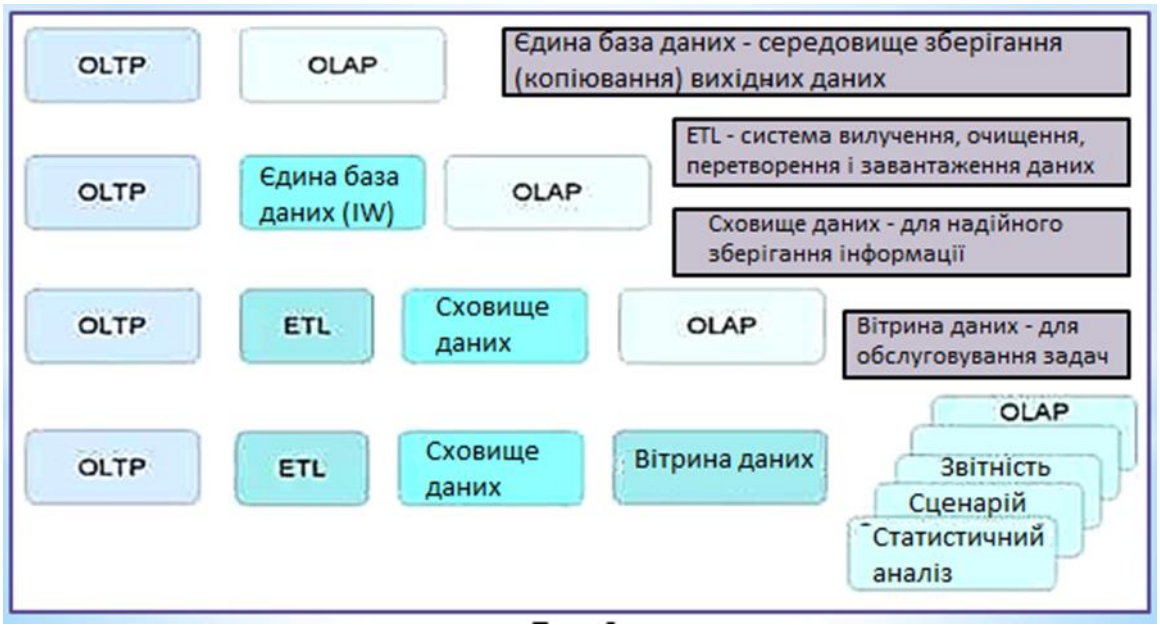


Рис.1.18. Еволюція розуміння місця OLAP в архітектурі обробки даних

Реально є **різні архітектури сховищ даних,** *наприклад:* ***архітектури корпоративного сховища даних на шести рівнях*** **(в організації може бути їх трохи)**, тому що, незважаючи на те, що самі компоненти можуть відсутні, або зберігаються в іншому виді.

Рис.1.19. Схема архітектури корпоративного сховища даних

Опис рівнів архітектури сховища даних

1. **Джерела даних -** ***транзакційні і успадковані системи, архіви, розрізнені файли відомих форматів, документи MS Office, інші джерела структурованих даних.***

2.**ETL**- *повинна мати високу пропускну здатність і обчислювальною продуктивністю, забезпечувати паралелізм обчислень і* ***працювати із кластерами, обчислювальними гридами.***

3.**Зберігання даних – забезпечує** *надійність, захист від несанкціонованого доступу.* **(Зони тимчасового зберігання -** *буферні бази*

даних, завантаження даних через контролер - потрібно **створення додаткових засобів**: адміністрування, моніторингу, забезпечення безпеки й аудита*).*

4.**SRD(ETL-2)** – виконують ***вибірку*** *(зі сховища даних),* ***реструктуризацію*** *(приведення до єдиного формату* ***SRD і*** *у відповідність із вимогами різних додатків) і* ***доставку*** *даних(у вітрини - відповідно до прав доступу, графіком доставки й вимогами до їхнього складу).*

*5.***Рівень надання даних** **-** *для поділу функцій зберігання й обслуговування різних завдань.***(Вітрини даних –** *для роздільної транзакційної і аналітичної обробки даних за ознаками обслуговуючих завдань).*

*6.***Рівень бізнес-додатків** представлений сценарними *розрахунками й статистичним аналізом, багатомірним аналізом, засобами планування й підготовки звітності.*

(Довідка:

Грид-Обчислення *(англ. grid — ґрати, мережа) — це форма розподілених обчислень, у якій «віртуальний* ***суперкомп'ютер» представлений у вигляді кластерів з'єднаних за допомогою мережі,*** *слабозв'язанных комп'ютерів, що працюють разом для виконання величезної кількості завдань (операцій, робіт).*

Кластер *— група комп'ютерів, об'єднаних високошвидкісними каналами зв'язку, що й представляє з погляду користувача* ***єдиний апаратний ресурс.)*****.**

На сьогоднішній день існує **два основні підходи до побудови архітектури Сховищ даних.** Це так звана **корпоративна інформаційна фабрика** (Corporate Information Factory, сорочене- CIF) **Білла Инмона** і

сховище даних з архітектурою шини (Data Warehouse Bus, сокр. BUS) **Ральфа Кімболла** (Ralph Kimball).

Білл Инмон (Bill Inmon), що нині одержав загальне визнання **як "батько концепції Сховища даних**", в 1991 р. спочатку називав сховища даних "**сховищами інформації**" (information warehouse).

Нові ідеї (причини й необхідність **) удосконалювання сховищ:**

1.Скорочення витрат:

- **Немає необхідності витрачати засоби на дороге встаткування для центрального ХД.**

- **Не треба містити висококваліфікований персонал,** що обслуговує це сховище.

- **Не потрібні серверні приміщення з дорогим устаткуванням систем** охолодження, пожежогасіння й моніторингу**.**

2.Треба працювати із самими свіжими даними:

- **Аналітичні системи повинні прямо працювати із джерелами даних,** минаючи всіх посередників.

- **У експертів немає довіри й до програм-посередників** -працювати тільки напряму з даними.

3. Усе, що необхідно, буде створено заново. Потрібно мати тільки робочу станцію й доступ до джерел даних, а також компілятор (програму або технічний засіб - для перекладу програми із проблемно-орієнтованої мови на машинно-орієнтовану мову).

Головне завдання: розробити програму, яка по запиту користувача буде сама ***звертатися до всіх джерел,*** сама буде *доставляти дані на користувацький комп'ютер*, сама буде ***перетворювати незбіжні формати*, сама буде *виконувати аналіз даних***, і сама ж *покаже все на екрані!?*

У цей час широке використовується **модель ХД із ВД** (див. рис.1.20).

Її **переваги**:

- знижує навантаження, *як по кількості користувачів, так і за обсягом даних у сховище;*

-кількість користувачів *знижується із сотень і тисяч до десятків вітрин*;

- при використанні засобів SRD кількість користувачів скорочується до одиниці, *уся логіка інформаційного постачання вітрин зосереджує в SRD.*

Рис.1.20. Розширена модель ХД із вітринами даних(ВД)

Архітектура сучасного сховища даних повинна задовольняти багатьом ***функціональним і нефункціональним вимогам***, які залежать від розв'язуваних ними конкретних завдань.

Принципи модульного конструювання ХД:

- **захищеність і надійність зберігання даних (**цінність інформації порівнянна з ринковою вартістю організації**);**
- **забезпечення якості даних**- *повні, точні і відтворені дані, доставлені в строк туди, де вони потрібні* (вимагає інвестицій і сприяє одержанню прибутку);
- **бути доступними співробітникам** (в обсязі, необхідному й достатньому для виконання своїх функціональних обов'язків);
- **забезпечення єдиного розуміння співробітниками даних** (повинне бути встановлений єдиний значеннєвий простір);

- **по можливості, усувати конфлікти в кодуваннях даних у системах і джерелах.**

Засоби ETL забезпечують *повний, надійний, точний збір інформації із джерел даних завдяки зосередженій у ній логіці збору, обробки й перетворення даних і взаємодії із системами ведення метаданих і НСІ.*

Система ведення метаданих підтримує актуальність бізнес-метаданих, технічних, операційних і проектних метаданих.

Система ведення НСІ *усуває конфлікти в кодуванні даних.*

Центральне сховище даних *несе тільки навантаження по надійному захисту і зберіганню даних.*

Засоби вибірки, реструктуризації й доставки даних (SRD) - єдиний користувач ЦХД, працює на заповнення вітрин даних і, тим самим знижуючи навантаження на ЦХД по обслуговуванню запитів користувачів.

Вітрини даних містять дані в структурах і форматах, оптимальних для вирішення завдань користувачів даної вітрини. Багаторазове повторення даних у вітринах не створює проблем по їхнім обслуговуванню.

Головні переваги цієї архітектури:

- надання доступу для зручної роботи користувачів з необхідним обсягом даних;

- можливість швидкого відновлення вмісту вітрин зі ЦСД при збої вітрини;

- забезпечення роботи користувачів при відсутності зв'язку зі ЦСД.

Місце OLAP в інформаційній структурі підприємства

Термін "OLAP" нерозривно пов'язаний з терміном "сховище даних" (Data Warehouse).

Дані в **OLAP** -сховище попадають **із оперативних систем** (OLTP-Систем), які призначені для автоматизації бізнес-процесів. Крім того, сховище може поповнюватися **за рахунок зовнішніх джерел**, наприклад статистичних звітів.

Завдання OLAP -сховища - надати всі вихідні дані для аналізу в одному місці й у простій, зрозумілій структурі, тобто здійснити **централізацію й зручне структурування даних.**

Є причина, що виправдовує появу окремого сховища - **складні аналітичні запити до оперативної інформації** гальмують поточну роботу компанії, надовго блокуючи таблиці й захоплюючи ресурси сервера.

Друга причина: **традиційні звіти**, побудовані на основі єдиного сховища, **позбавленого - гнучкості**. Їх не можна "покрутити", "розгорнути" або "згорнути", щоб одержати бажану виставу даних.

У якості інструмента, що **усувають** ці причини, виступає OLAP, що представляє собою необхідний атрибут **сховища даних, для аналізу накопичених у** цьому сховищі відомостей.

Місце OLAP в інформаційній структурі підприємства показане на рис.1.21.

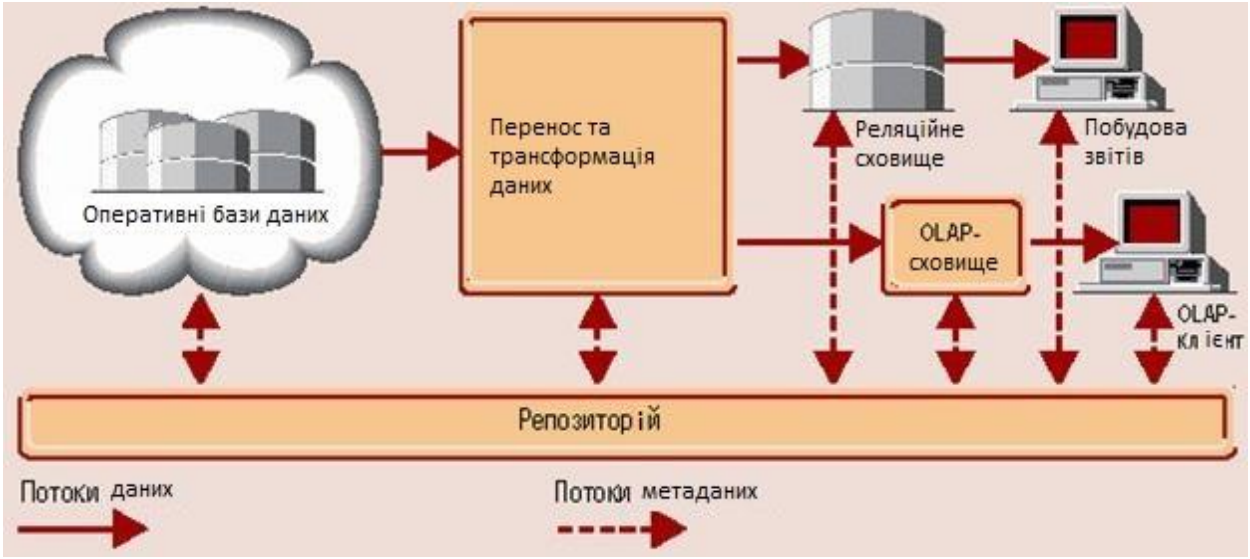


Рис.1.21. Місце OLAP в інформаційній структурі підприємства

Оперативні дані **збираються з різних джерел, очищаються, інтегруються й складаються в реляційне сховище**. При цьому вони вже доступні для аналізу за допомогою різних засобів побудови звітів. Потім дані (повністю або частково) **підготовляються для OLAP**. Вони можуть бути

завантажені в спеціальну **БД OLAP** або залишені **в реляційному сховищі**. Найважливішим його елементом є метадані, тобто інформація про структуру, розміщення й трансформації даних. Завдяки ним забезпечується ефективна взаємодія різних компонентів сховища.

OLAP застосовується скрізь, де є завдання аналізу багатофакторних даних. Взагалі, при наявності деякої таблиці з даними, у якій є **хоча б один описовий стовпчик (вимір) і один стовпчик із цифрами (заходи або факти) OLAP -** Інструмент, як правило, буде **ефективним засобом аналізу і генерації звітів.**

Деякі сфери застосування OLAP -Технологій:

1. Продажу
2. Закупівлі
3. Ціни
4. Маркетинг
5. Склад
6. Рух грошових коштів
7. Бюджет
8. Бухгалтерські рахунки
9. Фінансова звітність
10. Відвідуваність сайту
11. Обсяги виробництва
12. Споживання видаткових матеріалів
13. Використання приміщень
14. Плинність кадрів на підприємстві
15. Пасажирські перевезення

Інтелектуальний аналіз даних

Важко переоцінити значення даних в управлінні бізнесом або виробництвом, у банківській справі, у вирішенні наукових, інженерних і медичних задач. Потужні комп'ютерні системи, які зберігають і керують

величезними базами даних, стали невід'ємним атрибутом життєдіяльності, як великих компаній, так і навіть невеликих організацій.

Проте, наявність даних саме по собі ще недостатньо для поліпшення показників роботи. Потрібно вміти трансформувати дані в корисну інформацію для прийняття важливих бізнес рішень.

У цьому і полягає основне **призначення технологій Data mining** ("видобуток" або "розкопка даних"). Нерідко поруч із Data Mining зустрічаються слова "**виявлення знань у базах даних**" (knowledge discovery in databases) і "**інтелектуальний аналіз даних**". Виникнення всіх зазначених термінів пов'язане з новим витком у розвитку засобів і методів обробки даних.

В основу сучасної технології Data Mining **покладена концепція шаблонів (паттернов), що** відбивають ***фрагменти багатоаспектних відносин у даних***. Ці шаблони являють собою ***закономірності, властиві підвибіркам даних***, які можуть бути **компактно виражені в зрозумілій для людині формі**. Data Mining — це процес виявлення в даних раніше невідомих, нетривіальних, практично корисних і доступних інтерпретації знань, необхідних для прийняття рішень у різних сферах людської діяльності.

У загальному випадку процес інтелектуального аналізу даних – ІАД складається із трьох стадій (рис.1.22):

- **виявлення закономірностей** (вільний пошук);
- **використання виявлених закономірностей** для передбачення невідомих значень (прогностичне моделювання);
- **аналіз виключень**, призначений для виявлення і тлумачення аномалій у знайдених закономірностях.

Вільний пошук визначається як процес дослідження вихідної БД на предмет закономірностей без попереднього визначення гіпотез щодо виду цих закономірностей. Програма здійснює пошук аномалій, або шаблонів у даних, звільняючи аналітика від необхідності обмірковування й завдання відповідних запитів. Цей підхід особливо коштовний при дослідженні більших баз даних і їх пошук розкриває загальні закономірності, тобто є **індуктивним.**

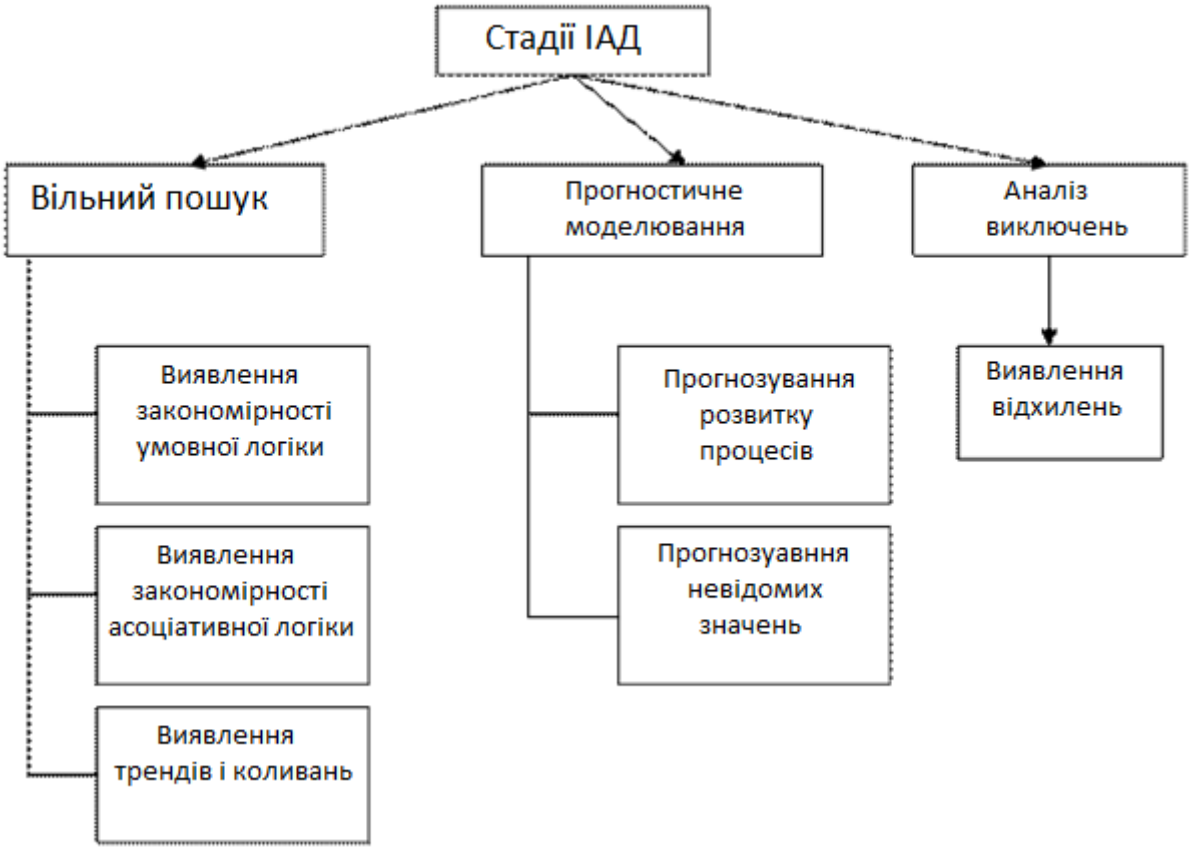


Рис.1.22. Стадії процесу інтелектуального аналізу даних (ІАД)

Прогностичне моделювання (Predictive Modeling) - коли використовуються знайдені в БД закономірності, які застосовуються для передбачення невідомих значень (передбачення, як здогадки про значення величин, цей підхід - **дедуктивний:**

1. При класифікації нового об'єкта (віднести його до певної групи результатів за відомими значеннями його атрибутів;

2. При прогнозуванні динамічного процесу (за результатами визначення періодичності змін можуть бути винесені припущення про ймовірний розвиток деякого динамічного процесу в майбутньому.

Аналіз виключень (Forensic Analysis)

Предметом даного аналізу є **аномалії в розкритих закономірностях**, тобто ***непояснені виключення***. Щоб знайти їх, слід спочатку визначити норму (стадію вільного пошуку), слідом за чим виділити її порушення.

Методи ІАД

Усі методи ІАД підрозділяються на **дві великі групи за принципом роботи з вихідними навчальними даними** (рис. 1.23).

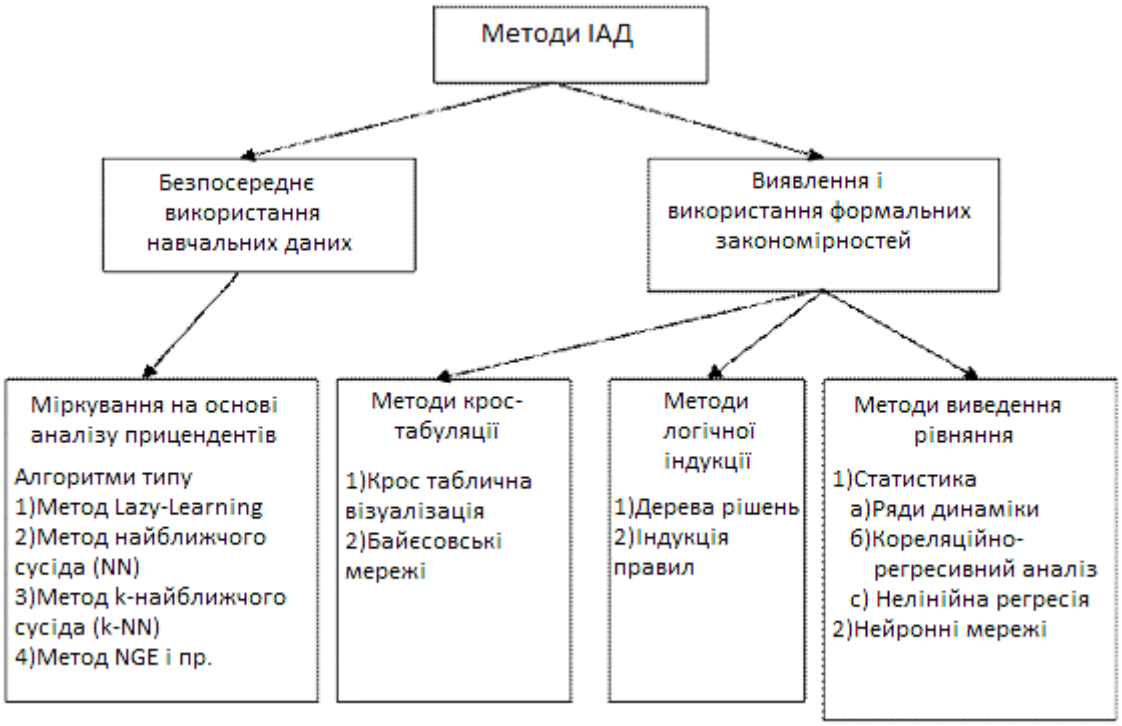


Рис.1.23. Класифікація технологічних методів ІАД

У першому випадку вихідні дані можуть зберігатися *в явному деталізованому вигляді* і безпосередньо використовуватися для прогностичного моделювання і/або аналізу виключень; це так звані **методи міркувань на основі аналізу прецедентів**. Головною проблемою цієї групи методів є ускладненість їх використання на більших обсягах даних, хоча саме при аналізі більших сховищ даних методи ІАД приносять найбільшу користь.

У другому випадку інформація *спочатку витягується з первинних даних і перетворюються в деякі формальні конструкції* (їх вигляд залежить від конкретного методу). Згідно з попередньою класифікацією, цей етап **виконується на стадії вільного пошуку**, яка в методах першої групи в принципі відсутня. Таким чином, **для прогностичного моделювання і аналізу виключень використовуються результати цієї стадії**, які набагато більш компактні, чим самі масиви вихідних даних.

Методи логічної індукції

Методи даної групи - найбільш виразні при оформленні знайдених закономірностей у максимально "прозорому" вигляді. Результатами застосування логічної індукції можуть бути **побудовані дерева рішень або зроблені набори символьних правил.**

Дерева рішень

Дерева рішень є **спрощеною формою індукції логічних правил**. Основна ідея їх використання полягає ***в послідовному поділі навчальної множини на основі значень обраного атрибута***, у результаті чого будується дерево, що містить:

- **термінальні вузли** (вузли відповіді), що задають імена класів;
- **нетермінальні вузли** (вузли рішення), які включають тест для певного атрибуту з відгалуженням до піддерева рішень для кожного значення цього атрибута.

У такому вигляді дерево рішень визначає класифікаційну процедуру природно: **будь-який об'єкт зв'язується з єдиним термінальним вузлом.** Цей **зв'язок починається з кореня, проходить шлях по дугах, яким відповідають значення атрибутів, і доходить до вузла відповіді з іменем класу.**

Популярність дерев – **у швидкості їх побудови й легкості використання при класифікації.**

Популярність Data mining?

Необхідність автоматизованого інтелектуального аналізу даних стала очевидною.

1. ***У першу чергу через величезні масиви історичної інформації, що*** й знову збирається. Важко навіть приблизно оцінити обсяг щоденних даних, що накопичуються різними компаніями, державними, науковими й медичними організаціями. Людський розум, навіть такий тренований, як розум професійного аналітика, просто не в змозі вчасно аналізувати настільки величезні інформаційні потоки.

2. ***Іншою причиною росту популярності data mining є об'єктивність одержуваних результатів***. Людині-аналітику, на відміну від машини, завжди властивий суб'єктивізм, він тією чи іншою мірою є заручником вже сформованих уявлень. Іноді це корисно, але частіше приносить і велику шкоду.

3. ***І, нарешті, data mining , що дешевше***. Виявляється, що вигідніше інвестувати гроші в рішення data mining, ніж ***постійно утримувати цілу армію високопідготовлених і дорогих професійних статистів.***

Data mining зовсім **не виключає повністю людську роль, але значно спрощує процес пошуку знань, роблячи його доступним для більш широкого кола аналітиків**, які не є фахівцями в статистиці, математиці або програмуванні.

Типові завдання для методів ІАД

- *Прогнозування*
- *Маркетинговий аналіз*.
- *Аналіз роботи персоналу*.
- *Аналіз ефективності продажу товарів поштою*.
- *Профілювання клієнтів*.
- *Оцінка потенційних клієнтів*.
- *Аналіз результатів маркетингових досліджень*.
- *Аналіз роботи регіональних відділень компанії*
- *Порівняльний аналіз конкуруючих фірм*.

Інтеграція OLAP і ІАД

Оперативна аналітична обробка й інтелектуальний аналіз даних - дві складові частини процесу підтримки прийняття рішень. Але сьогодні **більшість систем OLAP** загострює увагу**тільки на забезпеченні доступу до багатовимірних даних**, а **більшість засобів ІАД**, що працюють у сфері закономірностей, **мають справи з одномірними перспективами даних**. **Ці два види аналізу повинні бути тісно об'єднані**, тобто системи OLAP повинні фокусуватися не тільки на доступі, але й на пошуку закономірностей при роботі з даними.

Питання для самоконтролю

1.Що таке Бізнес-Аналіз (BI, Business Intelligence) ?

2.Що таке OLAP (Online Analytical Processing)?

3.Для чого призначені ІАС на базі Olap-Технологій?

4.Покажіть схемою основні компоненти інформаційної технології обробки даних.

5.Яке основне призначення ІАС?

6.Перелічите основні функції ІАС.

7.Покажіть схемою повну структуру ІАС.

8.Які нові концепції зберігання й аналізу корпоративних даних у складі ІАС?

9.Покажіть схемою архітектуру корпоративного сховища даних на шести рівнях в ІАС і розкрийте призначення її елементів.

10.Чим відомий Білл Инмон?

11.Покажіть схемою розширену модель ХД із вітринами даних і в чому її переваги?

1.4 Оцінка ефективності управління організацією

Ефективність у широкому розумінні означає міру досягнення поставленої мети. Ефективність виявляється кількісно як ставлення отриманого ефекту до витрат за його досягнення. Приватні оцінки ефективності – це оцінки діяльності окремих складових системи чи проміжні оцінки, що дозволяють контролювати динаміку реалізації загальної мети системи. Накопичений досвід організації контролю ефективності управлінської діяльності дозволяє сформулювати сукупність щодо нього вимог:

• відповідність справі, тобто чітка орієнтація на фіксацію та оцінку конкретних показників;

• своєчасність;

• орієнтація на результат;

• гнучкість, можливість внесення до показників та процедур контролю змін, обумовлених змінною ситуацією;

• простота: оптимізація кількості фіксованих показників та простота їх вимірювання;

• економічність: витрати на контроль повинні бути порівнювані з іншими видами витрат.

Критерії, на підставі значень яких формується оцінка результатів управління, бувають кількісними та якісними. Критерії та оцінки використовуються для вдосконалення процесу прийняття рішень, системи звітності та самих процесів управління.

Насправді ефективність управління найчастіше визначається аналітичними чи експертними методами з урахуванням зіставлення значень сукупності показників (ознак).

Завдання оцінки ефективності управлінського рішення полягає у тому, щоб оцінити:

• управлінську діяльність керівництва та інших управлінських структур організації;

• політику, що проводиться управлінськими структурами організації;

• реалізацію програм та планів;

• наслідки політики та реалізації програм і планів.

1.4.1. Традиційні підходи до оцінки ефективності організації

До оцінки ефективності організації широко використовуються наступні традиційні підходи: цільовий, системний і вибірковий.

Цільовий підхід.

Передбачає визначення ефективності економічної організації її здатністю досягати заздалегідь поставлених цілей. Використовується логіка цілей і засобів англійського економіста Л РОБІНСА . У цьому підході групи в організації діють раціонально для досягнення цілей. Раціоналізм полягає **у виборі такого варіанту використання ресурсів**, який би дозволив досягти поставленої мети з найменшими витратами. Цей підхід слід використовувати в тому випадку, якщо мета чітко визначена й прогрес можна точно зафіксувати й виміряти.

Організаційна ефективність залежить від:

- якості постановки цілей, тобто відповідності намічених цілей умовам і вимогам зовнішнього середовища, можливостям підприємства й інтересам персоналу;

- сили й спрямованості мотивацій, що спонукують членів організації до досягнення цілей;

- адекватності обраних стратегій поставленим цілям;

- обсягу і якості ресурсів, використовує організація для досягнення цілей

Перші три фактори характеризують **стратегічні аспекти** організаційної ефективності, а останній – **тактичні.**

Системний підхід

Згідно з ним критерієм ефективності організації є її **здатність до адаптації.** Цей підхід зосереджує увагу на внутрішніх характеристиках організації й апелює скоріше до засобів підтримки відносин між учасниками організації, чим до цілей.

Використовуються у системному підході внутрішнє виділення ресурсів і визначення ієрархічних залежностей - правила взаємодії учасників займають центральне місце, а **оцінка витрат відступає на задній план**.

Такий підхід більш придатний для бюджетних організацій. **Недоліком системного підходу** є й те, що оцінка внутрішніх характеристик організації вимагає певного їхнього кількісного визначення.

Спроби кількісно визначити всі формальні й неформальні характеристики організації (ступінь згуртованості, ступінь раціональності ієрархічних відносин) **можуть привести до надмірного ускладнення процедури оцінки ефективності й росту витрат**, пов'язаних з нею, і це ще **не гарантує ефективної роботи організації.**

Вибірковий підхід

Труднощі використання підходу полягають в **ідентифікації стратегічних складових** (від яких найбільшою мірою залежить діяльність організації) і **в здатності встановити, як організація залежить від них**. До факторів впливу ставляться **інституціональні фактори** (економічні закони, правове поле, практика ведення бізнесу, політичні переваги й ін.), оскільки саме їхня зміна часто порушує рівновагу й зсув економічного балансу на користь тих або інших зацікавлених сторін.

Кожний з підходів має певні переваги й недоліки. Гарні результати може дати **зважена й збалансована комбінація всіх підходів, при якому недоліки одного могли б компенсуватися перевагами іншого**.

Сучасна теорія організації використовує активно свої підходи:

Ситуаційний підхід заснований на визнанні того, що в організаційній діяльності не існує єдино правильного шляху.

Організація повинна пристосовуватися до умов навколишнього середовища. Неможливо забезпечити створення таких структур, методів, типів організаційного порядку, які були б ідеально пристосовані для будь-яких часу, цілей, цінностей, ситуації.

Кожному типу управлінської ситуації, розв'язуваних завдань, зовнішнього середовища відповідають свої **оптимальні вимоги** до стану організації, **стратегія** й **структура.**

Екологічний підхід затверджує, що серед організацій «виживає найбільш пристосована», має місце процес природного добору й заміни організацій. У спрощеному вигляді даний підхід можна описати так:

- у центрі уваги дослідників перебувають не окремі організації, а групи, або популяції, організацій;
- ефективність організації визначається її здатністю виживати;
- роль навколишнього середовища у формуванні структури, стратегії організації зізнається абсолютної, уважається, що менеджмент не виявляє істотного впливу на здатність організації до виживання;
- оскільки природні й соціальні ресурси обмежені, то в процесі твердої конкуренції одні організації вціліють, а інші припинять існування.

Поряд з варіантами традиційних підходів до оцінки організаційної ефективності знаходять застосування **комплексні підходи**, **як сучасні** – вихідні з різноманіття діяльності сучасної організації і її результатів, що ставляться до самих різних сфер.

Сучасні підходи комбінують кілька показників ефективності в єдину систему, включаючи:

- **Підхід з погляду всіх економічно зацікавлених сторін** (кредитори, і постачальники, і співробітники, і власники / власники). Сильна сторона такого підходу в тому, що він **відбиває широкий погляд на організаційну ефективність (із самих різних сторін) з урахуванням факторів її розвитку як внутрішніх, так і зовнішнього середовища**.
- **Підхід з погляду конкуруючих (управлінських) цінностей** (установок), засновано на комбінуванні багатьох показників виробничого процесу й організаційної ефективності, застосовуваних на практиці й менеджерами, і фахівцями-дослідниками.

Факторами, що визначають пріоритетність критеріїв організаційної ефективності, виступають:

- вплив вищого керівництва;
- вимірність цілей;
- умови навколишнього середовища.

1.4.2. Методика оцінки ефективності управлінських рішень

При розгляді економічної ефективності (ЭЭ) методично важко визначити вартість прибавочного продукту, отриманого в результаті реалізації конкретного управлінського рішення (УР), тобто його ринкову вартість.

Реалізоване у вигляді інформації УР безпосередньо не виражається в матеріально-речовинній формі товару, послуги або знань, а створює для них умови.

Позитивний економічний ефект від УР – це економія, **негативний– збиток**.

Відомі ряд методів для виміру (точніше, оцінки) ЭЭ, серед яких частіше використовується:

– **непрямий метод зіставлення різних варіантів;**

- за кінцевими результатами;

- за безпосередніми результатами діяльності.

Непрямий метод припускає аналіз ринкової вартості УР і затратна УР шляхом аналізу варіантів УР для того самого типу об'єкта, розроблених і реалізованих приблизно в однакових умовах. УР до конкретної реалізації проходить ще багато рівнів рішення й виробництва, тому необхідно відокремити вплив суб'єктивного фактору, що гальмує або прискорювального даний процес.

Даний метод дозволяє замість ринкової вартості УР використовувати ринкову вартість зробленої продукції. Так, при реалізації двох варіантів УР

відносну економічну ефективність для першого рішення можна визначити з наступного співвідношення:

$$ЭЭ= (П2Т/ З2Т – П1Т/ З1Т) х100\% , \quad (1.1)$$

де:

П1Т – прибуток, отримана за реалізацію товару при першому варіанті УР;

П2Т – прибуток, отримана за реалізацію товару при другому варіанті УР;

З1Т – витрати на виробництво товару при першому варіанті УР;

З2Т – витрати на виробництво товару при другому варіанті УР.

Так, якщо керівник своїми рішеннями тільки підтримує виробництво на одному рівні, те економічна ефективність УР буде дорівнює нулю, а інші види ефективності при цьому можуть бути і значними, наприклад, організаційна, соціальна.

Метод визначення за кінцевими результатами заснований на розрахунках ефективності виробництва в цілому й виділенні фіксованої (статистично обґрунтованої) частини (ДО):

$$ЭЭ= (П х ДО) / ОЗ, \quad (1.2)$$

де:

П- прибуток отримана від реалізації товару;

ОЗ- загальні витрати;

ДО- частка УР в ефективності виробництва(ДО= 20-30%).

Метод визначення ЭЭ за безпосередніми результатами діяльності

заснований на оцінці безпосереднього ефекту від УР при досягненні цілей, реалізації функцій, методів і ін. Основними параметрами при оцінці ЭЭ є стандарти(тимчасові, ресурсні, фінансові й ін.). величину ЭЭ визначають зі співвідношення:

$$Ээі= Сі/ Рі х100\%, \quad (1.3)$$

де:

Сі- стандарт на використання(витрату) і – го ресурсу для розробки й реалізації УР;

Рі- реальне використання(витрати) і - го ресурсу для розробки й реалізації УР.

При розрахунках ЭЭ даним методом необхідно визначити значення ЭЭ по декільком ресурсам**(m)** і потім по пріоритетності ресурсів **(Пі)** знайти

середнє значення ЭЭ:

$$ЭЭ = (Ээі \times Пі) / m. \quad (1.4)$$

Приклади оцінки економічної ефективності управлінських ршень

Приклад 1. Компанія «Гарячий хліб» робить і продає хлібобулочні вироби й інші продукти. Керівник компанії реалізував *УР по зміні функціональних обов'язків і скоротив одного працівника.*

Іншим працівникам за виконання додаткових функцій *побільшали матеріальна винагорода.* У результаті вдосконалювання функціональних обов'язків і кращої роботи персоналу *собівартість продукції зменшилась на 1 %, а ціна виробу зменшилась на 0,5 %, але загальна ціна реалізації збільшилася на5 % через збільшення обсягу продажів.* Загальні дані наведені в табл.1.3:

Таблиця 1.3

Етап праці компанії	Спільна ціна реалізації в місяць , млн.од.	Спільні затрати в місяць, млн.од.	Прибуток, млн. од.
До реалізації УР	2,592	2,074	0,518
Після реалізації УР	2,722	2,054	0,668

Рішення: Розрахуємо економічну ефективність УР двома методами: *зіставлення кінцевих результатів* і за кінцевими результатами.

- **По методу зіставлення кінцевих результатів**:

ЭЭ= (0,668 / 2,054 – 0,518 / 2,074) х 100 % = 7,6 %.

- **По методу кінцевих результатів**(ДО= 20-30 %):

ЭЭ= (0,668 / 2,054) х 0,25 х 100 % = 8,1 %.

Приклад 2. Місцевий екскаваторний завод виробляє гусеничні землерийні машини. Збут машин зменшується, що не відповідає можливостям заводу. Керівник відділу маркетингу прийняв УР про розширення форми оплати за продукцію у вигляді лізингу (передачі виробничого обладнання у тимчасове користування лізингоодержувачу- за договором), як лізингодавець виступив сам завод. Машини стали йти із заводу швидше, чим збільшилося фінансове наповнення його розрахункового рахунку. Через рік роботи довелося відмовитися від цієї системи. І тоді головний інженер заводу *ухвалив рішення щодо створення постійної й тимчасової частин робочого персоналу.* Постійна частина персоналу працює незалежно, а *тимчасова – залежно від кількості замовлень.* Загальні дані для розрахунків наведені в табл.1.4:

Таблиця 1.4

Найменування рішення на заводі	Спільна ціна реалізації в місяць , млн.од.	Спільні затрати в місяць , млн.од.	Прибуток, млн.од.
Організація форми оплати	8,051	8,234	-0,183
Організація постійної і змінної частин персоналу	8,051	6,537	1,514

Потрібно оцінити економічну ефективність двох УР.

Задача: Розрахувати економічну ефективність УР двома методами: *зіставлення кінцевих результатів* і *за кінцевими результатами*.

Рішення.

За методом зіставлення кінцевих результатів:

- **А.** Розрахуємо економічну ефективність другого рішення щодо першого.

ЭЭ= (1,514 / 6,537 + 0,183 / 8,234) х100 % = 25,4 %.

- **Б.** Розрахуємо економічну ефективність першого рішення щодо другого**.**

ЭЭ= (- 0,183 / 8,234 – 1,514 / 6,537) х100 % = – 25,4 %.

За методом кінцевих результатів (ДО= 20-30 %):

- **А.** Для першого рішення**:**

ЭЭ= – (0,183 / 8,234) х0,25 х100 % = – 0,56 %.

- **Б.** Для другого рішення:

ЭЭ= (1,514 / 6,537) х0,25 х100 % = 5,7 %.

Приклад 3. ВАТ «Буддор» проектує й прокладає дороги місцевого й республіканського значення. Збори акціонерів прийняли постанову про початок робіт із проектування нових доріг з сучасними покриттями. У рамках даного рішення директор ВАТ виділив фінансові ресурси, персонал і техніку для проектного відділу, а також визначив час проектування. Загальні дані для розрахунків наведені в табл.1.5:

Таблиця 1.5

Стан ресурсу	Найменування ресурсу		
	Фінанси, тис.од.	Персонал, тис.од.	Оргтехніка, комплектів, тис. од.
Пріоритет	1,2	1	1,1
Виділено	200	16	9
Використано	220	13	8

Потрібно оцінити економічну ефективність УР.

Рішення: Розрахуємо економічну ефективність УР :

- **по кожному ресурсу**:

ЭЭ1= 200 / 220 х100 % = 90,9 %;

ЭЭ2= 16/13 х100 % = 123 %;

ЭЭ3= 9/8 х100 % = 112,5 %.

- **загальна економічна ефективність** складе:

ЭЭ= (90,9 х1,2 + 123 х1 + 112,5 х1,1) / 3 = 118,6 %.

Завдання для самостійного рішення

Задача . Компанія «Ласунка» робить і продає кондитерські вироби різних найменувань. Керівник компанії реалізував УР по зміні функціональних обов'язків і скоротив одного працівника.

Іншим працівникам за виконання додаткових функцій побільшили матеріальну винагороду. У результаті вдосконалювання функціональних обов'язків і кращої роботи персоналу собівартість продукції зменшилась на 2 %, а ціна виробу теж зменшилась на 0,7 %, але загальна ціна реалізації збільшилася на 3 % через збільшення обсягу продажів. Загальні дані наведені в табл. 1.6**:**

Таблиця 1.6

Етап праці компанії	Спільна ціна реалізації в місяць , млн.од.	Спільні затрати в місяць, млн.од.	Прибуток, млн.од.
До реалізації УР	2,383	2,174	0,613
Після реалізації УР	2,578	2,154	0,705

Потрібно оцінити економічну ефективність УР.

Задача-Ситуація. Компанія ВАТ «Азіяпак» 8 років успішно працює на ринку України. Вона займається виробництвом і продажем пакувального матеріалу для рідких харчових продуктів, а також забезпечує зацікавлені компанії технологічним устаткуванням по виробництві пакувального матеріалу. У компанії працює 1040 людей. Компанія має одну філію в Сахно. В 2013 р. чистий прибуток компанії склав20 млн. руб. при валовому доході140 млн. грн. і витратах120 млн. грн.

Директорат компанії за підсумками 2020 р. обговорював питання про збільшення доходу. На голосування було винесено три альтернативні УР:

1. Організувати ще дві філії – одну у м. Миколаєві, а іншу в м. Слов'янці. За результатами маркетингових досліджень у цих містах є великий і довгочасний попит на продукцію компанії;

2. Розібратися в управлінській і виробничій діяльності компанії, навести там порядок, знизити витрати й посилити адміністративну і технологічну дисципліну;

3. Зробити ставку на поліпшення умов роботи персоналу,

стимулювання їх продуктивної праці й творчої діяльності по принципу: «Спочатку стимулювання, а потім- продуктивність». За рахунок цього можна знизити невиробничі витрати й підсилити інтелектуальний і соціальний потенціал компанії. Орієнтовні дані розрахунків наведені в табл.1.7.

Таблиця 1.7

Основні дані щодо УР, винесені на голосування

Параметри	Варіанти рішень		
	1	2	3
Валовий дохід, млн.	215	150	230
Затрати, млн.	1800	140	185
Чистий прибуток, млн.	35	10	45
Час реалізації УР, міс.	18	3	6
Соціальна стійкість	Середня	Низька	Висока
Технологічні перспективи	Високі	Низькі	Середні

Питання для самоконтролю

1.Які види ефективності було б доцільно розглянути в наведеній ситуації?

2 Які значення економічної ефективності мають запропоновані УР?

3.Які пріоритети функціональної ефективності можна запропонувати в даній ситуації?

ТЕМА 2. Застосування методологічних підходів до створення систем управління інформаційною безпекою

2.1. Методичні підходи до побудови систем захисту інформації

Однією з ознак нинішнього періоду є перехід від індустріального суспільства до інформаційного, в якому інформація стає більш важливим ресурсом, ніж матеріальні або енергетичні ресурси.

І в цих умовах основним виступає правило: **хто володіє інформацією, той володіє світом.**

У конкурентній боротьбі широко поширені різноманітні дії, спрямовані на отримання (добування, придбання) конфіденційної інформації різними способами, аж до прямого промислового шпигунства з використанням сучасних технічних засобів розвідки. Встановлено, що 47% охоронюваних відомостей видобувається за допомогою технічних засобів промислового шпигунства.

В сучасних умовах захисту інформації від неправомірного оволодіння нею відводиться далеко не останнє місце. При цьому **цілями захисту інформації** є:

- запобігання розголошенню, витоку і несанкціонованого доступу до охоронюваним відомостями;
- запобігання протиправних дій зі знищення, модифікації, спотворення, копіювання, блокування інформації;
- запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи;
- забезпечення правового режиму документованої інформації як об'єкта власності; захист конституційних прав громадян на збереження особистої таємниці та конфіденційності персональних даних, наявних в інформаційних системах;
- збереження державної таємниці, конфіденційності документованої інформації відповідно до законодавства;

- забезпечення прав суб'єктів в інформаційних процесах і при їх розробці, виробництві і застосуванні інформаційних систем, технологій та засобів їх забезпечення .

Як випливає з цього визначення цілей захисту інформації інформаційна безпека - досить ємна і багатогранна проблема, яка охоплює не тільки визначення необхідності захисту, а й те, як інформацію захищати, від чого захищати, коли захищати, чим захищати і якою має бути цей захист.

2.1.1. Концепція інформаційної безпеки

Концепція забезпечення безпеки інформації в організації визначає систему поглядів на проблему і являє собою систематизований виклад цілей і завдань захисту, основних принципів побудови, організаційних, технологічних та процедурних аспектів забезпечення безпеки інформації.

Концепція забезпечення безпеки інформації в організації є,перш за все, методологічною основою для:

- формування і проведення єдиної політики в галузі забезпечення безпеки інформації в організації;
- прийняття управлінських рішень і розробки практичних заходів щодо втіленню політики безпеки інформації і вироблення комплексу узгоджених заходів нормативно-правового, технологічного та організаційно-технічного характеру, спрямованих на виявлення, відображення та ліквідацію наслідків реалізації різних видів загроз безпеки інформації.

Інформаційна безпека-це стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держав.

Інформація - відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх подання.

Розуміючи **під безпекою** стан захищеності життєво важливих інтересів особистості, підприємства, держави від внутрішніх і зовнішніх загроз, можна

виділити і **компоненти безпеки** - такі як персонал, матеріальні та фінансові кошти і інформацію.

Аналіз стану справ у сфері захисту інформації показує, що вже склалася цілком сформована концепція і структура захисту, основу якої складають:

• добре розвинений асортимент технічних засобів захисту інформації, вироблених на промисловій основі;

• значне число мають необхідні ліцензії організацій, що спеціалізуються на вирішенні питань захисту інформації;

• досить чітко окреслена система поглядів на цю проблему;

• наявність значного практичного досвіду та ін.

І, тим не менш, як свідчать вітчизняні та зарубіжні засоби масової інформації (ЗМІ), число злочинних дій над інформацією не тільки не зменшується, а й має досить стійку тенденцію до зростання. Досвід показує, що для боротьби з цією тенденцією необхідна злагоджена й цілеспрямована організація процесу захисту інформаційних ресурсів і в першу чергу-забезпечення безпеки інформації, яке не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення та розвитку засобів захисту, безперервному контролі їх стану та виявленні їх вузьких і слабких місць. Безпека інформації може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту у структурних елементах виробничої системи і на всіх етапах технологічного циклу обробки інформації.

Найбільший ефект досягається тоді, коли всі використовувані засоби, методи і заходи об'єднуються в єдиний цілісний механізм -в **систему захисту інформації (СЗІ).** При цьому завжди треба виходити з того, що ніяка СЗІ не може забезпечити необхідного рівня безпеки інформації без належної підготовки користувачів і дотримання ними всіх встановлених правил, спрямованих на захист інформації. Концептуальна модель безпеки інформації представлена на рис.2.1.

Рис. 2.1. Концептуальна модель безпеки інформації

Основні положення Концепції повинні базуватися на якісному осмисленні питань безпеки інформації та на економічному (кількісному) аналізі ризиків і обґрунтуванні необхідних витрат на захист інформації.

У **Концепції інформаційної безпеки** повинні бути відображені наступні питання:

- характеристика організації, як об'єкта інформаційної безпеки (об'єкта захисту);
- призначення, цілі створення та експлуатації інформаційних систем (ІС) організації;
- структура, склад і розміщення основних елементів ІС організації, інформаційні зв'язки з іншими об'єктами;
- категорії інформаційних ресурсів, що підлягають захисту;
- категорії користувачів ІС організації, режими використання та рівні доступу до інформації;
- інтереси організації та суб'єктів інформаційних відносин, уражених при експлуатації ІС;
- вразливість основних компонентів ІС організації;

- цілі та завдання забезпечення інформаційної безпеки організації і основні шляхи їх досягнення (вирішення завдань системи захисту);
- перелік основних небезпечних факторів, що впливають і значущих загроз інформаційній безпеці;
- зовнішні і внутрішні діючі фактори, загрози безпеки інформації і їх джерела;
- шляхи реалізації ненавмисних суб'єктивних загроз безпеці інформації в ІС організації;
- навмисні дії сторонніх осіб, зареєстрованих користувачів і обслуговуючого персоналу;
- витік інформації по технічним каналам;
- неформальна модель можливих порушників;
- підхід до оцінки ризику в ІС організації;
- основні положення технічної політики в галузі забезпечення безпеки інформації в ІС організації;
- принципи забезпечення інформаційної безпеки організації;
- основні заходи і методи (способи) захисту від загроз, засоби забезпечення необхідного рівня захищеності ресурсів ІС;
- організаційні (адміністративні) заходи захисту;
- структура, функції і повноваження підрозділу забезпечення інформаційної безпеки;
- фізичні засоби захисту;
- технічні (програмно-апаратні) засоби захисту;
- управління системою забезпечення безпеки інформації;
- контроль ефективності системи захисту;
- першочергові заходи щодо забезпечення безпеки інформації в ІС організації;
- перелік нормативних документів, що регламентують діяльність в області захисту інформації;
- основні терміни та визначення.

З урахуванням накопиченого досвіду можна визначити **систему захисту інформації** як організовану сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

З позицій системного підходу до захисту інформації пред'являються певні вимоги. **Захист інформації повинен бути**:

- безперервним, ця вимога виходить з того, що зловмисники тільки і шукають можливість, як би обійти захист, який їх цікавить;
- плановим, планування здійснюється шляхом розробки кожною службою детальних планів захисту інформації в сфері своєї компетенції з урахуванням загальної мети підприємства (організації);
- цілеспрямованим - захищається то, що має захищатися в інтересах конкретної мети, а не все підряд;
- конкретним- захисту підлягають конкретні дані, що об'єктивно потребують охорони, втрата яких може заподіяти організації певної шкоди:
- активним, коли захищати інформацію необхідно з достатнім ступенем наполегливості;
- надійним, коли методи і форми захисту повинні надійно перекривати можливі шляхи неправомірного доступу до охоронюваних секретів, незалежно від форми їх подання, мови вираження і виду фізичного носія, на якому вони закріплені;
- універсальним, вважається, що в залежності від виду каналу витоку або способу несанкціонованого доступу його необхідно перекривати, де б він не виявився, розумними і достатніми засобами, незалежно від характеру, форми і види інформації:
- комплексним, коли для захисту інформації у всьому різноманітті структурних елементів повинні застосовуватися всі види і форми захисту в повному обсязі. Неприпустимо застосовувати лише окремі форми або технічні засоби. Комплексний характер захисту виникає з того, що захист - це специфічне явище, що представляє собою складну систему нерозривно взаємопов'язаних і

взаємно залежних процесів, кожен з яких в свою чергу має безліч різних взаємно взаємно зумовлюючих один до одного сторін, властивостей, тенденцій.

Зарубіжний і вітчизняний досвід показує, що для забезпечення виконання настільки багатогранних вимог безпеки **система захисту інформації повинна відповідати певним умовам**:

- охоплювати весь технологічний комплекс інформаційної діяльності;
- бути різноманітною по використовуваних засобів, багаторівневої з ієрархічною послідовністю доступу;
- бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації;
- бути нестандартною, різноманітною. При виборі засобів захисту не можна розраховувати на необізнаність зловмисників щодо її можливостей;
- бути простою для технічного обслуговування і зручною для експлуатації користувачами;
- бути надійною, будь-які поломки технічних засобів є причиною появи неконтрольованих каналів витоку інформації;
- бути комплексною, володіти цілісністю, що означає-жодна її частина не може бути вилучена без шкоди для всієї системи.

До системи безпеки інформації пред'являються також **певні вимоги**:

- чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;
- надання користувачеві мінімальних повноважень, необхідних йому для виконання дорученої роботи;
- зведення до мінімуму числа загальних для декількох користувачів засобів захисту;
- облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;
- забезпечення оцінки ступеня конфіденційності інформації;
- забезпечення контролю цілісності засобів захисту і негайне реагування на їх вихід з ладу.

Таким чином, система захисту інформації, як будь-яка інша система, повинна мати певні види власного забезпечення, спираючись на які, вона буде виконувати свою цільову функцію.

З огляду на це **СЗІ може мати**:

• правове забезпечення - сюди входять нормативні документи, положення, інструкції, керівництва, вимоги яких є обов'язковими в рамках сфери їх дій;

• організаційне забезпечення - мається на увазі, що реалізація захисту інформації здійснюється певними структурними одиницями - такими, як служба захисту документів; служба режиму, допуску, охорони; служба захисту інформації технічними засобами; інформаційно-аналітична діяльність та ін .;

• апаратне забезпечення, коли передбачається широке використання технічних засобів як для захисту інформації, так і для забезпечення діяльності власне СЗІ;

• інформаційне забезпечення, воно включає в себе відомості, дані, показники, параметри, що лежать в основі рішення задач, які забезпечують функціонування системи. Сюди можуть входити як показники доступу, обліку, зберігання, так і системи інформаційного забезпечення розрахункових завдань різного характеру, пов'язаних з діяльністю служби забезпечення безпеки;

• програмне забезпечення, до якого відносяться різні інформаційні, облікові, статистичні і розрахункові програми, що забезпечують оцінку наявності та небезпеки різних каналів витоку і шляхів несанкціонованого проникнення до джерел конфіденційної інформації;

• математичне забезпечення, яке передбачає використання математичних методів для різних розрахунків, пов'язаних з оцінкою небезпеки технічних засобів зловмисників, зон і норм необхідного захисту;

• лінгвістичне забезпечення, сюди входять норми і регламенти діяльності органів. служб, засобів, що реалізують функції захисту інформації; різного роду методики, що забезпечують діяльність користувачів при виконанні своєї роботи в умовах жорстких вимог захисту інформації.

Під системою безпеки інформації (рис.2.2) будемо розуміти організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз.

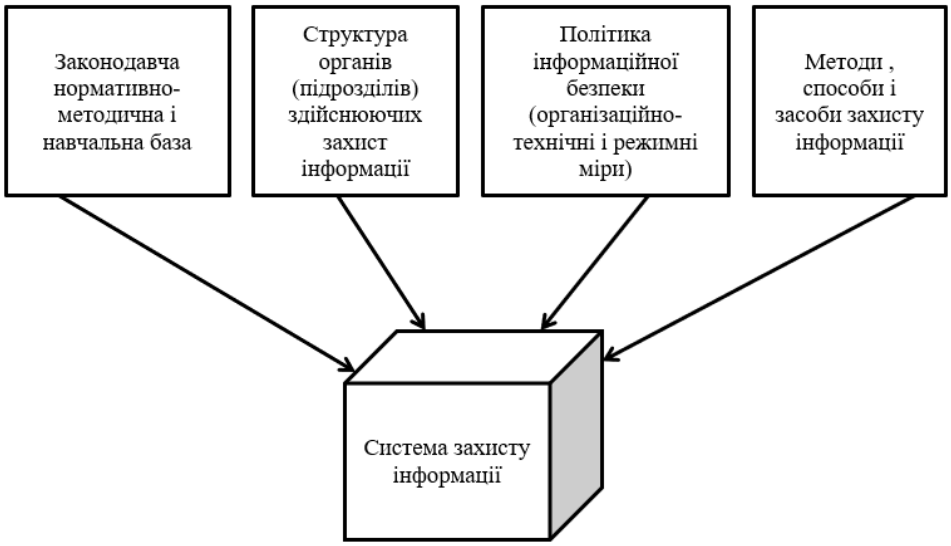


Рис.2. 2. Схема системи захисту інформації

Розуміючи **інформаційну безпеку** як стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, країни, можна визначити **загрози безпеки інформації**. джерела цих загроз, способи їх реалізації та цілі, а також інші умови і дії, що порушують безпеку. При цьому, природно, слід розглядати і заходи захисту інформації від неправомірних дій, що призводять до заподіяння шкоди.

Практика показала, що для аналізу такого значного набору джерел, об'єктів, дій доцільно використовувати методи імітаційного моделювання, при яких формується як би "заступник" реальних ситуацій. При цьому слід враховувати, що модель не копіює оригінал, вона простіше його представляє. Модель повинна бути досить загальною, щоб описувати реальні дії з урахуванням їх складності.

Можна запропонувати наступні **компоненти моделі інформаційної безпеки на першому рівні декомпозиції**:

• об'єкти загроз;

• загрози;

• джерела загроз;

• цілі загроз з боку зловмисників:

• джерела інформації;

• способи неправомірного оволодіння конфіденційною інформацією (способи доступу);

• напрямки захисту інформації;

• способи захисту інформації;

• засоби захисту інформації.

Об'єктом загроз інформаційній безпеці виступають відомості про склад, стан і діяльність об'єкта захисту (персоналу, матеріальних і фінансових цінностей, інформаційних ресурсів).

Загрози інформації виражаються в порушенні її цілісності, конфіденційності, повноти і доступності.

Джерелами загроз виступають конкуренти, злочинці. корупціонери, адміністративно-управлінські органи.

Джерела загроз переслідують при цьому наступні цілі:

- ознайомлення з охоронюваними відомостями,

- їх модифікація в корисливих цілях (спотворення),

- знищення (руйнування) - нанесення прямих матеріальних збитків.

Модель реалізації загроз інформаційній безпеці представлена на рис.2.3.

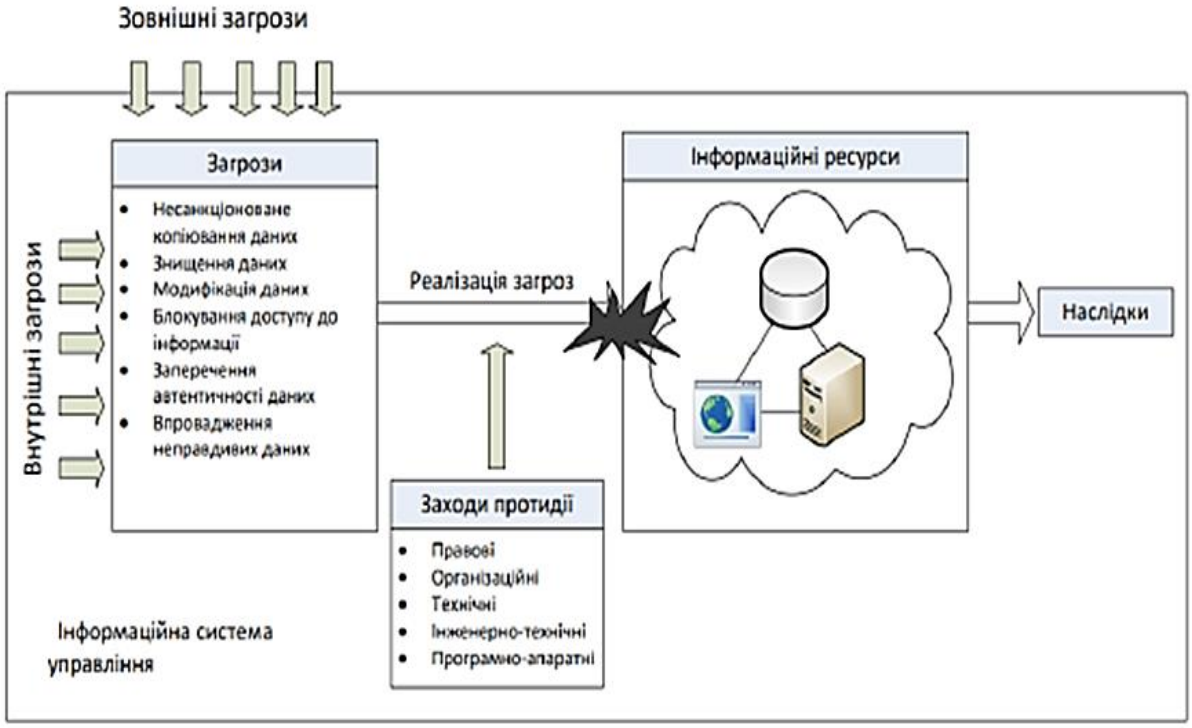


Рис. 2.3. Модель реалізації загроз інформаційній безпеці

Неправомірне заволодіння конфіденційною інформацією можливо за рахунок її розголошення джерелами відомостей, за рахунок витоку інформації через технічні засоби і за рахунок несанкціонованого доступу до охоронюваних відомостей.

Джерелами конфіденційної інформації є люди, документи, публікації, технічні носії інформації, технічні засоби забезпечення виробничої та трудової діяльності, продукція і відходи виробництва.

Основними напрямками захисту інформації є правовий, організаційний та інженерно-технічний захист інформації як виразники комплексного підходу до забезпечення інформаційної безпеки.

Засобами захисту інформації є фізичні засоби, апаратні засоби, програмні засоби та криптографічні методи. Останні можуть бути реалізовані як апаратно, програмно , так і змішано - програмно-апаратними засобами.

В якості засобів захисту виступають всілякі заходи, шляхи, способи і дії, що забезпечують попередження протиправних дій, їх запобігання, припинення та протидія несанкціонованому) доступу.

Під **загрозами конфіденційної інформації** прийнято розуміти потенційні чи реально можливі дії по відношенню до інформаційних ресурсів, що призводять до неправомірного оволодіння охоронюваними відомостями. Такими діями є:

• ознайомлення з конфіденційною інформацією різними шляхами і способами без порушення її цілісності;

• модифікація інформації в кримінальних цілях як часткова або значна зміна складу і змісту відомостей;

• руйнування (знищення) інформації як акт вандалізму з метою прямого нанесення матеріального збитку.

В кінцевому підсумку протиправні дії з інформацією призводять до порушення її конфіденційності, повноти, достовірності і доступності, що, в свою чергу, призводить до порушення як режиму, управління, так і його якості в умовах помилкової або неповної інформації.

Джерела загроз інформації і їх вплив на процеси управління інформаційною безпекою можна представити у вигляді схеми (рис.2.4).

Джерелами зовнішніх загроз є:

• недобросовісні конкуренти;

• злочинні угруповання і формування;

• окремі особи і організації адміністративно-управлінського апарату

Джерелами внутрішніх загроз можуть бути:

• адміністрація підприємства:

• персонал:

• технічні засоби забезпечення виробничої та трудової діяльності.

Співвідношення зовнішніх і внутрішніх загроз на усередненому рівні можна охарактеризувати так:

- 82% загроз відбувається власними співробітниками фірми при їх прямої або опосередкованої участі;

- 17% загроз відбувається ззовні - зовнішні загрози;

- I% загроз відбувається випадковими особами.

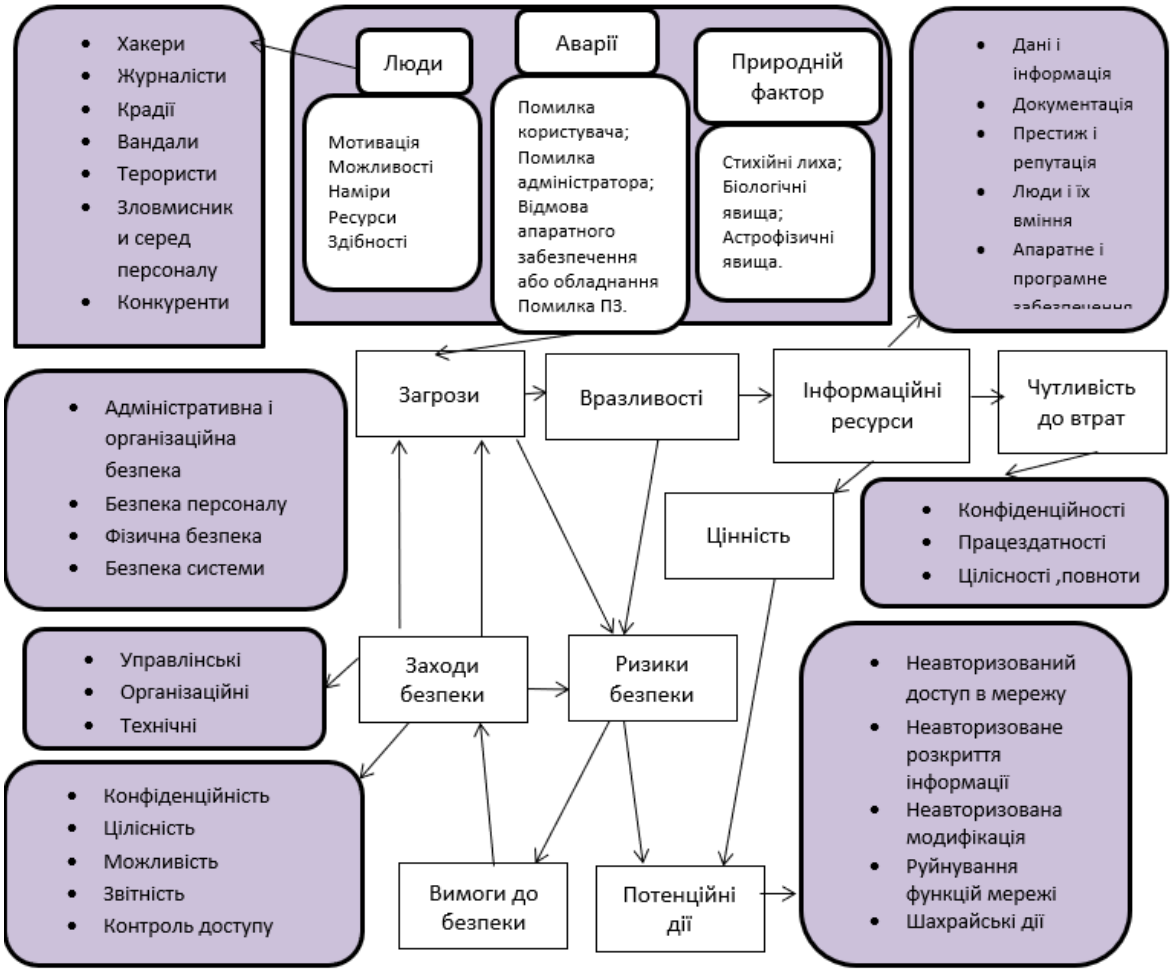


Рис.2.4. Схема джерел загроз і їх вплив на процеси управління інформаційною безпекою

До дій, що призводять до неправомірного оволодіння конфіденційною інформацією відноситься: **Розголошення, Витік, Несанкціонований доступ**.

Розголошення - це навмисні або необережні дії з конфіденційною інформацією, що призвели до ознайомлення з ними осіб, що не допущені до них. Розголошення виражається в повідомленні, передачі, наданні, пересиланні, опублікуванні, втраті і в інших формах обміну і дій з ділової та наукової інформацією. Реалізується розголошення за формальними і неформальними каналами поширення інформації. До формальних комунікацій відносяться ділові зустрічі, наради, переговори і тому подібні форми спілкування: обмін офіційними діловими і науковими документами засобами передачі офіційної інформації (пошта, телефон, телеграф і ін.). Неформальні комунікації включають

особисте спілкування (зустрічі, листування та ін., виставки, семінари, конференції і інші масові заходи, а також засоби масової інформації (преса, газети, інтерв'ю, радіо, телебачення та ін.).

Як правило, причиною розголошення конфіденційної інформації є недостатнє знання працівниками правил захисту комерційних секретів і нерозуміння (або недорозуміння) необхідності їх ретельного дотримання. Тут важливо відзначити, що суб'єктом в цьому процесі виступає джерело (власник) охоронюваних секретів.

Витік - це безконтрольний вихід конфіденційної інформації за межі організації або кола осіб, яким вона була довірена. Витік інформації здійснюється за різними технічними каналами.

Несанкціонований доступ - але протиправне навмисне оволодіння конфіденційною інформацією особою, яка не має права доступу до охоронюваних секретів. Несанкціонований доступ до джерел конфіденційної інформації реалізується різними способами: від ініціативного співробітництва, що виражається в активному прагненні продати секрети, до використання різних засобів проникнення до комерційних секретів.

Для реалізації цих дій зловмисникові доводиться проникати на об'єкт або створювати поблизу нього спеціальні пости контролю і спостереження - стаціонарні або в рухомому варіанті, обладнаних найсучаснішими технічними засобами.

З урахуванням викладеного наведемо умови, що **сприяють неправомірному оволодінню конфіденційною інформацією**:

• **розголошення** (примітивна балакучість співробітників) - 32%;

• **несанкціонований доступ** шляхом підкупу і схиляння до співпраці з боку конкурентів і злочинних угруповань - 24%;

• **відсутність на підприємстві належного контролю** і жорстких умов забезпечення інформаційної безпеки - 14%;

• **традиційний обмін виробничим досвідом** - 12%;

• **безконтрольне використання інформаційних систем** -10%;

• **наявність передумов виникнення серед співробітників конфліктних ситуацій** - 8%.

Серед форм і методів недобросовісної конкуренції найбільшого поширення мають такі:

• **економічне придушення**, що виражається в зриві угод та інших угод (48%), блокування діяльності підприємства (31%), компрометації підприємства (11%), шантажі керівників підприємства (10%);

• **фізичне придушення**: пограбування та розбійні напади на офіси, склади, вантажі (73%), погрози фізичної розправи над керівниками підприємства і провідними фахівцями (22%), вбивства і захоплення заручників (5%);

• **інформаційний вплив**: підкуп співробітників (43%), копіювання інформації (24%), проникнення в бази даних (18%), продаж конфіденційних документів (10%), підслуховування телефонних переговорів і переговорів у приміщеннях (5%), а також обмеження доступу до інформації, дезінформація;

• **фінансове придушення** включає такі поняття, як інфляція, бюджетний дефіцит, корупція, розкрадання фінансів, шахрайство;

• **психічний тиск** може виражатися у вигляді хуліганських витівок, погрози і шантажу, енерго інформаційного впливу.

2.1.2. Напрями захисту інформації при забезпеченні інформаційної безпеки

Напрями забезпечення безпеки розглядаються як нормативно-правові категорії, що визначають **комплексні заходи захисту інформації на державному рівні, на рівні підприємства, на рівні окремої особистості**.

З урахуванням сформованої практики забезпечення інформаційної безпеки виділяють наступні **напрямки захисту інформації**:

• **правовий захист** - але спеціальні закони, інші нормативні акти, правила, процедури та заходи, що забезпечують захист інформації на правовій основі;

• **організаційний захист** - це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або послаблює нанесення будь-якого збитку виконавцям;

• **інженерно-технічний захист** - це використання різних технічних засобів, що перешкоджають нанесенню шкоди виробничої діяльності.

Крім цього, захисні дії, орієнтовані на забезпечення інформаційної безпеки, можуть бути охарактеризовані цілим рядом інших параметрів дії на об'єкти захисту (характер загроз, способи дій, охоплення і масштабність).

Так, за характером загроз захисні дії від них орієнтовані на захист інформації від розголошення, витоку і несанкціонованого доступу.

За способами дій їх можна поділити на попередження, виявлення, припинення і відновлення збитку чи інших збитків.

За охопленням захисні дії можуть бути орієнтовані на територію, будівлю, приміщення, апаратуру або окремі елементи апаратури.

Масштабність захисних заходів характеризується як об'єктовий, груповий або індивідуальний захист.

Організаційна захист - це регламентація виробничої діяльності і взаємин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне заволодіння конфіденційною інформацією і прояв внутрішніх і зовнішніх загроз.

Організаційна захист забезпечує:

• охорону, режим, роботу з кадрами, з документами;

• використання технічних засобів безпеки та інформаційно-аналітичну діяльність з виявлення внутрішніх і зовнішніх загроз виробничої діяльності.

Організаційні заходи відіграють істотну роль у створенні надійного механізму захисту інформації, тому що можливості несанкціонованого використання конфіденційних відомостей в значній мірі обумовлюються не технічними аспектами, а зловмисними діями, недбалістю і халатністю користувачів або персоналу захисту. Впливу цих аспектів практично неможливо уникнути за допомогою технічних засобів. Для цього необхідна сукупність

організаційно-правових та організаційно-технічних заходів, які виключали б (або, принаймні, зводили б до мінімуму) можливість виникнення небезпеки конфіденційної інформації.

До **основних організаційних заходів** можна віднести:

- **організацію режиму і охорони**. Її мета - виключення можливості таємного проникнення на територію і в приміщення сторонніх осіб; забезпечення зручності контролю проходу і переміщення співробітників і відвідувачів; створення окремих виробничих зон по типу конфіденційних робіт з самостійними системами доступу; контроль н дотримання тимчасового режиму праці та перебування на території персоналу фірми; організація і позичена надійного пропускного режиму і контролю співробітників і відвідувачів і ін .;
- **організацію роботи з співробітниками**, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення з співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін .;
- **організацію роботи з документами**, включаючи організацію розробки і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення;
- **організацію використання технічних засобів** збору, обробки, накопичення і зберігання конфіденційної інформації;
- **організацію робіт з аналізу внутрішніх і зовнішніх загроз** конфіденційній інформації і вироблення заходів щодо забезпечення її захисту;
- **організацію роботи з проведення систематичного контролю** за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання і знищення документів і технічних носіїв .

У кожному конкретному випадку організаційні заходи носять специфічні для даної організації форму і зміст, спрямовані на забезпечення безпеки інформації в конкретних умовах.

Захист інформації на основі організаційних заходів відіграє велику роль в забезпеченні надійності і ефективності, тому що несанкціонований доступ і витік інформації найчастіше обумовлені зловмисними діями або недбалістю користувачів або персоналу. Ці фактори практично неможливо виключити або локалізувати за допомогою апаратних і програмних засобів, криптографії та фізичних засобів захисту.

Тому сукупність організаційних, організаційно-правових та організаційно-технічних заходів, що застосовуються спільно з технічними методами, мають на меті виключити, зменшити або повністю усунути втрати при дії різних негативних факторів.

Організаційні засоби захисту комп'ютерних систем та інформаційних мереж застосовуються:

• при проектуванні, будівництві та обладнанні приміщень, вузлів мережі і інших об'єктів інформаційної системи, що виключають вплив стихійних лих, можливість недозволеного проникнення в приміщення і ін .;

• при підборі і підготовці персоналу, в цьому випадку передбачаються перевірка прийнятих на роботу, створення умов, при яких персонал був би зацікавлений в збереженні даних, навчання правилам роботи із закритою інформацією, ознайомлення з заходами відповідальності за порушення правил захисту та ін .;

• при зберіганні і використанні документів та інших носіїв (маркування, реєстрація, визначення правил видачі і повернення, ведення документації та ін.);

• при дотриманні надійного пропускного режиму до технічних засобів, до комп'ютерних та інформаційних систем при змінній роботі (виділення відповідальних за захист інформації в змінах, контроль за роботою персоналу, ведення (можливо і автоматизоване) журналів роботи, знищення в установленому порядку закритих виробничих документів);

• при внесенні змін до програмного забезпечення (суворе санкціонування, розгляд і затвердження проектів змін, перевірка їх на задоволення вимог захисту, документальне оформлення змін і ін.);

• при підготовці і контролі роботи користувачів.

Одним з найважливіших організаційних заходів є **створення спеціальних штатних служб захисту інформації** в закритих інформаційних системах у вигляді **адміністратора безпеки мережі** і **адміністратора розподілених баз і банків даних**, що містять відомості конфіденційного характеру.

Очевидно, що організаційні заходи повинні чітко плануватися, направлятися і здійснюватися якоюсь організаційною структурою, якимось спеціально створеним для цих цілей структурним підрозділом, укомплектованим відповідними фахівцями з безпеки виробничої діяльності та захисту інформації.

Найчастіше таким структурним підрозділом є **служба безпеки підприємства.**

Питання для самоконтролю

1. Які можуть бути цілі захисту інформації?
2. Що визначає концепція забезпечення безпеки інформації в організації ?
3. Що розуміється під інформацією і її безпекою?
4. Як виглядає концептуальна модель безпеки інформації?
5. Які питання відображаються в Концепції інформаційної безпеки (ІБ)?
6. Яка структура системи захисту інформації (СЗІ)?
7. Які існують вимоги до захисту інформації?
8. Які види забезпечення може мати СЗІ?
9. Приведіть види загроз інформації, які розглядаються в Моделі реалізації загроз ІБ?
10. Які основні компоненти можуть бути у моделі інформаційної безпеки?
11. Що відноситься до конфіденційної інформації і в чому полягає несанкціонований доступ до неї?

12. Які умови сприяють неправомірному оволодінню конфіденційною інформацією?

13. Які виділяють основні напрямки захисту інформації з практики забезпечення інформаційної безпеки?

14. Що таке організаційна захист інформації?

2.2. Методологічні підходи до дослідження систем управління

У сучасному менеджменті розглядається безліч самих різних організацій, які являють собою «сукупність» людей, груп, об'єднаних для досягнення якої-небудь мети, розв'язку якого-небудь завдання на основі принципів поділу праці й розподілу обов'язків.

Різноманітність завдань має велике значення при розгляді організації як об'єкта управління. Безліч цілей і завдань, що коштують перед організаціями різного класу складності й різної галузевої приналежності приводить до того, що для керування ними потрібні спеціальні знання й мистецтво, методи й приймання, що забезпечують ефективну спільну діяльність працівників усіх структурних підрозділів.

Кожна організація має конкретну систему управління, яка також є об'єктом дослідження.

Система управління будь-якої організації є складною системою, створеної для збору, аналізу й переробки інформації з метою одержання

максимального кінцевого результату при певних обмеженнях (наявності ресурсів, наприклад).

Дослідження системи управління необхідні як з наукової, так і із практичної точок зору.

З наукового погляду дослідження припускає розробку й чітке формулювання методології проведення досліджень, для того, щоб розробити фундаментальні теоретичні положення.

Із практичної точки зору дослідження повинні вміти проводити конкретні люди (аналітики, проектувальники, співробітники у відділах), отже, їхнім необхідно озброїти конкретними знаннями, навчити різним методам проведення досліджень, роз'яснити, для чого це потрібно і які цілі при цьому досягаються.

Дослідження необхідно проводити не тільки, *коли організаціям загрожує банкрутство або серйозна криза*, але й тоді, *коли організації функціонують успішно й стабільно* досягають певних результатів.

Необхідність проведення досліджень *продиктована ще й постійно мінливими цілями функціонування організацій*, що неминуче в умовах ринкової конкуренції й постійно мінливого попиту споживачів.

Необхідно усвідомити головне: дослідження проводяться з метою побудови певної (еталонної) моделі системи управління, до якої повинна прагнути будь-яка організація.

2.2.1. Система управління організації як об'єкт дослідження

Система управління як об'єкт дослідження має наступні **ознаки**, по яких можна судити *про ступінь організованості систем*. До таких вимог ставляться:

1) детермінованість елементів системи; проявляється ***в організації взаємодії підрозділів,*** при якій діяльність одного елемента позначається на інших елементах системи.

2) динамічність системи: тобто здатність під впливом зовнішніх і внутрішніх збурювань *залишатися якийсь час у певному незміненому якісному стані*.

3) наявність у системі керуючого параметра- це такий її параметр (елемент), за допомогою якого *можна управляти діяльністю всієї системи і її окремими елементами.*

4) **наявність у системі контролюючого параметра**; тобто такого елемента, який *постійно контролював би стан суб'єкта управління***,** не виявляючи при цьому на нього (або на будь-який елемент системи) керуючого впливу.

5) наявність у системі каналів (принаймні, одного) зворотнього зв'язка. Наявність прямих і зворотних зв'язків (п'ята вимога) у системі забезпечується чіткою регламентацією діяльності апарата управління по прийманню й передачі інформації при підготовці управлінських рішень.

Процес дослідження здійснюється в рамках управляємої системи і управляємих **підсистем**, отже, стосується всіх аспектів діяльності організації. Метод, який використовується для діагностики внутрішніх проблем, називають ***управлінським обстеженням***.

Даний метод заснований на комплексному дослідженні різних функціональних зон організації, основні з яких:

• виробництво;

• фінанси

• персонал;

• імідж організації.

Аналізуються також **фактори**:

- економічні;
- політичні;
- ринкові;
- соціальні;
- конкуренції;
- міжнародні й ін.

Таким чином, **дослідження** як складова частина менеджменту організації — це сукупність методів організаційного й техніко-економічного дослідження всіх зазначених факторів і системних характеристик конкретної організації.

Пошук шляхів і методів удосконалювання системних характеристик організації є **основною метою досліджень** як складеної частини менеджменту.

До таких характеристик з позиції загального менеджменту ставляться:

- мети системи керування;
- функції керування;
- управлінські розв'язки;
- структура керування.

В основу ***дослідження як складеної частини менеджменту організації*** **покладені наступні методологічні підходи (**рис.2.5)

• **Системний підхід, *що*** означає дослідження конкретного об'єкта як системи.

• **Комплексний підхід** припускає враховувати при аналізі як внутрішнє так і зовнішнє середовище організації.

• **Інтеграційний підхід,** коли дослідження здійснюються як по вертикалі (між окремими елементами системи керування), так і по горизонталі (на всіх стадіях життєвого циклу продукту).

• **Ситуаційний підхід,** коли мотивом до проведення аналізу є конкретні ситуації, широкий діапазон яких суттєво впливає на ефективність управління.

• **Інноваційний підхід,** заснований на вмінні організації швидко реагувати на зміни, які диктуванні зовнішнім середовищем.

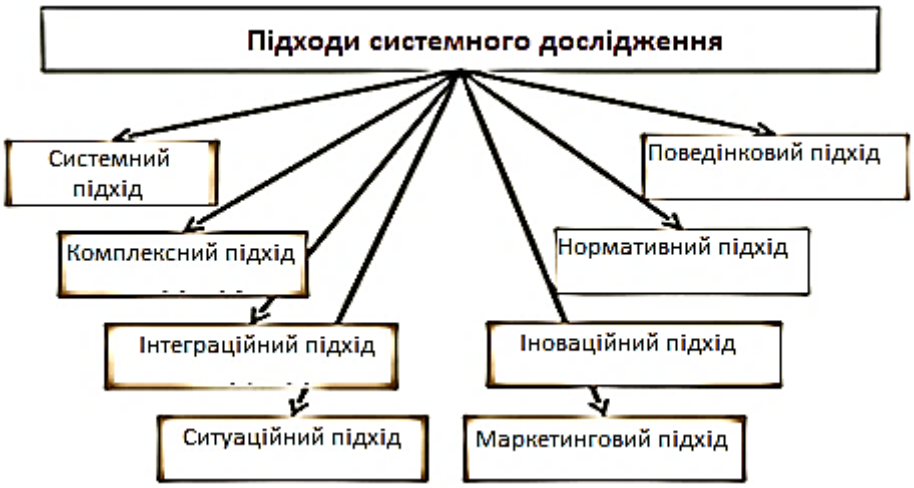


Рис.2.5. Методологічні підходи дослідження систем управління

• **Маркетинговий підхід** припускає орієнтацію управляємої системи **на споживача.**

• **Нормативний підхід** пов'язаний з обліком **сукупності найважливіших нормативів,** якими керується у своїй діяльності апарат управління організації.

• **Процесний підхід**– підхід до дослідження систем управління як до безперервного виконання сукупності взаємозалежних між собою робіт і загальних функцій **управління**.

• **Функціональний підхід**, який означає **дослідження функцій управління**, що забезпечують прийняття управлінських рішень заданого рівня якості при мінімальних витратах на **управління** або виробництво.

• **Загальнодержавний підхід** в **оцінці результатів управлінської діяльності й витрат на зміст апарата управління.**

• **Творчий колективний підхід** для **пошуку найбільш економічного й ефективного варіанта вдосконалювання системи управління.**

• **Підхід відповідності інформаційної й організаційної структур** (у теорії прийняття рішень і ефективних комунікацій).

• **Емпіричний підхід** – підхід, при якому об'єкт **досліджується на основі вже наявного досвіду**.

У результаті проведення досліджень повинні бути сформульовані **конкретні пропозиції з удосконалення системи управління організацією.**

Система управління - це система організації і підтримки рішень, спрямованих на ріст організованості самої системи. Вона включає: суб'єкт, об'єкт управління, зв'язки між ними и вплив середовища на її функціонування (рис.2.6). Саме процеси прийняття рішень визначають зміст процесу управління в цих системах і конкретний спосіб реалізації системної функції управління зміною організованості.

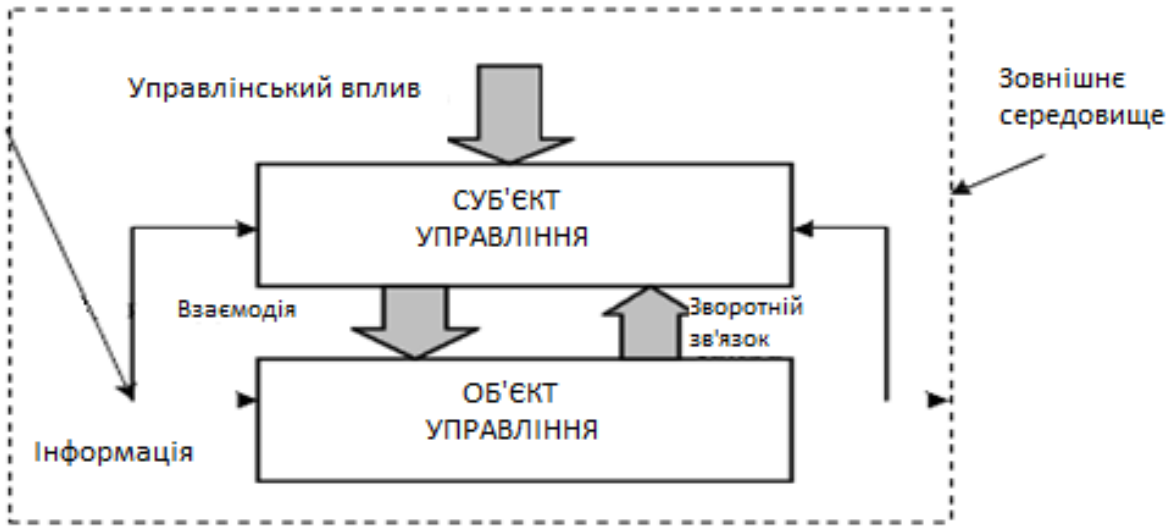


Рис.2.6. Схема системи управління

У системі управління соціально-економічними системами виділяють чотири основні складові:

- механізм управління (мета, функції, принципи, методи)**;**

- структура систем управління (управляюча система в статиці; управляєма, яка характеризує її побудову, розташування і співвідношення органів і ланок управління, які входять до неї);

- процеси управління (управляюча система в динаміці**);**

- удосконалення управління (поліпшення, оптимізація, модернізація, раціоналізація і інші зміни з урахуванням конкретних умов функціонування).

Дослідження систем управління— це вид діяльності, спрямований на розвиток і вдосконалення **управління відповідно до постійно мінливих зовнішніх і внутрішніх умов**. В умовах динамічності сучасного виробництва і суспільного устрою **управління повинне перебувати в стані безперервного розвитку**, який сьогодні **неможливо забезпечити без дослідження шляхів і можливостей цього розвитку, без вибору альтернативних напрямків**. Дослідження **управління** здійснюється **в щоденній діяльності менеджерів і персоналу і у роботі спеціалізованих аналітичних груп,** лабораторій, відділів. Іноді для проведення дослідження запрошують **консультаційні фірми.** Необхідність у дослідженнях систем **управління** продиктована досить **великим**

колом проблем. Декомпозиційне відображення елементів системи управління представлено на рис.2.7.

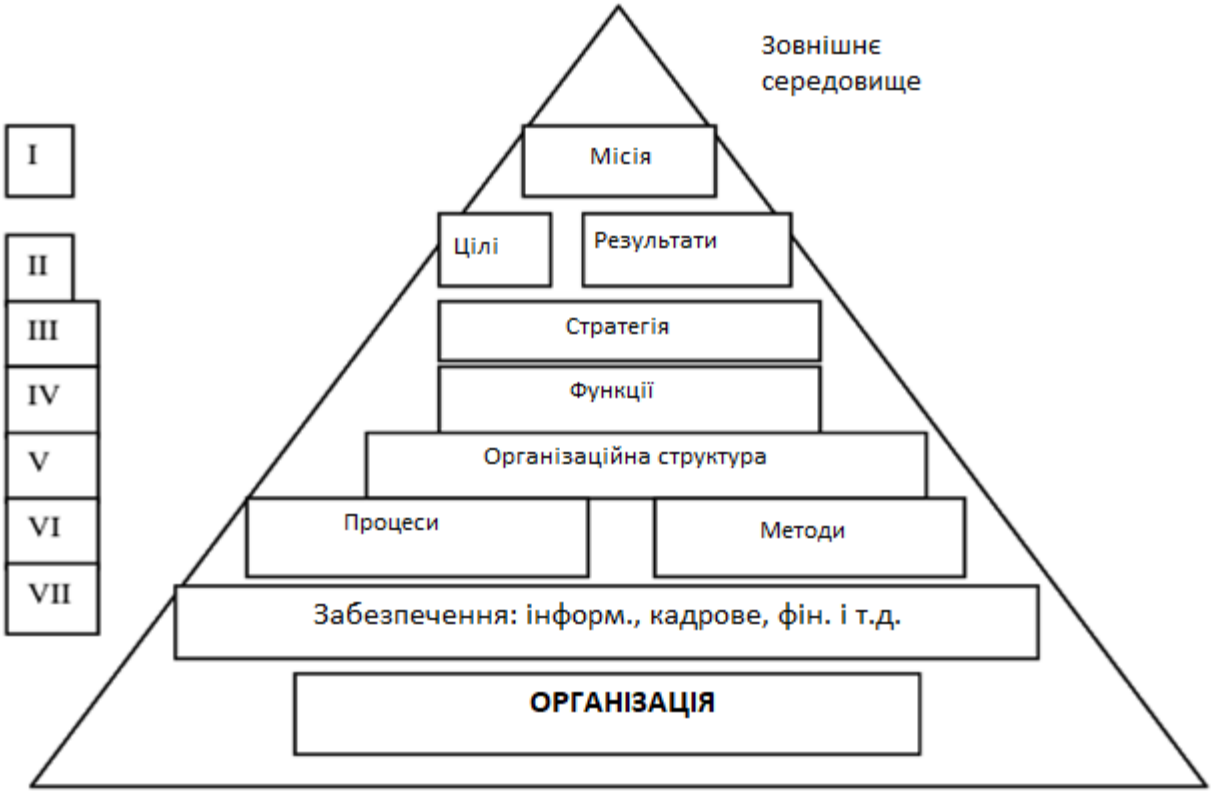


Рис.2.7. Декомпозиційне відображення елементів системи управління

Порівнюючи при декомпозиції фактичний стан елементів і компонентів системи управління із критеріями або характеристиками їх нормального, (нормативного) стану і використовуючи критерії ефективності і методи оцінювання можна визначити відхилення і вплив на ефективність функціонування СУ в цілому. Це дозволяє ситуаційно формулювати як мінімум одну із двох задач її дослідження – **удосконалювання (розвиток) або реструктуризацію (реорганізацію).**

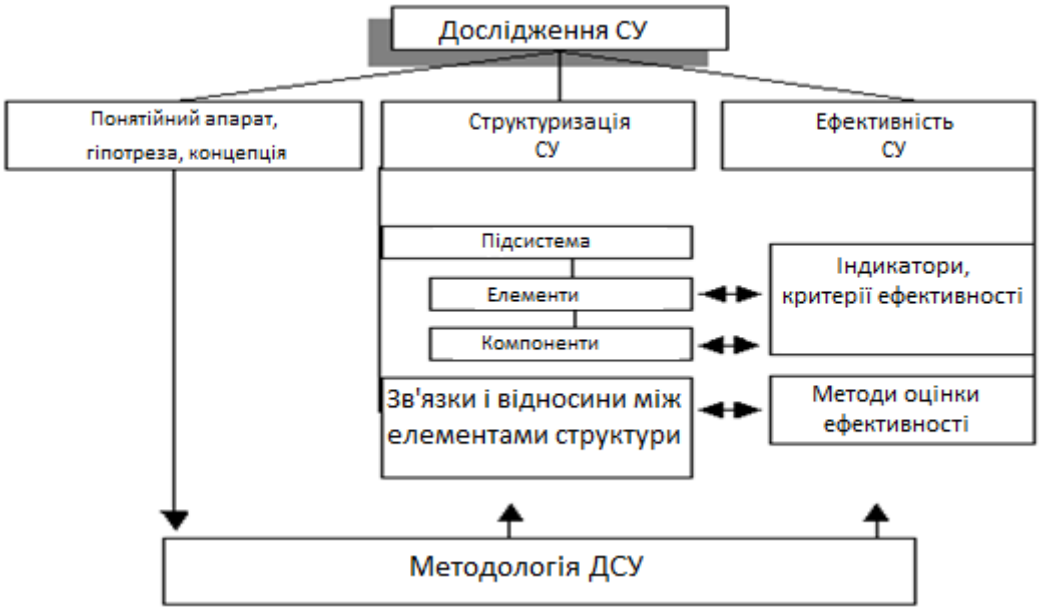


Рис.2.8. Методологічні особливості дослідження систем управління (ДСУ)

Дослідження систем управління (рис. 2.8) **можуть бути різними як по цілям, так і по методології їх проведення.**

По цілям* досліджень** можна виділити ***теоретичні, ***практичні*** й ***науково-практичні*** (рис.2.9). *Практичні дослідження* призначені для швидких ефективних рішень і досягнення бажаних результатів. *Науково-практичні дослідження* орієнтовані на перспективу, більш глибоке розуміння тенденцій і закономірностей розвитку організацій, підвищення освітнього рівня працівників.

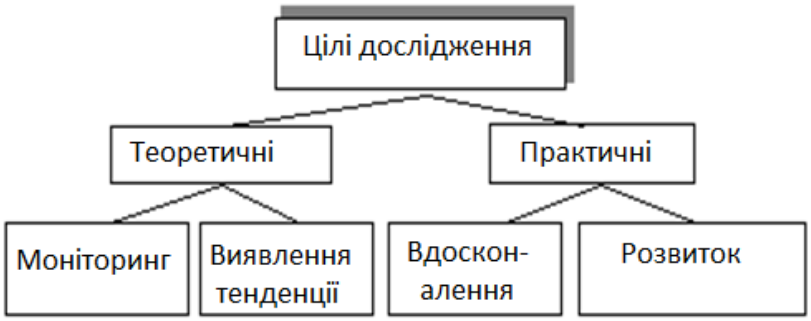


Рис.2.9. Структуризація теоретичних і практичних цілей дослідження

По методології проведення слід виділити, насамперед, дослідження ***емпіричного характеру, які опираються на систему наукових знань*** (рис.2.10).

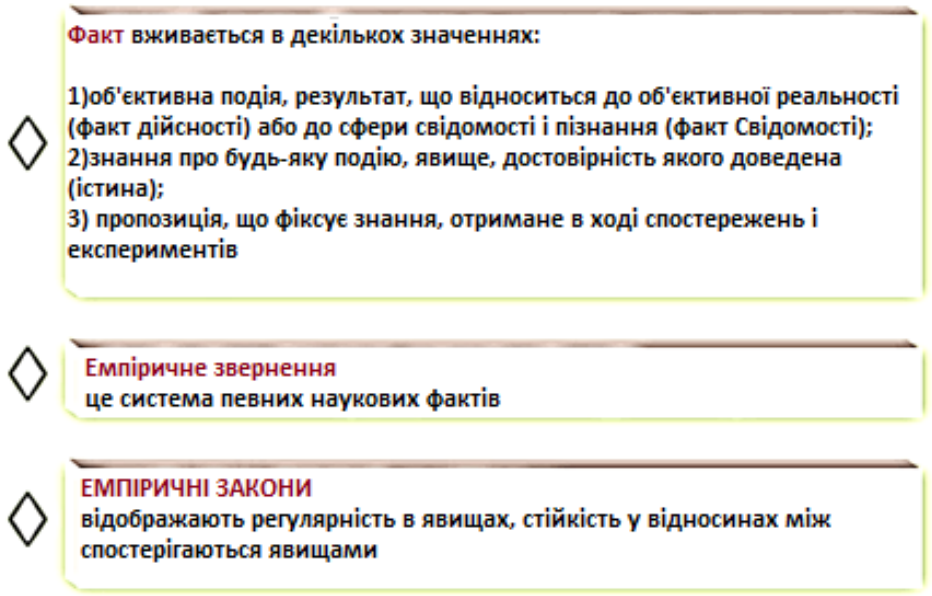


Рис.2.10. Структура емпіричного рівня дослідження.

Різноманітні дослідження ***<u>по використанню ресурсів власних або приваблюваних</u>***: по трудомісткості, тривалості, інформаційному забезпеченню, організації їх проведення.

Спочатку необхідно виявити й проаналізувати проблеми. Під ***<u>проблемою</u>*** *розуміється невідповідність фактичного стану управляємого об'єкту (наприклад, виробництва продукції) бажаному або заданому (запланованому). Факт вживається в декількох значеннях:*

1)об'єктивна подія, результат, що відноситься до об'єктивної реальності(факт дійсності) або до сфери свідомості і пізнання (факт Свідомості);

2)знання про будь-яку подію, явище, достовірність якого доведена (істина);

3)пропозиція, що фіксує знання, отримане в ході спостережень і експериментів

Сукупність факторів і умов**, що* **викликають появу тієї або іншої проблеми, називається *ситуацією, а розгляд проблеми з обліком ситуаційних факторів, що впливають на ***неї, дозволяє описати проблемну ситуацію.***

Аналіз ситуаційних факторів дозволяє *розглянути проблему* у зв'язку з подіями, які її викликали, і із змінами у внутрішньому й зовнішньому середовищі та почати пошук рішень.

Таким чином, *визначити проблему — значить установити границі системи, у межах якої вона розглядається, рівень, на якому вона повинна вирішуватися.*

Дослідження як вид діяльності в процесі управління організацією у вирішенні проблем включає наступні роботи:

- розпізнання проблем і проблемних ситуацій;
- визначення причин їх походження, властивостей, змісту, закономірностей проведення й розвитку;
- установлення місця цих проблем і ситуацій (як у системі наукових знань, так і в системі практичного керування);
- знаходження шляхів, засобів і можливостей використання нових знань про дану проблему;
- розробка варіантів вирішення проблем;
- вибір оптимального варіанта розв'язку проблеми за критеріями результативності, оптимальності і ефективності.

У реальній практиці всі ці роботи перебувають у тісному взаємозв'язку, характеризуючи при цьому ступінь професіоналізму дослідників, конкретні цілі й завдання їх діяльності.

Головне в дослідженнях: вони проводяться **з метою побудови певної (еталонної) моделі системи управління, до якої повинна прагнути завжди будь-яка організація.**

Дослідження систем управління включає:

- ***уточнення мети розвитку й функціонування*** підприємства і його підрозділів;

• ***виявлення тенденцій розвитку підприємства*** в конкретному ринковому середовищі;

• ***виявлення факторів***, що ***забезпечують досягнення сформульованої мети й перешкоджаючих їй***;

• ***збір необхідних даних для розробки заходів щодо вдосконалення*** діючої системи **управління**;

• ***одержання необхідних даних для прив'язки сучасних моделей, методів і засобів до умов*** конкретного підприємства.

Таким чином:

1. Для успішної роботи організацій у сучасних умовах необхідно періодично проводити дослідження з метою вдосконалення діючих систем управління.

2. Проведення досліджень здійснюється відповідно до обраної мети й у певній послідовності.

2.2.2. Методологічні положення дослідження систем управління

Методологія - це логічна організація діяльності людину, що полягає у визначенні мети і предмета дослідження, підходів і орієнтирів у його поведінці, виборі засобів і методів, що визначають одержання оптимального результату. У табл.2.1 представлений зміст методології дослідження.

Таблиця 2.1

Основні складові методології дослідження

Складова	Характеристика
Об'єкт	У загальному випадку це явище, процес, система, на які спрямоване дослідження. Об'єкт визначає межі дослідження.
Предмет	Конкретні властивості, відносини, сторони об'єкта дослідження.Предметом дослідження є певна проблема.
Ціль	Якийсь бажаний результат, який досягається в процесі дослідження. Метою дослідження може бути вивчення певного об'єкта для подальшого вироблення заходів по вирішенню виявленої проблемної ситуації
Підхід	Комплекс вихідних установок, що обумовлюють парадигму, стратегію, тактику і інструментарій дослідження.
Методи	Сукупність способів аналізу, рішення дослідницької проблеми
Принципи	Основні правила, відповідно до яких проводиться дослідження.
Гіпотеза	Обгрунтоване припущення, що висувається з метою з'ясування характеристик досліджуваних породжує проблему.

Методологія будь-якого дослідження починається з вибору, постановки й формулювання його мети. **Ціль** - основа розпізнавання й вибору проблем у дослідженні.

Мети дослідження можуть бути поточними й перспективними, загальними й локальними, постійними й епізодичними.

Головну роль у методології відіграють **засоби і методи дослідження**,

Методологія дослідження повинна включати також **визначення й формулювання орієнтирів і обмежень**, які дозволяють проводити дослідження більш послідовне й цілеспрямовано.

У ході дослідження звичайно **керуються виробленою концепцією. Концепція** - це комплекс положень, зв'язаних загальної вихідною ідеєю, що визначають діяльність людину й спрямованих на досягнення поставленої мети.

Методологічна схема дослідження - це комплекс, комбінація, пріоритети, послідовність основних елементів методології: концепція, гіпотеза, проблема, аналіз, підхід, методи, проект, рекомендації, **модель,** мета, розв'язок, рецепт.

Центральне місце в методології дослідження займають виявлення й точне визначення **проблеми**. **Методи дослідження** - це сукупність прийомів обробки інформації, що дозволяють досягти його цілей. В окрему групу при

класифікації методів дослідження виділяють ***евристичні або творчі методи*** дослідження.

Методологія дослідження систем управління ґрунтується на розумній організації діяльності керівників і менеджерів підприємства по раціоналізації системи управління (2.11).

Вона припускає визначення:

- цілей, предмета досліджень.
- границь дослідження,
- вибір засобів і методів досліджень,
- засобів (ресурсів) і етапів проведення дослідницьких робіт.

Рис.2.11. Взаємозв'язок понять методологія, метод і методика

Характеристики дослідження систем управління:

1. ***Потреба в дослідженні*** *визначає* ***масштаб і глибину дослідження*** *системних характеристик, реалізація яких найбільшою мірою впливає на досягнення поставлених цілей.*

*2.****Об'єктом досліджень*** *є* ***система управління конкретної організації.*** *Для її вивчення необхідно знати затверджені* ***схеми управління, посадові інструкції….*** *Організація може бути описана рядом параметрів:*

- *мети організації, організаційна структура,*
- *зовнішнє й внутрішнє середовище, блок використовуваних ресурсів,*
- *нормативна й правова основа,*
- *специфіка процесу функціонування,*
- *система соціально-економічних відносин.*

Предметом дослідження є **взаємини між співробітниками** апарата управління, а також **між підрозділами**, розташованими на різних рівнях системи управління. При цьому предметом дослідження є **конкретна проблема (або комплекс проблем**).

Серед цих проблем можуть бути наступні*:* ***розвиток структури управління; мотивація персоналу; мотивація техніки й інформаційних систем управління; розробка управлінських рішень; підготовка персоналу*** й ін.

Вибір основної проблеми організації, що стримує її розвиток, її всебічне дослідження й аналіз — це інтуїція і майстерність, професіоналізм менеджера і керівника організації.

3. ***Ресурси***— це **комплекс засобів**, що забезпечують успішне проведення досліджень. Це, насамперед, *матеріальні ресурси, трудові ресурси, фінансові ресурси, інформаційні ресурси, технічні засоби*, необхідні для обробки результатів, а також *правові документи*, що характеризують об'єкт дослідження.

4. ***Ефективність досліджень*** вимагає **порівняння витрат на проведення досліджень і отриманих результатів.**

5. ***Результати досліджень*** можуть бути представлені в різних формах. Це може бути *нова модель системи управління*, нові регламентуючі *документи, скоректовані розрахункові формули*.

У загальному **вигляді організація проведення дослідження** включає **етапи:**

- підготовка дослідження, тобто розробка програми, визначення одиниць спостереження, визначення методів збору інформації, проведення пробного (пілотажного) дослідження:

- **збори необхідної інформації** з обліком її синтаксичних, семантичних і прагматичних аспектів;

- **підготовка інформації до обробки**;

- **обробка інформації і її аналіз**;

- **підготовка результатів дослідження**.

Іноді процеси дослідження конкретного об'єкту проводиться відповідно до обраної (рекомендованої) моделі системи управління, що часто називається **еталоном**. Етапи проведення дослідження відповідно до еталонної моделі представлені на рис.2.12.

При дослідженні системи управління на практиці висуваються завдання:

- досягнення оптимального співвідношення між управляючою й управляємою підсистемами (сюди входять показники норм управління, показники ефективності роботи апарата управління, скорочення витрат на керування);
- підвищення продуктивності праці управлінських працівників і робочих виробничих підрозділів;
- поліпшення використання матеріальних, трудових, фінансових ресурсів у управляючої й управляємої підсистемах;
- зниження витрат на продукцію або послуги й підвищення їх якості.

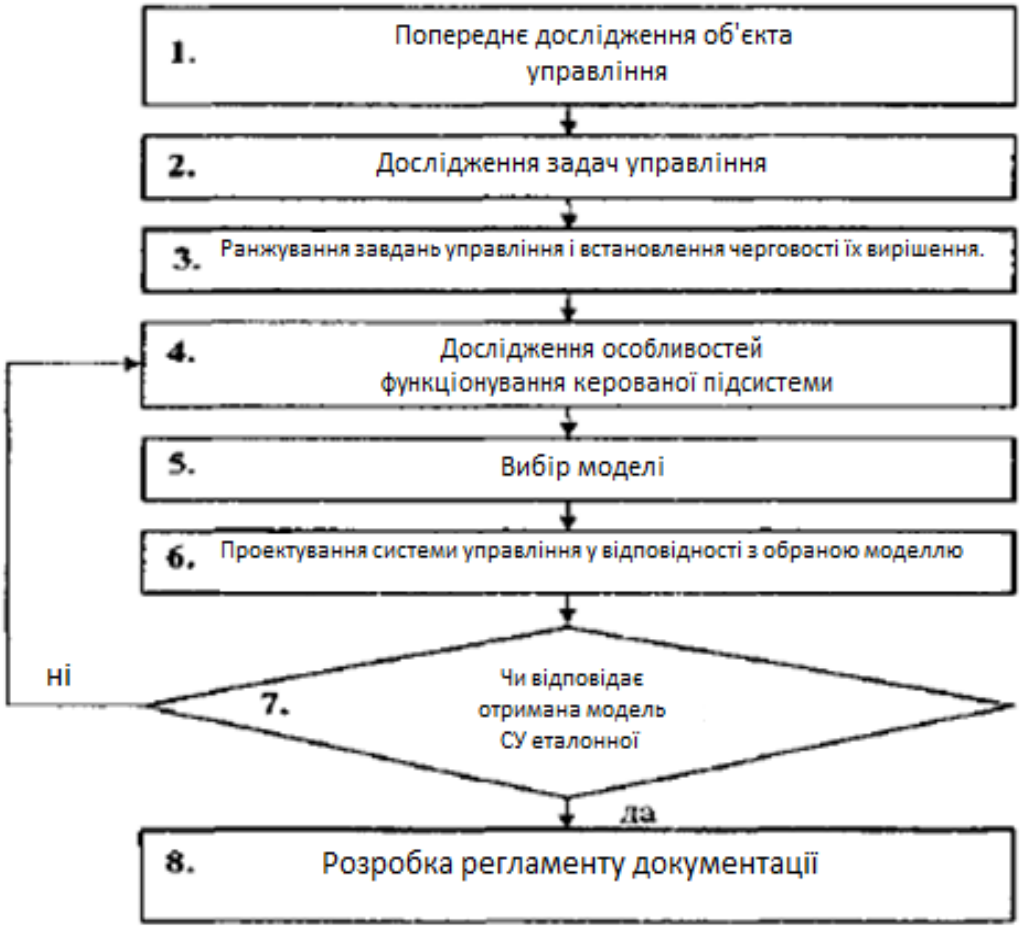


Рис.2.12. Дослідження об'єкта управління відповідно до еталонної моделі

При дослідженні системи управління на практиці висуваються завдання:

- досягнення **оптимального співвідношення між управляючою й управляємою підсистемами** (сюди входять показники норм керованості, показники ефективності роботи апарата управління, скорочення витрат на управління);
- **підвищення продуктивності праці управлінських працівників** і робочих виробничих підрозділів;
- **поліпшення використання матеріальних**, трудових, фінансових **ресурсів у управляючої й управляємої підсистемах;**
- **зниження витрат на продукцію або послуги й підвищення їх якості.**

Цільова ієрархія завдань при вирішенні проблем і проблемних ситуацій:

- ***розпізнання проблем і проблемних ситуацій;***
- ***визначення причин їх походження****, властивостей, змісту, закономірностей поведінки й розвитку, каналів і напрямків впливу;*
- ***установлення місця цих проблем і ситуацій*** *(як у системі наукових знань, так і в системі практичного управління);*
- ***знаходження*** *шляхів, засобів і можливостей використання* ***нових знань про дану проблему;***
- ***розробка варіантів вирішення проблем****;*
- ***вибір оптимальних варіантів вирішення нових проблем за критеріями*** *результативності, оптимальності, ефективності (вартості).*

Результатами дослідження можуть бути ***окремі рекомендації, нова модель системи управління, поліпшені норми керованості, більш досконалі методики, що сприяють оперативному й успішному дозволу проблеми***. Додатково необхідно **підрахувати ефективність досліджень**, тобто розмітити витрати на проведення досліджень і отримані результати.

Результати аналізу подають на розгляд керівництву підприємства або спеціальної експертної комісії.

Питання для самоконтролю

1. Що розуміється під дослідженням систем управління? Які види досліджень ви знаєте?
2. Охарактеризуйте послідовність етапів проведення досліджень.
3. Чому дослідження систем управління — складова частина менеджменту організації?
4. Перелічите вимоги, пропоновані до системи управління як об'єкту дослідження.
5. У чому сутність методології дослідження систем управління?

6. У чому сутність загальної концепції дослідження систем управління?

7. Яке значення для проведення досліджень мають такі характеристики процесу управління, як мета організації, функції управління, управлінські рішення, організаційна структура?

2.3. Застосування процесного підходу до створення СУІБ організації

Процесний підхід – це одна з концепцій управління, яка остаточно сформувалася у 80-х роках минулого століття. Відповідно до цієї концепції вся діяльність організації сприймається як набір процесів.

Для того, щоб керувати, необхідно управляти процесами.

Головне поняття, яке використовує процесний підхід - це поняття процесу. Процес (від лат. Processes - просування).

Існують різні визначення, але найбільш часто використовується визначення стандарту ISO 9001.

Процес - це сукупність взаємопов'язаних або взаємодіючих видів діяльності, яка перетворює входи на виходи. Процес для цієї діяльності вимагає певних ресурсів і керуючих впливів (управління).

Важливою складовою процесу, яка відображена у цьому визначенні, є систематичність дій. Події процесу мають бути повторюваними, а чи не випадковими.

Процесний підхід змінює поняття структури організації. Основним елементом стає процес. Відповідно до одного з принципів процесного підходу організація складається не з підрозділів, а з процесів.

2.3.1. Процесний підхід до управління організацією

Входами до процесу зазвичай є виходи інших процесів. На рис. 2.13 представлена узагальнена ілюстрація даного визначення.

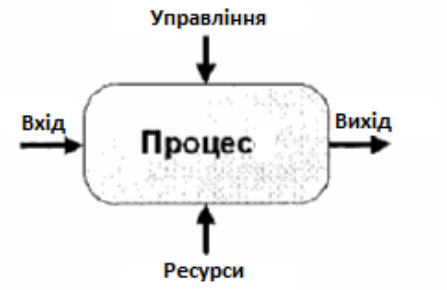


Рис.2.13. Узагальнена ілюстрація поняття «процес»

Входами можуть бути специфічні вимоги, включаючи ресурси - **підмножини активів організації**, які використовуються або споживаються в процесі виконання певної діяльності. **На виході** виходять в тій чи іншій мірі задоволені вимоги і сам безпосередній результат процесу.

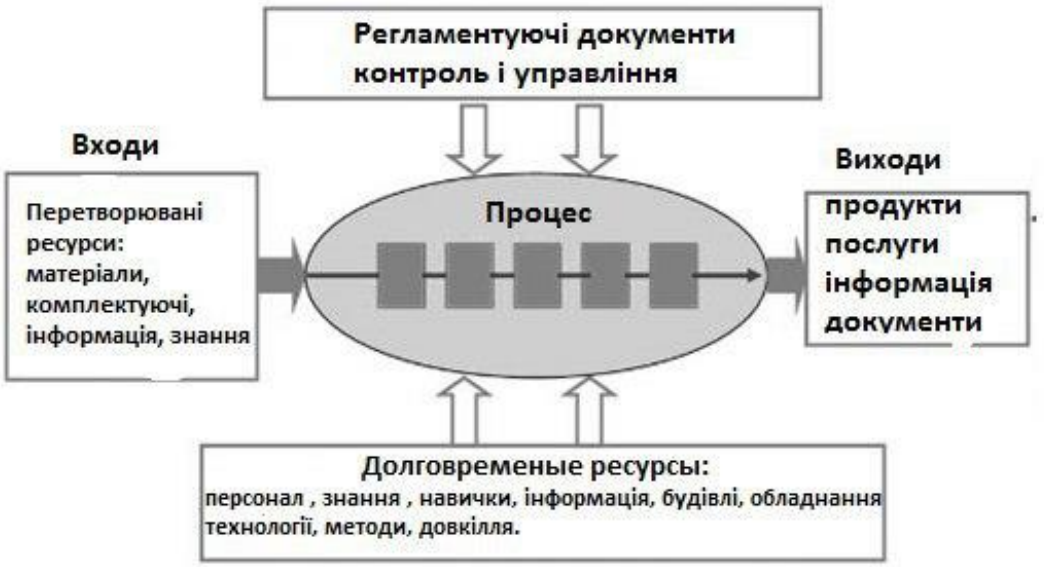


Рис.2.14. Ілюстрація поняття «процес»

Ключові елементи процесного підходу

Процесний підхід передбачає наявність ключових елементів, без яких він не може бути впроваджений в організацію.

До таких **ключових елементів** (рис.2.15) ставляться: **хід процесу; вихід процесу; ресурси; власник процесу; споживачі і постачальники процесу; показники процесу.**

Входами процесу є елементи, що зазнають зміни в ході виконання дій. Під входами у процесному підході розглядають матеріали, обладнання, документацію, різну інформацію, персонал, фінанси та ін.

Виходами процесу є очікувані результати, заради яких вдаються до дій. Виходом може бути як матеріальний продукт, так і різного роду послуги або інформація.

Ресурсами є елементи, необхідні для процесу. На відміну від входів, ресурси не змінюються в процесі. Такими ресурсами процесний підхід визначає обладнання, документацію, фінанси, персонал, інфраструктуру, середу та ін.

Власник процесу - процесний підхід вводить це поняття як одне з найголовніших. У кожного процесу повинен бути свій власник. Власником є людина, що має в своєму розпорядженні необхідну кількість ресурсів і відповідає за кінцевий результат (вихід) процесу.

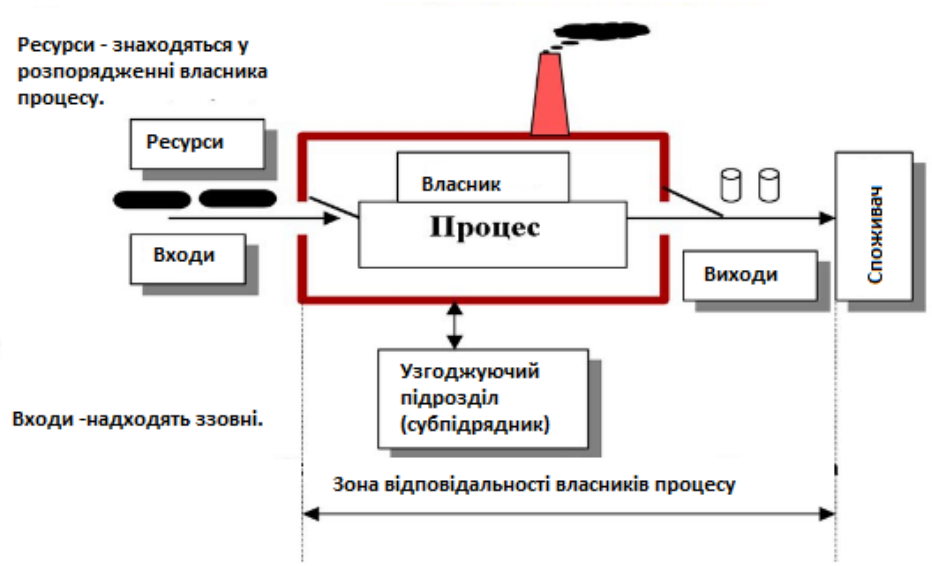


Рис.2.15. Визначення входів-виходів і ресурсів процесу

У кожного процесу повинні бути **постачальники і споживачі** (рис.2.16).

Постачальники забезпечують вхідні елементи процесу, а **споживачі** зацікавлені в отриманні вихідних елементів.

У процесі можуть бути як **зовнішні, так і внутрішні постачальники і споживачі**. Якщо у процесу немає постачальників, то процес не буде виконаний. Якщо у процесу немає споживачів, то процес не затребуваний.

Рис.2.16. Спрощена схема процесу в організації

Показники процесу (рис.2.17) необхідні для отримання інформації про його роботу і прийнятті відповідних управлінських рішень. Показники процесу це набір кількісних або якісних параметрів, що характеризують сам процес і його результат (вихід).

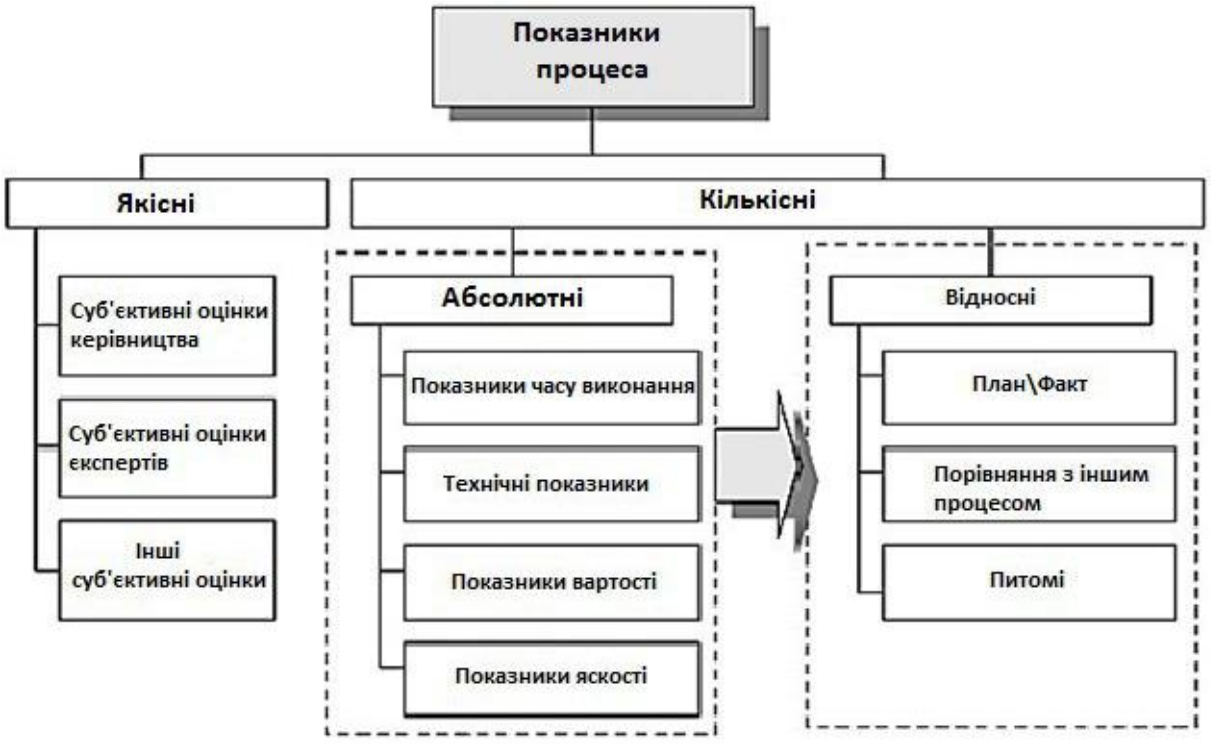


Рис.2.17. Показники процесу

Складові процесу: Технологія. Персонал. Устаткування. Оснащення та інструмент. Контрольно-вимірювальне обладнання. Документація на робочих місцях. Основні матеріали. Допоміжні матеріали. Виробниче середовище. Теплоенергоносії. Програмне забезпечення.

Спираючись на визначення процесу **всі дії всередині організації** можна розглядати або як процес (бізнес-процес), або як його частину. Найчастіше в організаціях використовується **поняття бізнес-процесу**. Використання поняття «бізнес-процес» (англ. Business process) викликано сформованими традиціями в світі.

Управління - це теж процес, що складається з серії безперервних взаємопов'язаних дій (управлінських функцій), кожне з яких саме по собі є процесом, важливим для успіху організації (підприємства, компанії). Кожна управлінська функція теж являє собою процес, тому що також складається з серії взаємопов'язаних дій. Управління підсумовує всі ці управлінські функції, склад яких вперше був запропонований Файолем: «**Управляти - це значить передбачати, організовувати, розпоряджатися, координувати і**

контролювати». Деякими прикладами управлінських процесів є процеси комунікаційні та прийняття управлінських рішень, виробничі (технологічні) процеси.

Керівництво організацією можливо здійснювати тільки за допомогою управління її процесами (бізнес-процесами).

Процесний підхід до управління, або процесне управління - це підхід до управління, який розглядає його як безперервну серію взаємозалежних управлінський функцій.

Процесне управління - планомірна діяльність по сформуванню цілеспрямованої поведінки організації за допомогою виділення, опису та менеджменту системи взаємопов'язаних і взаємодоповнюючих процесів організацій і їх ресурсного оточення.

Тому **процесне управління** -це інструмент корпоративного управління, що забезпечує реалізацію стратегії організації. Управління може бути ефективним тоді, коли воно свідомо націлене на управління процесами.

Система управління, в основу якої покладено процес, - це система, в якій основним об'єктом управління на підприємстві є бізнес-процес. Тому застосування процесного підходу вимагає опису, оптимізації та автоматизації бізнес-процесів.

При застосуванні процесного підходу структура управління організації включаються два рівня:

-управління в рамках кожного бізнес-процесу;

- управління групою бізнес-процесів на рівні всієї організації.

Основою управління окремими бізнес-процесом і групою бізнес-процесів є показники ефективності, серед яких виділяють:

- витрати на його здійснення;

- розрахунок часу на його здійснення;

- показники якості бізнес-процесу.

Процеси в організації можна розділити на кілька груп:

1. Основні (процеси життєвого циклу), що забезпечують запланований результат діяльності організації. Призначення процесу – створення основних продуктів діяльності організації; результатом є основний продукт і / або напівфабрикат для його виготовлення та виконання проміжних процесів. Ресурси і сервіси в основному призначені для основних процесів.

2. Допоміжні, які призначені для забезпечення нормального функціонування основних та інших процесів необхідними ресурсами; вони забезпечують роботу основних процесів (сервісне обслуговування обладнання, забезпечення енергоресурсами і виробничим середовищем, забезпечення роботи офісу, інформаційне забезпечення, управління навколишнім середовищем і т.д.). Забезпечення інформаційної безпеки (ЗІБ) відноситься до допоміжної основної діяльності в управлінських процесах.

Основні види процесів в організації:

1. **Процеси управління (менеджменту)**, що відносяться до стратегічного планування, постановки цілей і встановлення політик, забезпечення комунікацій і т. п. Призначення процесів - управління діяльністю організації; в результаті це і є сама діяльність всією організацією. За своєю природою всі управлінські завдання є інформаційними.

2. **Процеси вимірювання, аналізу та вдосконалення**. Призначення процесів - вхідні дані використовуються для процесів удосконалення всієї діяльності організації.

Ефективність процесу визначається досягнутими результатами в порівнянні з використаними ресурсами і може оцінюватися за допомогою внутрішніх і зовнішніх процесів контролю (перевірки).

2.3.2. Використання вимог зі стандартизації до систем і процесів управління інформаційною безпекою

На початку XX століття стала розвиватися наука **УПРАВЛІННЯ**, її назвали менеджментом, це означає «управляти», «керувати». Менеджмент включає основні функції управління (прогнозування, цілепокладання,

планування, організація діяльності, мотивування персоналу, лідерство, контроль, облік і аналіз, коригування діяльності і т. д.) І визначає ефективне досягнення цілей організації (підприємства, компанії) при оптимальному використанні ресурсів . Таким чином, ***менеджмент є найбільш ефективним способом управління.*** Часто слова «менеджмент» і «управління» використовуються як синоніми.

Для структурування всіх процесів управління і для забезпечення обліку всіх значимих елементів процесного підходу застосовується циклічна модель або цикл **PDCA (від англ. Plan-Do-Check-Act - плануй - виконуй - перевіряй - дій ») (**рис. 2.18) , запропонована і розвинена двома американськими вченими і фахівцями в теорії управління якістю. Шухарт (Waller A. Shewhart) вперше описав цикл PDCA в 1939 році у своїй книзі «Статистичні методи з точки зору управління якістю». Демінг (William Edwards Deming) пропагував використання циклу PDCA в якості основного способу досягнення безперервного поліпшення. Ця формула більше відома як «цикл Демінга». Він також **ввів модифікацію циклу PDCA - цикл PDSA (від англ. Study - вивчай).** Загальна блок-схема алгоритму процесу відповідно до циклу PDCA показана на рис. 2.19.

Рис.2.18. Циклічна модель або цикл PDCA

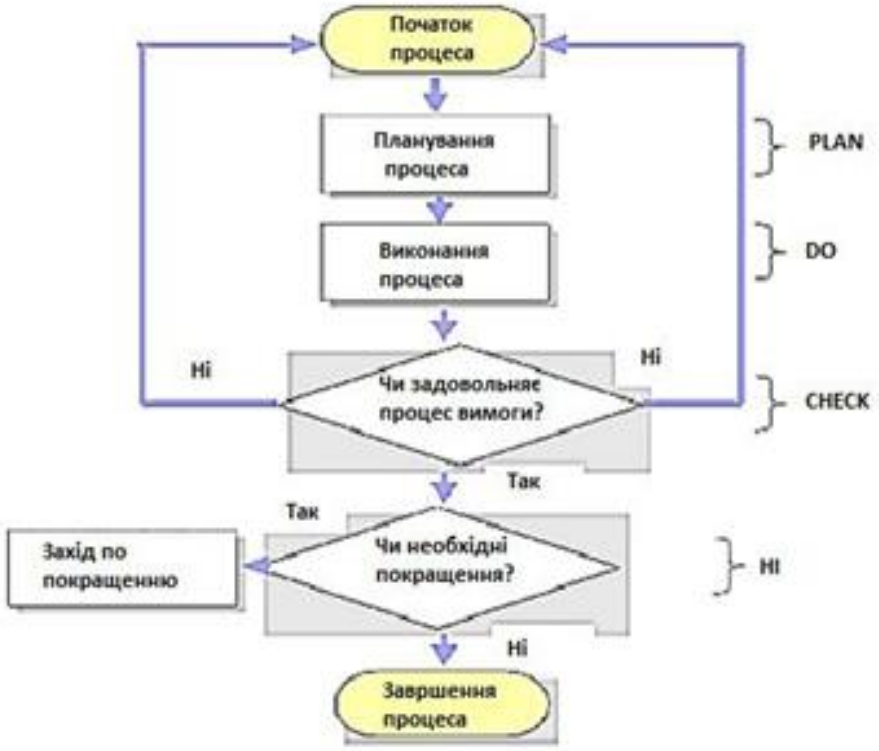


Рис.2.19. Загальна блок-схема алгоритму процесу відповідно до циклу PDCA

1. «Плануй» (Plan) - визначення цілей і завдань, а також способів досягнення цілей. На даному етапі забезпечується єдине напрямок діяльності організації до досягнення її цілей за рахунок визначення процесів, необхідних для отримання результатів відповідно до існуючих вимог в позначений відрізок часу. Для цього визначаються і описуються поточний і бажаний стан процесів за рахунок виявлених невідповідностей та причин їх виникнення. Планування не є окремою разовую подією, якщо організація прагне функціонувати як можна довше. Тому вона переглядає свої цілі, якщо повне досягнення початкових планів практично завершено або їх виконання неможливо в силу ряду причин. Друга причина, по якій планування повинне здійснюватися безперервно, - це постійна невизначеність майбутнього.

Зміни в навколишньому середовищі, помилки в судженнях і інші фактори призводять до того, що події реалізуються не так, як це передбачало керівництво при виробленні перших начальних планів. Тому щоб плани узгоджувалися з реальністю, їх необхідно регулярно переглядати. В процесі планування

необхідно консультуватися з власниками процесів, які мають найповніші знання про них.

2. «Здійснюй» (Do) - реалізація процесу: навчання та підготовка кадрів, виконання робіт. На даному етапі в першу чергу проводиться створення певної структури, яка повинна виконувати плани і тим самим досягати мети організації.

Відбувається впровадження процесів, в якому здійснюється виконання запланованих заходів. Тут слід пам'ятати про те, що стандарти завжди недосконалі, тому необхідно покладатися на досвід і знання кваліфікованих працівників. На всіх етапах проходження циклу Демінга виникає проблема нестачі кваліфікованих і підготовлених працівників. Тому необхідно впроваджувати програми навчання і займатися цілеспрямованою підготовкою кадрів.

3. «Перевіряй» (Check) - перевірка результатів виконання робіт, проведених на попередньому етапі. Даний етап говорить про те, що необхідно проводити моніторинг процесів і вимірювати їх по відношенню до політиків, цілям і вимогам до продукції за певний період і повідомляти про отримані результати в порівнянні з прогнозованими (очікуваними).

4 . «Дій, або впливай» (Act) - здійснення відповідних дій, які спрямовані на постійне удосконалення (поліпшення) показників процесів. На даному етапі на основі результатів, отриманих раніше, вдаються до дій по корекції відхилень від початкових планів і постійного поліпшення функціонування процесів.

2.3.3. Впровадження системи управління інформаційною безпекою

У світі активно ведеться робота в напрямку стандартизації СУІБ і окремих процесів управління ІБ. У відповідність з цими стандартами ЗІБ в будь-якій організації полягає у виконанні наступних дій:

- визначення цілей ЗІБ;
- створення ефективної СУІБ;

- розрахунок сукупності деталізованих не тільки якісних, а й кількісних показників для оцінки відповідності рівня ІБ заявленим цілям;

- застосування інструментарію ЗІБ і оцінки її поточного стану;

- використання методик (з на задній системою критеріїв і захисних заходів, або заходів ЗІБ) в процесі аналізу та управління ризиками, які дозволяють об'єктивно оцінити поточний стан справ в організації.

Основоположником подібної стандартизації стала серія стандартів ISO 9000, що пред'являють вимоги до систем менеджменту якості, дотримання яких дозволяє контролювати якість виробленої продукції або послуг, що надаються. При розробці стандартів на СУІБ багато було взято за основу саме зі стандартів серії ISO 9000, наприклад, основний підхід - процесний підхід і використання циклічної моделі PDCA для безперервного вдосконалення як самої системи, так і окремих її процесів.

Дуже велика кількість процесів управління з систем менеджменту якості з деякими змінами присутні і в СУІБ (внутрішні аудити ІБ, коригувальні і попереджуючі дії і т. д.).

СУІБ в організації визначається як частина загальної системи управління, яка заснована па використанні методів оцінки бізнес-ризиків для розробки, впровадження, функціонування, моніторингу, аналізу, супроводу (підтримки) і вдосконалення (поліпшення) ІБ.

Саме СУІБ визначає модель захисту інформаційних активів організації для досягнення її бізнес-цілей на основі оцінки ризиків і встановлення рівня прийнятних для організації ризиків, що відбивають ефективне усунення та управління ризиками.

Основним об'єктом розгляду стандарту ISO 27001 є «система менеджменту ІБ» (СМІБ). Метою побудови такої системи є вибір відповідних заходів управління ІБ, призначених для захисту інформаційних активів і які гарантують довіру зацікавлених сторін.

Цей стандарт визначає загальну організацію СУІБ, вимоги до неї, розробку і управління СУІБ, вимоги до документації СУІБ, відповідальність керівництва

в контексті управління ІБ (його обов'язки і управління ресурсами), внутрішній аудит СУІБ, аналіз СУІБ і напрямки удосконалення СУІБ і т. д. Застосування стандарту дозволить на основі процесного підходу управляти конфіденційністю, цілісністю і доступністю важливого активу компанії - інформацією.

Стандарт ISO 27001 також описує цикл PDCA як основу функціонування всіх процесів системи управління інформаційною безпекою. Стандарт ISO 27002 призначений для управління ІБ організації поза завлежності від сфери її діяльності (в ньому викладені практичні правила по управлінню ІБ - використанню СУІБ).

В область дії СУІБ організації включаються:

- бізнес-процеси;

- технології;

- активи (кадри, фінансові кошти, засоби обчислювальної техніки,, телекомунікаційні засоби, різні види інформації; процеси, продукти і послуги, що надаються всім зацікавленим сторонам-клієнтам, партнерам і т. д.);

- обґрунтування вибору обмеженої частини в організації (перерахування конкретних офісів, що входять в зону дії) або всієї організації в цілому.

Безпека бізнес-процесів забезпечується станом використовуваних інформаційних активів або дотриманням основних властивостей інформації: конфіденційності, цілісності, доступності. Основні процеси будь-якої системи управління інформаційною безпекою представлені на рис.2.20.

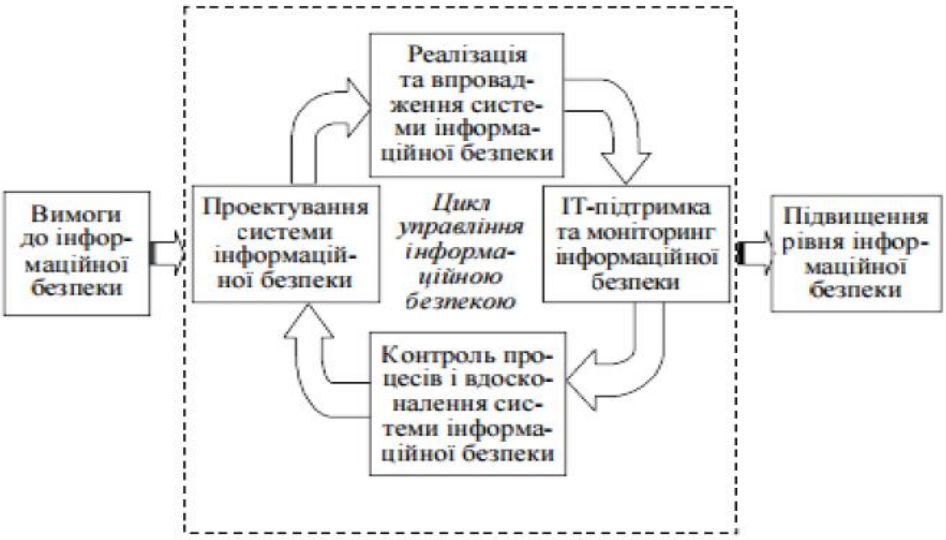


Рис.2.20. Основні процеси будь-якої системи управління інформаційною безпекою

У той же час СУІБ, яка побудована відповідно до вимог ISO / IEC 27001, являє собою комплексну систему, що включає і механізми управління, і механізми захисту інформації (рис. 2.21).

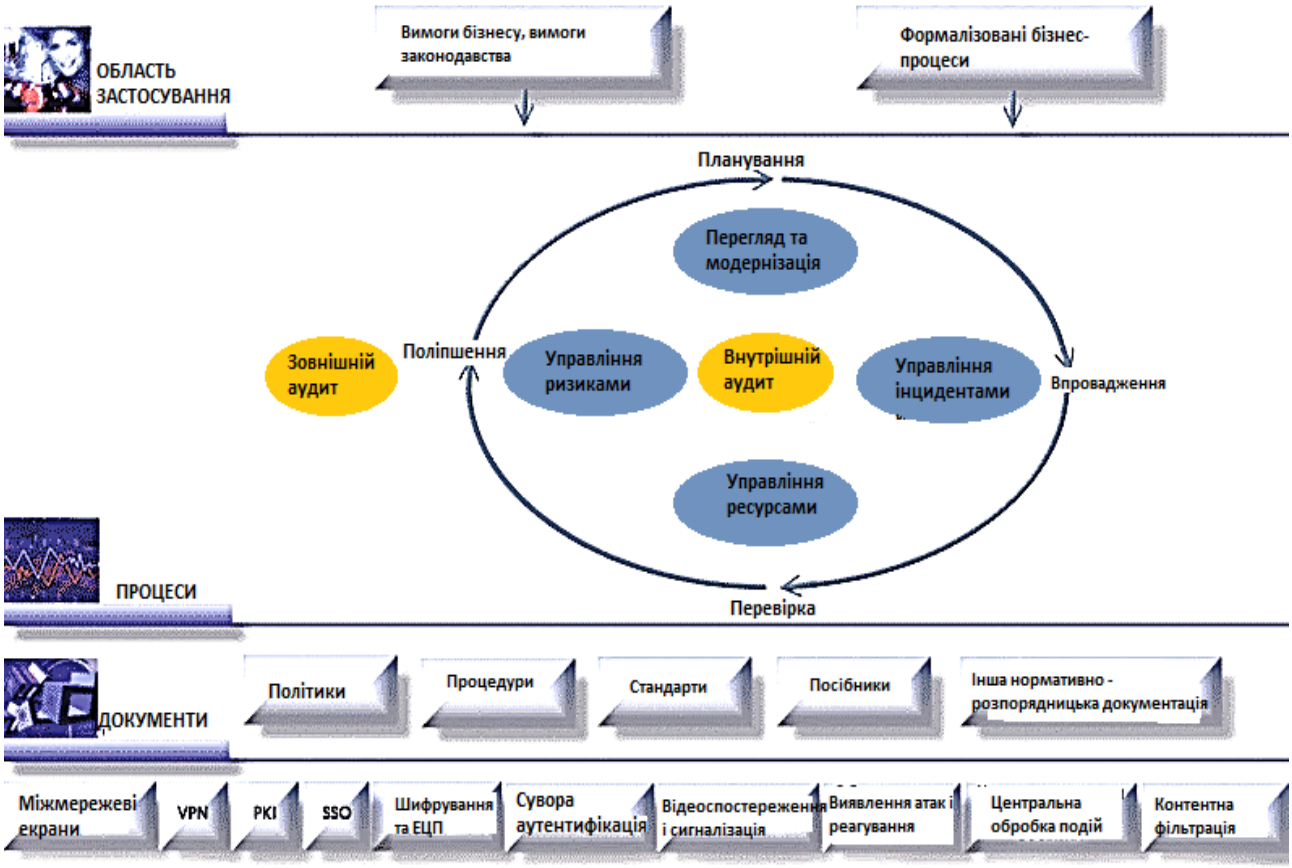


Рис.2.21. Схема комплексної СУІБ.

З точки зору процесів управління СУІБ входить в загальну систему менеджменту організації і надає додаткові механізми управління в частині забезпечення захисту критичної інформації (рис. 2.22).

Рис.2.22. Місце СУІБ в загальній системі менеджменту організації

«Процесний підхід» щодо забезпечення та управління ІБ, виконання будь-якої діяльності з СУІБ можуть розглядатися як процеси.

Основні види діяльності, це: розробка, реалізація, експлуатація, моніторинг, аналіз, супровід і вдосконалення СУІБ організації (рис.2.23).

Для опису процесів СУІБ циклічна модель PDCA передбачає безперервний цикл заходів: «планування - реалізація - перевірка - вдосконалення».

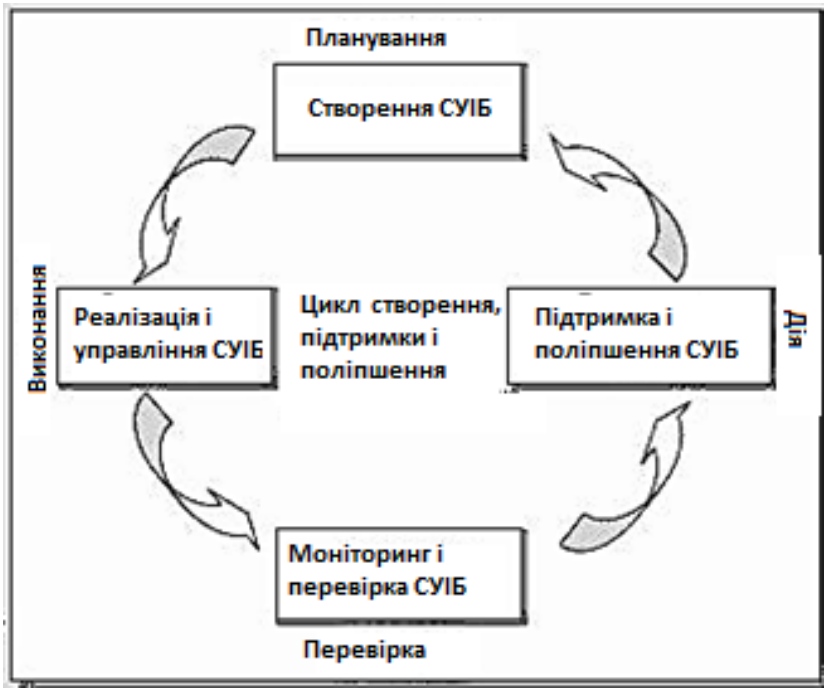


Рис.2.23.Циклічна модель PDCA для СУІБ

Одна з основних цілей впровадження СУІБ - створення таких умов в організації, коли відбувається постійний моніторинг і поліпшення кожного з процесів ОІБ і суміжних процесів. Взаємно посилюючи один до одного, ці поліпшення дозволяють створити все більш досконалу систему. Приватним критерієм поліпшення кожного з процесів може служити зниження кількості невідповідностей, що виявляються в ході різних перевірок, таких як внутрішні аудити, моніторинг ефективності процесів і т. д.

Початком розробки СУІБ є аудит організації на відповідність положенням ISO / IEC 27001.

Під час виконання аудиторських робіт вирішуються такі основні завдання:

- аналіз структури організації;

- аналіз інформації, що захищається області діяльності і організаційно-розпорядчих документів;

- аналіз структури і функціональних особливостей, використовуваних інформаційних технологій автоматизованої системи збору, обробки, передачі та зберігання інформації;

- перевірка виконання вимог ISO / IEC 27001 до СУІБ;

- розробка комплексних рекомендацій по методологічному, організаційно-управлінському, технологічному, технічному і апаратно-програмному забезпеченню для створення, побудови або вдосконалення СУІБ.

При введенні СУІБ в експлуатацію застосовуються всі розроблені процедури і механізми організації, які реалізують обрані цілі і засоби управління при створенні (вдосконаленні) комплексної СУІБ.

У процедури СУІБ включаються: управління документацією; управління записами; внутрішні аудити; коригуюча дія; запобіжні дії; управління інцидентами; аналіз функціонування СУІБ керівництвом організації; оцінка ефективності механізмів управління СУІБ та ін.

Останній етап формування СМІБ –це сертифікація на відповідність вимогам міжнародного стандарту ISO / IEC 27001.

Питання для самоконтролю

1. Які елементи процесу можуть бути виключені з визначення: вхідні дані процесу, вихідні дані процесу, керуючий вплив, ресурси?

2. Які види діяльності організації можна назвати процесом (або бізнес-процесом)?

3. Що розуміється під ресурсами в рамках визначення поняття процесу?

4. Що розуміється під керуючим впливом у рамках визначення понятті процесу?

5. У чому полягає процесний підхід?

6. Дайте визначення поняття «менеджмент».

7. Які основні функції управління?

8. Що таке система управління, яка заснована на процесному підході?

9. До яких процесів організації може бути застосована циклічна модель PDCA?

2.4. Застосування системного підходу до створення СУІБ організації

Системний підхід є оцінкою великої кількості інформації різної природи за допомогою універсальних показників.

Системний підхід включає такі розділи:

• виявлення всіх аспектів оцінюваного критерію:

• дослідження кожного з аспектів оцінюваного критерію

відповідними методами аналізу;

• універсалізація отриманих результатів оцінок;

• обробка результатів;

• вироблення рекомендацій щодо покращення оцінюваного критерію.

Системний підхід досліджує як управління загалом, і прийняття окремих рішень. Системний підхід відрізняється універсальністю, його успішне застосування значною мірою залежить від професійної підготовки експерта, який повинен мати чітке уявлення про специфічні особливості досліджуваного об'єкта та вміти виявити ефективні показники.

2.4.1. Системний підхід в процесах управління інформаційної безпекою

Існують три методологічних підходи до вивчення системних об'єктів (близьких за змістом один до одного):

- **структурно-функціональний аналіз;**
- **структуралізм;**
- **системний підхід.**

Головним методологічним принципом у всіх трьох підходах є принцип цілісності, проте він реалізується через різні поняття.

Структурно-функціональний аналіз займається вивченням різних частин системи з точки зору виконуваних ними функцій по відношенні до цілого. Він вживає два методологічні принципи:

- виділення структури об'єкта як деяким інваріант;
- функціональне опис цієї структури.

Основним поняттям в **структуралізму** є поняття структури, а функції елементів розглядається як передумова існування структури.

Системний підхід спрямований на отримання цілісного уявлення про об'єкт. У системному підході принцип цілісності реалізується через більш загальне поняття "системи", яке пов'язане з цілою низкою таких понять, як елемент, структура, функція, зв'язок, відношення, організація і т. д. Системний підхід використовується для дослідження не будь-яких об'єктів, а лише таких, які мають внутрішньо властивою їм цілісністю. Таким об'єктами, наприклад, є соціальні та складні технічні системи.

Системний підхід спирається на **два наукових напрямки**: **загальну теорію систем і системний аналіз.**

Предмет загальної теорії систем полягає в вивченням загальних властивостей систем довільної природи.

Предмет системного аналізу полягає в вивченням загальних закономірностей функціонування складних динамічних систем. Він являє собою комплекс спеціальних процедур, прийомів і методів, що забезпечують реалізацію системного підходу. Системний аналіз призначений для вирішення в першу чергу слабоструктурованих проблем, тобто проблем, склад елементів і взаємозв'язку яких встановлені тільки частково. Такі проблеми виникають, як правило, в ситуаціях, характерних наявністю фактору невизначеності і формалізації елементів.

В даний час спостерігається підвищений інтерес до стандарту ISO / IEC 27001 з боку організацій, що працюють в різних галузях. Відповідність йому стає важливим фактором комерційного успіху організації завдяки цілому ряду переваг. Сертифікат відповідності СУІБ вимогам стандарту ISO / IEC 27001 видається незалежним органом по сертифікації після успішного проходження сертифікаційного аудиту.

Самим трудомістким і складним етапом на шляху до сертифікації є власне створення системи управління ІБ і впровадження її механізмів в організації.

Зусилля, які витрачені на створення системи управління інформаційною безпекою, дозволять організації вийти на новий рівень відносин з клієнтами, партнерами, акціонерами, продемонструвати надійність компанії і надати можливість успішної конкуренції з провідними компаніями на міжнародному ринку.

Системний підхід в процесах управління ІБ - це спосіб мислення і аналізу, згідно з яким СУІБ розглядається як сукупність взаємопов'язаних елементів, що мають спільну мету - забезпечити безпеку інформації.

Після цілеспрямованого об'єднання елементів за принципом «кожен з кожним», система набуває нові специфічні властивості, які не притаманні жодному зі складових елементів. При цьому першорядне значення набувають то властивості системи, які визначають якість взаємодії її елементів.

На жаль, необхідність системного підходу до питань забезпечення безпеки інформаційних технологій поки ще не знаходить належного розуміння в користувачів сучасних ІКС. Однак, сьогодні фахівці з різних галузей знань, так чи інакше, змушені займатися питаннями забезпечення інформаційної безпеки.

Фахівці найчастіше не розуміють один одного, оскільки у кожного з них свій підхід, своя модель представлення системи захисту інформації. Такий стан справ зумовлений відсутністю системного підходу, який би запропонував врахувати взаємні зв'язки (відношення) між існуючими поняттями, визначеннями, принципами, засобами і механізмами ІБ.

Процес створення СУІБ вимагає установки жорстких логічних і функціональних зв'язків між різнорідними компонентами СУІБ. При цьому значимість властивостей окремих елементів СЗІ знижується, а на перший план висуваються загальносистемний властивості. Як показує практика, саме якість зазначених зв'язків визначає ефективність СУІБ в цілому.

СУІБ повинна бути саме системою, а не простим, багато в чому випадковим і хаотичним набором Деяких технічних засобів і організаційних заходів, як це найчастіше спостерігається на практиці.

Поняття системності полягає не просто в створення відповідних механізмів інформаційної безпеки, а являє собою регулярний процес, здійснюваний на всіх етапах життєвого циклу ІКС. При цьому всі кошти, методи і заходи, які використовуються для захисту інформації об'єднуються в цілісний механізм - СУІБ.

СУІБ (варіант) - це документована система управління, певна в рамках компанії, яка включає в себе:

1. Політику інформаційної безпеки (визначає поняття ІБ, цілі і завдання СУІБ, відповідальність керівництва і т.д.).

2. План по оцінці ризиків безпеки (визначає порядок оцінки і аналізу ризиків безпеки).

3. Перелік інформаційних активів, що підпадають в області дії СУІБ.

4. Положення про застосування контролів (визначає набір контрзаходів, спрямованих на мінімізацію ризиків ІБ).

5. Вичерпний набір взаємопов'язаних процедур, приватних політик (підполітік), регламентів та інструкцій, спрямованих на формалізацію процесів захисту інформації.

Підполітики – це документи політики безпеки процедурного рівня.

Основні розділи Політики інформаційної безпеки:

- Цілі і завдання Політики безпеки
- Законодавча і нормативна основа забезпечення ІБ
- Модель загроз інформаційній безпеці
- Вимоги до комплексної системи захисту організації
- Організаційні заходи захисту інформації
- Технологічні заходи захисту інформації
- План короткострокових і довгострокових заходів по реалізації Політики безпеки

Приватні політики (підполітики) ІБ

- надання доступу до інформаційних ресурсів
- забезпечення безпеки комунікацій

- забезпечення безпеки додатків
- вибору технічних засобів
- антивірусний захист;
- забезпечення фізичної безпеки засобів інформатизації і захисту інформації;
- взаємодії з організаціями-підрядниками.

Наявність системи управління інформаційною безпекою (Information Security Management), зокрема аналізу інформаційних ризиків та управління ними (Risk Management), є обов'язковою умовою організації режиму ІБ на будь-якому підприємстві. Підприємства застосовують будь-який варіант системи управління ризиками. Багато зарубіжних національних інститутів стандартів та організацій, що спеціалізуються на вирішенні комплексних проблем інформаційної безпеки, запропонували схожі концепції управління інформаційними ризиками.

Вважається, що система управління ризиками організації має мінімізувати можливі негативні наслідки, пов'язані з використанням інформаційних технологій, та забезпечити виконання основних бізнес-цілей підприємства.

Для цього система управління ризиками інтегрується у систему управління життєвим циклом інформаційних технологій компанії, чим підтверджується виконанням вимог базового стандарту в сфері управління ІБ- ISO:27001.

Схема управління ризиками, інтегрована в СУІБ, представлена на рис.2.24.

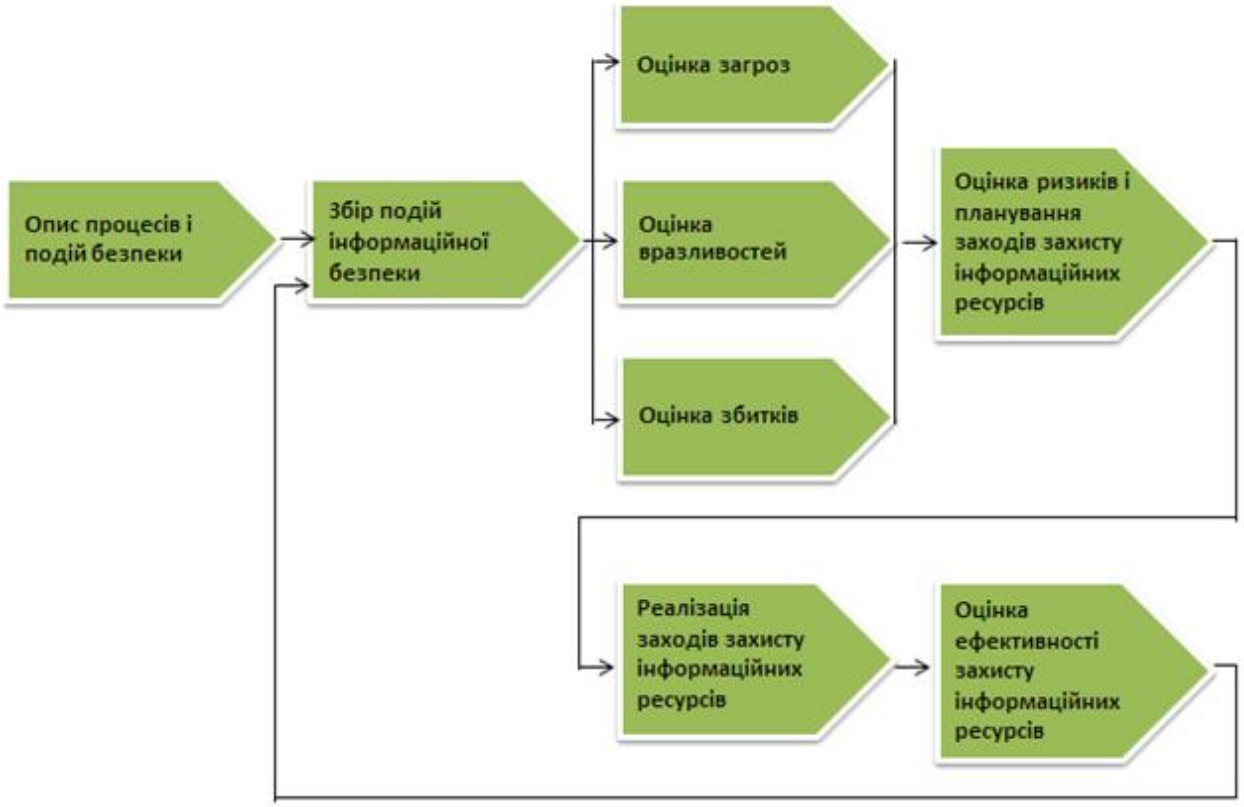


Рис.2.24. Схема управління ризиками інтегрована в СУІБ

На етапі управління ризиками розробляється певна стратегія управління ризиками. Наприклад, тут можливі такі підходи до управління інформаційними ризиками компанії:

- зменшення ризику;
- ухилення від ризику;
- зміна характеру ризику;
- прийняття ризику.

Загальна схема управління ризиками включає якісний і кількісний аналіз по результатам моніторингу і контролю подій ІБ, які приводять до ризиків представлена на рис.2.25.

Рис.2.25. Схема управління ризиками (загальна)

Нині існують різні підходи до оцінки ризиків. Вибір підходу залежить від рівня вимог, що пред'являються в організації до режиму інформаційної безпеки, характеру, що приймаються до уваги загроз (спектру впливу загроз) та ефективності потенційних контрзаходів щодо захисту інформації. Зокрема, розрізняють мінімальні, або базові, і підвищені, або повні вимоги до режиму ІБ.

Для формулювання додаткових підвищених вимог необхідно:

- визначити цінність ресурсів;

– до стандартного набору додати перелік загроз, актуальних для досліджуваної інформаційної системи;

- розрахувати ймовірності загроз;

- виявити вразливості ресурсів;

– оцінити потенційні збитки від впливів зловмисників.

Порядок оцінки і аналізу ризиків інформаційної безпеки представлений на рис.2.26.

Якісна шкала оцінки ризиків представлена в табл.2.2 і 2.3, а приклад визначення рівня ризику інформаційної безпеки- у табл.2.4.

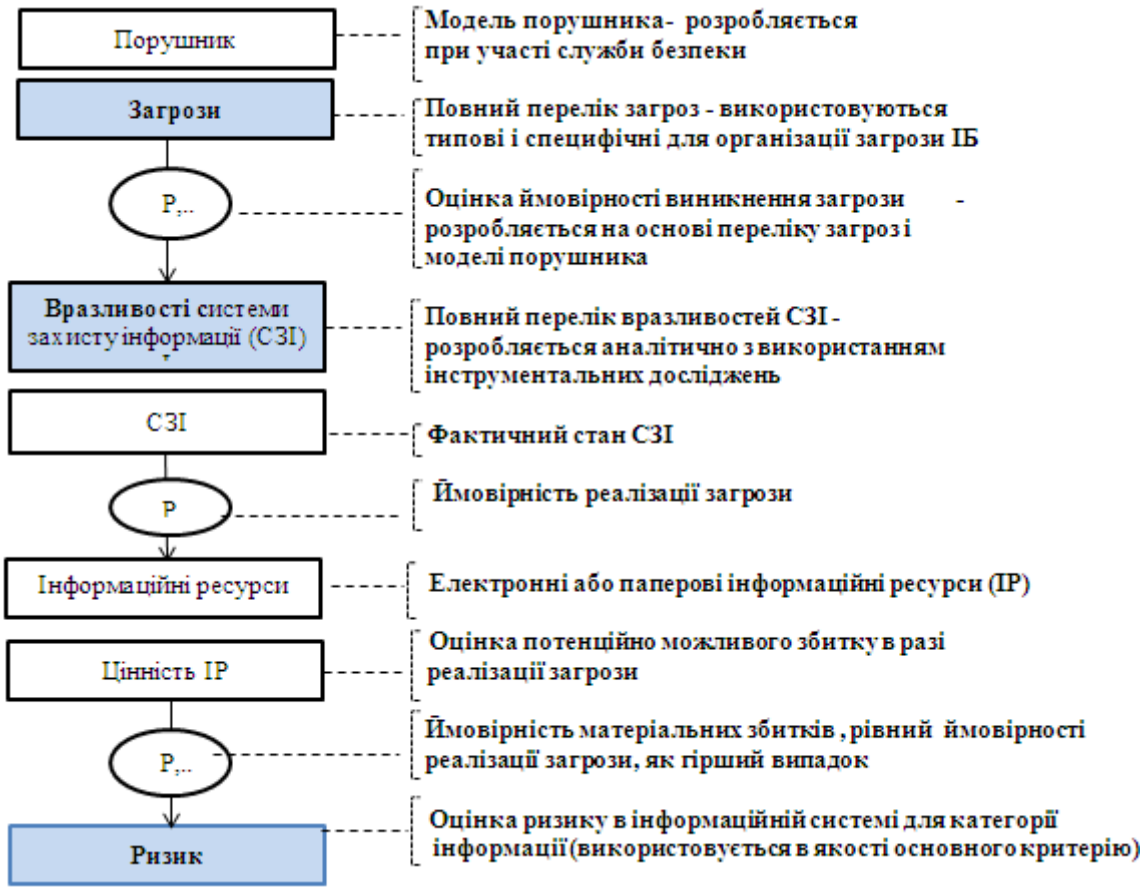


Рис.2.26. Схема оцінки ризику

Таблиця 2.2.

Якісна оцінка ризиків (збитки)

Якісна шкала оцінки рівня збитків	
1	Малий збиток
	Приводить до незначних втрат матеріальних активів, які швидко відновлюються, або до незначного впливу на репутацію компанії
2	Помірний збиток
	Викликає помітні втрати матеріальних активів або помітний вплив на репутацію кампанії
3	Середній збиток
	Приводить до істотних втрат матеріальних активів або наносить значну шкоду репутації компанії
4	Великий збиток
	Викликає великі втрати матеріальних активів і наносить велику шкоду репутації компанії
5	Критичний збиток
	Приводить до критичних втрат матеріальних активів або до повної втрати репутації кампанії

Таблиця 2.3.

Якісна оцінка ризиків (атаки)

Якісна шкала оцінки ймовірності проведення атаки	
1	Дуже низька
	Атака практично ніколи не буде проведена. Рівень відповідає числовому інтервалу ймовірності [0, 0.25)
2	Низька
	Ймовірність проведення атаки досить низька. Рівень відповідає числовому інтервалу ймовірності [0.25, 0.5)
3	Середня
	Ймовірність проведення атаки приблизно рівна 0,5
4	Висока
	Атака , скоріше всього, буде проведена. Рівень відповідає числовому інтервалу ймовірності (0.5, 0.75]
5	Дуже висока
	Атака майже 100% буде проведена. Рівень відповідає числовому інтервалу ймовірності (0.75, 1]

Таблиця 2.4.

Приклад визначення рівня ризику інформаційної безпеки

Імовірність атаки / Збиток	Дуже низька	Низька	Середня	Висока	Дуже висока
Малий збиток	Низький ризик	Низький ризик	Низький ризик	Середній ризик	Середній ризик
Помірний збиток	Низький ризик	Низький ризик	Середній ризик	Середній ризик	Високий ризик
Середній збиток	Низький ризик	Середній ризик	Середній ризик	Високий ризик	Високий ризик
Великий збиток	Середній ризик	Середній ризик	Високий ризик	Високий ризик	Високий ризик
Критичний збиток	Середній ризик	Високий ризик	Високий ризик	Високий ризик	Високий ризик

2.4.2. Практика побудови системи управління інформаційною безпекою

Є компанії, які працюють з аутсорсингу і надають своїм замовникам повний комплекс послуг в області захисту інформаційних ресурсів і широкий спектр інших IT-сервісів (забезпечення засобами захисту інформації на основі найсучасніших технологій, надійного обладнання і програмного забезпечення; побудова комплексних систем ІБ, побудова сучасної IT-інфраструктури і т. д.).

Наприклад, при створенні СУІБ фахівці компанії ARinteg керуються найкращими світовими стандартами і практиками, зокрема рекомендаціями експертів Інституту програмування Університету Карнегі-Меллон, згідно з якими ефективне управління ІБ бізнесу має характеризуватися такими ознаками:

1. Охоплення всього підприємства
2. Відповідальність керівників
3. ІБ розглядається в якості вимоги бізнесу
4. ІБ забезпечується з урахуванням ризиків
5. Визначено ролі і розділені зони відповідальності
6. Адекватна політика інформаційної безпеки
7. Достатність ресурсів, які виділяються
8. Персонал навчений і поінформований
9. Безпечний життєвий цикл ПЗ
10. Планована, керована і яка вимірюється.
11. Регулярний аудит

СУІБ може бути представлена у вигляді моделі процесів інформаційної безпеки (див. рис.2.27), що відповідає спеціальним нормативним документам щодо забезпечення інформаційної безпеки - міжнародним стандартом ISO / IEC 15408 "Інформаційна технологія - методи захисту - критерії оцінки інформаційної безпеки і стандарту" - це сукупність зовнішніх і внутрішніх факторів і їх вплив на стан інформаційної безпеки в компанії і на забезпечення схоронності ресурсів (матеріальних або інформаційних). Прямокутниками на рис. представлені зовнішні та внутрішні фактори. Пунктирними стрілками вказані напрямки управлінського впливу, а суцільними - природного можливого впливу.

У схемі показані **об'єктивні фактори**:

- загрози інформаційній безпеці. Вони характеризуються ймовірністю виникнення і реалізації;
- уразливості системи інформаційної безпеки, які впливають на ймовірність реалізації загрози;

- втрати, що відображають реальний збиток в результаті реалізації загрози інформаційній безпеці.

- ризики, що відображають завдання шкоди організації в результаті реалізації загрози інформаційній безпеці.

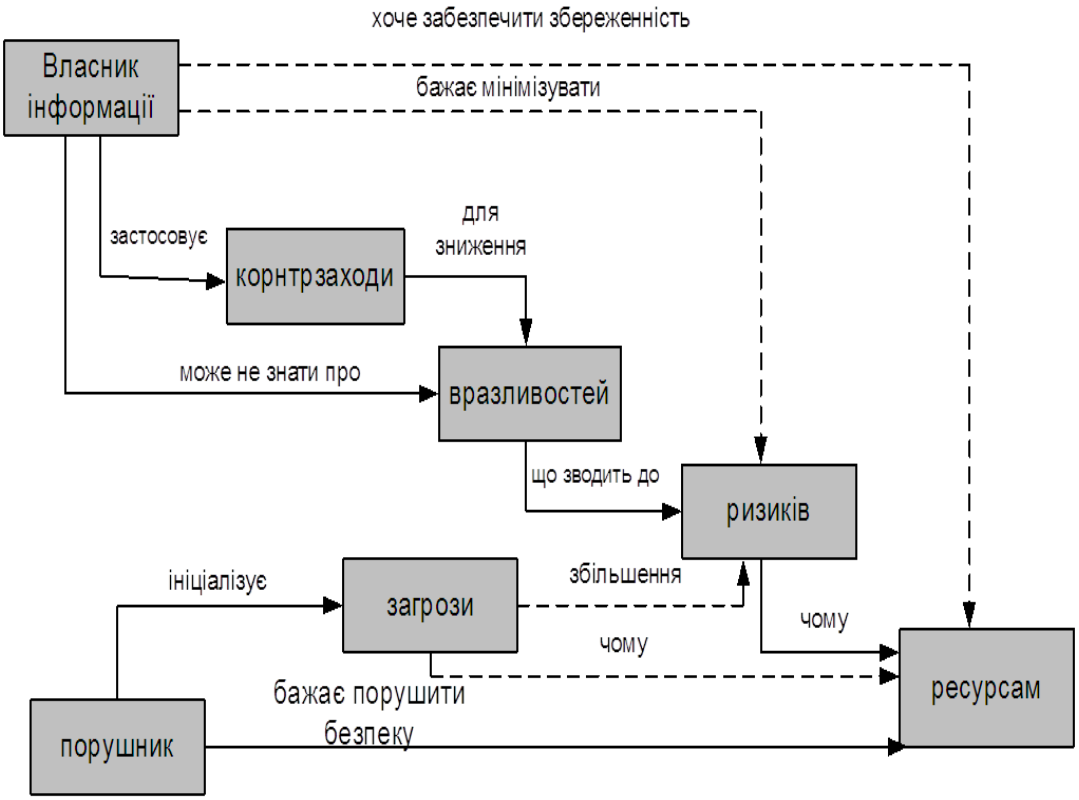


Рис.2.27. Схема СУІБ у вигляді моделі процесів інформаційної безпеки

Для побудови збалансованої системи інформаційної безпеки передбачається спочатку провести аналіз ризиків в області інформаційної безпеки. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему інформаційної безпеки (контрзаходи) належить побудувати таким чином, щоб досягти заданого рівня ризику.

Методика проведення аналітичних робіт включає: визначення меж дослідження, побудову моделі інформаційної технології, вибір контрзаходів, управління ризиками, оцінку захищеності, аналіз ризиків.

Запропонована методика дозволяє:

* Повністю проаналізувати і документально оформити вимоги, пов'язані із забезпеченням інформаційної безпеки;

* Уникнути витрат на зайві заходи безпеки, можливі при суб'єктивній оцінці ризиків;

* Надати допомогу в плануванні і здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем;

* Забезпечити проведення робіт в стислі терміни;

* Уявити обгрунтування для вибору заходів протидії;

* Оцінити ефективність контрзаходів, порівняти різні варіанти контрзаходів.

Визначення меж дослідження

В ході робіт повинні бути встановлені межі дослідження. Для цього необхідно виділити ресурси інформаційної системи, для яких в подальшому будуть отримані оцінки ризиків. При цьому належить розділити розглядаються ресурси і зовнішні елементи, з якими здійснюється взаємодія. Ресурсами можуть бути кошти обчислювальної техніки, програмне забезпечення, дані. Прикладами зовнішніх елементів є мережі зв'язку, зовнішні сервіси і т. п.

Побудова моделі інформаційної технології

При побудові моделі будуть враховуватися взаємозв'язку між ресурсами. Наприклад, вихід з ладу будь-якого обладнання може призвести до втрати даних або виходу з ладу іншого критично важливого елемента системи. Подібні взаємозв'язки визначають основу побудови моделі організації з точки зору ІБ.

Ця модель, в відповідність до запропонованої методики, будується наступним чином: для виділених ресурсів визначається їх цінність, як з точки зору асоційованих з ними можливих фінансових втрат, так і з точки зору шкоди репутації організації, дезорганізації її діяльності, моральної шкоди від розголошення конфіденційної інформації і т. д. Потім описуються взаємозв'язку ресурсів, визначаються загрози безпеки і оцінюються ймовірності їх реалізації.

Вибір контрзаходів

На основі побудованої моделі можна обґрунтовано вибрати систему контрзаходів, що знижують ризики до допустимих рівнів і володіють найбільшою цінової ефективністю. Частиною системи контрзаходів будуть рекомендації з проведення регулярних перевірок ефективності системи захисту.

Управління ризиками

Забезпечення підвищених вимог до ІБ передбачає відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Планування цих заходів проводиться після завершення етапу аналізу ризиків та вибору контрзаходів. Обов'язковою складовою частиною цих планів є періодична перевірка відповідності існуючого режиму ІБ політиці безпеки, сертифікація інформаційної системи (технології) на відповідність вимогам певного стандарту безпеки.

Оцінка захищеності

На завершення робіт, можна буде визначити міру гарантії безпеки інформаційного середовища Замовника, засновану на оцінці, з якої можна довіряти інформаційному середовищі об'єкта.

Даний підхід передбачає, що велика гарантія випливає з застосування великих зусиль при проведенні оцінки безпеки.

Адекватність оцінки заснована на:

* Залученні в процес оцінки більшого числа елементів інформаційного середовища об'єкта Замовника;

* Глибині, що досягається за рахунок використання при проектуванні системи забезпечення безпеки більшого числа проектів і описів деталей виконання;

* Строгості, яка полягає в застосуванні більшого числа інструментів пошуку і методів, спрямованих на виявлення менш очевидних вразливостей або на зменшення ймовірності їх наявності.

Відповідальним в управлінні ІБ є розробка і використання методології аналізу ризиків, результатом якої є їх оцінка. Мета процесу оцінювання

ризиків полягає у визначенні характеристик ризиків в інформаційній системі і її ресурсах. На основі таких даних вибираються необхідні засоби управління ІБ.

Процес оцінювання ризиків містить кілька етапів:

* Опис об'єкта і заходів захисту;
* Ідентифікація ресурсу і оцінювання його кількісних показників (визначення потенційного негативного впливу на бізнес);
* Аналіз загроз інформаційної безпеки;
* Оцінка вразливостей;
* Оцінювання існуючих і передбачуваних засобів забезпечення інформаційної безпеки;
* Оцінка ризиків.

Ризик характеризує небезпеку, якій може піддаватися система і організація, в яку вона впроваджена, і залежить від:

* Показників цінності ресурсів;
* Ймовірностей нанесення збитку ресурсів (які висловлюються через ймовірності реалізації загроз для ресурсів);
* Ступеня легкості, з якою уразливості можуть бути використані при виникненні загроз (уразливості системи захисту);
* Існуючих або планованих способів забезпечення ІБ.

Розрахунок цих показників виконується **на основі математичних методів**, що мають такі характеристики, як обгрунтування і параметри точності методу.

Побудова профілю захисту

На цьому етапі розробляється план проектування системи захисту інформаційного середовища Замовника. Проводиться оцінка доступних засобів, здійснюється аналіз та планування розробки та інтеграції засобів захисту (рис. 2). Необхідною елементом роботи є твердження у Замовника допустимого ризику об'єкта захисту.

Забезпечення підвищених вимог до інформаційної безпеки передбачає відповідні заходи на всіх етапах життєвого циклу інформаційних технологій.

Планування цих заходів проводиться після завершення етапу аналізу ризиків та вибору контрзаходів. Обов'язковою складовою частиною цих планів є періодична перевірка відповідності існуючого режиму ІБ політиці безпеки, сертифікація інформаційної системи (технології) на відповідність вимогам певного стандарту безпеки.

Робота з побудови плану захисту об'єкта починається з побудови профілю захисту даного об'єкта. При цьому частина цієї роботи вже була пророблена при проведенні аналізу ризиків.

Таким чином, в цілому розглянута методика дозволяє оцінити або переоцінити рівень поточного стану інформаційної безпеки підприємства, виробити рекомендації щодо забезпечення (підвищення) інформаційної безпеки підприємства, знизити потенційні втрати підприємства або організації шляхом підвищення стійкості функціонування корпоративної мережі, розробити концепцію і політику безпеки підприємства, а також запропонувати плани захисту конфіденційної інформації підприємства, що передається по відкритих каналах зв'язку, захисту інформації підприємства від навмисного спотворення (руйнування), несанкціонованого доступу до неї, її копіювання або використання

Питання для самоконтролю

1. Що таке ризик?
2. Розкрийте призначення трьох методологічних підходів до вивчення системних об'єктів.
3. Системний підхід у процесах управління ІБ, це:_____. Показати варіанти.
4. Приведіть основні розділи Політики інформаційної безпеки.
5. Покажіть схему управління ризиками для системи ІБ підприємства.
6. Яка існує таблиця оцінки рівня ризиків ІБ (шкали оцінювання)?
7. Як може бути представлена СУІБ у вигляді моделі процесів інформаційної безпеки?

8. Які ознаки характеризують ефективне управління ІБ бізнесу? Перелічити.

9. Перелічіть мети системи інформаційної безпеки .

10. Які показники сили функції захисту?

11. Приведіть можливий алгоритм оцінювання інформаційних ризиків.

12. У чому полягає гарантія безпеки інформаційного середовища?

13. У чому полягає мета процесу оцінювання ризиків ?

2.5. Застосування підходу до створення системи управління інцидентами інформаційної безпеки організації

Управління інцидентами є одним з найважливіших процесів розвитку й удосконалювання системи управління інформаційною безпекою.

Саме цей процес дозволяє зрозуміти недоліки процесів і контролю забезпечення інформаційної безпеки, одержати вихідні дані для розробки планів відновлення безперервності бізнесу й визначити ключові ролі персоналу у випадку виникнення позаштатних ситуацій в будь-якої організації.

Ключові цілі процесів управління інцидентами:

1. Швидко знайти інцидент.

2.Точно ідентифікувати інцидент.

3. Правильно управляти інцидентом.

4. Стримати інцидент і мінімізувати наслідки.

5. Відновити сервіси.

6. Зрозуміти причини.

7. Запровадити поліпшення для запобігання повторень.

Як показують дослідження, висвітлення основних процедур та процесів управління інцидентами завжди будуть пов’язані із організацією та супроводженням систем менеджменту інформаційною безпекою.

2.5.1 Розробка та впровадження системи управління інцидентами інформаційної безпеки

Останнім часом бізнес все частіше турбують питання забезпечення ІБ.

Комп'ютер без пароля, забуті ключі на столі, пачка конфіденційної роздрукованої документації біля принтера, відсутність мережевого екрану з Інтернет - це тільки кілька прикладів проблем з безпекою, які можуть привести до витоку інформації.

Виходом із ситуації є впровадження Системи Менеджменту Інформаційної Безпеки (СМІБ), заснованої на вимогах міжнародного стандарту ISO 27001(рис.2.28).

Впровадження СМІБ проводиться в кілька етапів:

• Оцінка існуючої СМІБ на підприємстві.

Проводиться аналіз усталених процесів в області організації ІБ. Порівнюється поточна ситуація зі стандартом. Визначаються цілі впровадження СМІБ.

• Оцінка ризиків.

Впроваджується система управління ризиками. Фахівці допомагають ідентифікувати і ранжувати активи, визначити загрози і рівень ризиків.

• Розробка комплекту документації.

Розробка процедур і політик безпеки, на підставі результатів оцінки ризиків, націлених на досягнення цілей СМІБ.

• Розробка і прийняття заходів, спрямованих на забезпечення ІБ.

Впровадження організаційних і технічних засобів захисту активів.

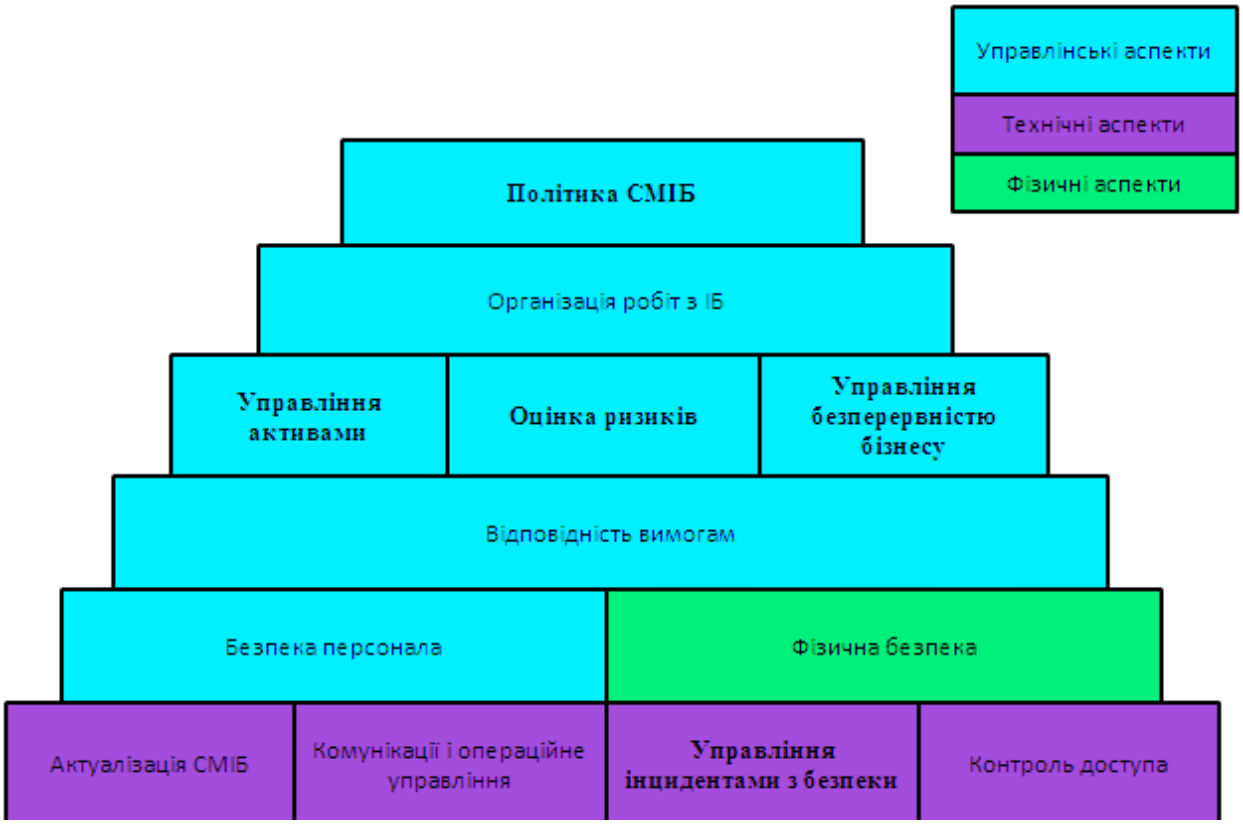


Рис.2.28. Схема системи менеджменту інформаційної безпеки

При введенні СМІБ в експлуатацію задіяні всі розроблені процедури і механізми організації, реалізують обрані цілі і засоби управління при створенні (вдосконалення комплексної СМІБ.

Розробляються політики і процедури повинні охоплювати наступні **ключові процеси СМІБ**:

- управління ризиками;
- управління інцидентами;
- управління ефективністю системи;
- управління персоналом;
- управління документацією та записами системи управління ІБ;
- перегляд і модернізація системи;
- управління безперервністю бізнесу і відновлення після переривань.

У цих процесах також присутні внутрішні аудити і оцінка ефективності механізмів управління СМІБ.

Всі розроблені положення політики СМІБ, підполітік, процедур та інструкцій доводяться до відома рядових співробітників при їх початковому і наступному періодичному навчанні та інформуванні.

Для нових підприємств і тих, у яких вже є налагоджена СМІБ, пропонується також впровадження або вдосконалення **системи управління інцидентами інформаційної безпеки (СУІБ)**- на рис. 2.29.

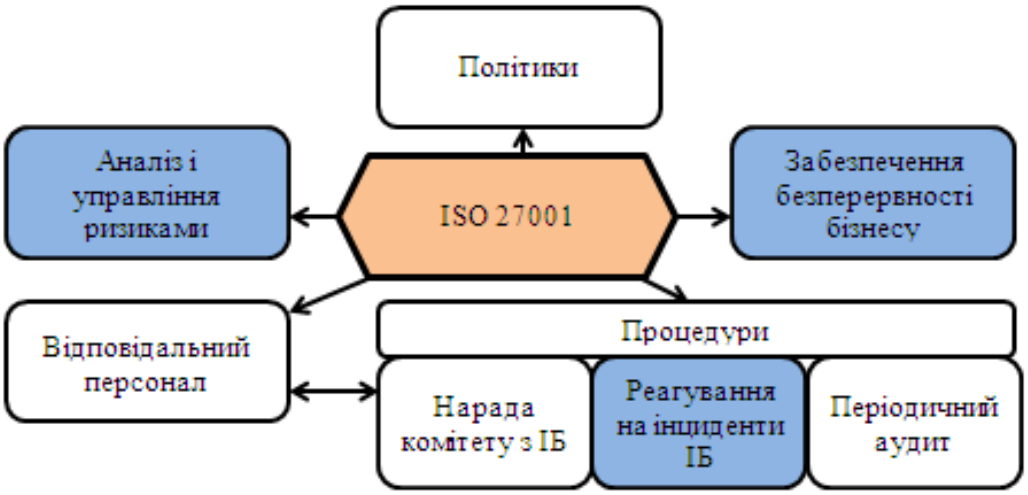


Рис.2.29. Удосконалена комплексна СМІБ (СУІБ)

Місце системи управління інцидентами ІБ, як підсистеми при реалізації системного підходу до побудови СУІБ, представлено на рис.2.30 (відповідно до стандарту ISO / IEC 27035).

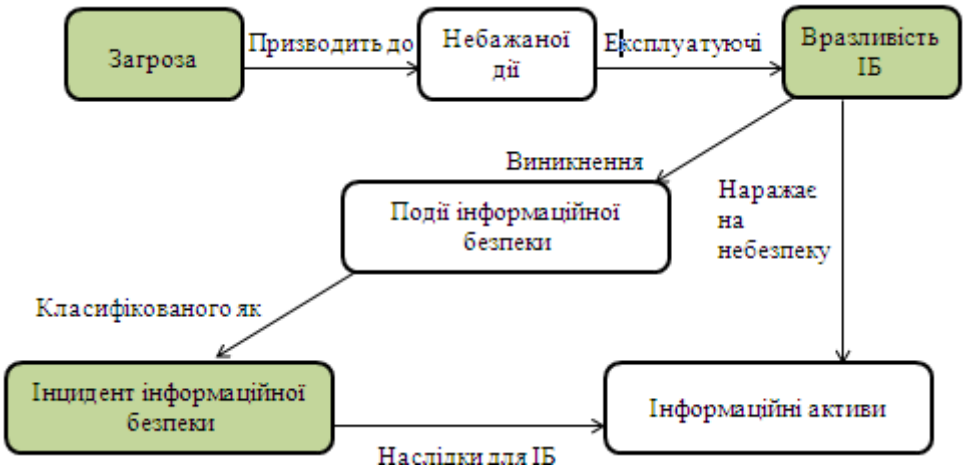


Рис.2.30. Ланцюги інциденту інформаційної безпеки в СУІБ

Зі зберігання й пошуку подій, пов'язаних з інцидентами, в СУІБ з метою проведення аналізу або відповідності вимогам з керівними документами на сьогоднішній день є абсолютним мінімумом для підприємств усіх масштабів, що явно недостатньо!

СУІБ повинна дозволяти в першу чергу забезпечення виконання завдань, пов'язаних з організацією захисту від нових видів атак (комплексних атак, атак розподілених у часі):

• проводити аналіз журналів подій і даних, що надходять від інформаційних систем в режимі реального часу;

• здійснювати аналіз контексту;

• корелювати події ІБ, що надходять від безлічі різних систем - серверів, мережевого обладнання, ПЗ з урахуванням таких параметрів як пріоритет події, цінність системи та ін .;

• виносити рішення про важливість того, що відбувається;

• генерувати сповіщення про інцидент;

• забезпечити можливість групової роботи за рішенням з інцидентами відповідальними співробітниками.

Такі компанії, як вендори: ArcSight, McAfee, IBMQradar, EnterasysSIEM - пропонують свої системи. Основні елементи цих систем показані на рис.2.31.

Рис.2.31. Схема системи управління інцидентами ІБ

2.5.2. Управління інцидентами інформаційної безпеки

Для опису процедури управління інцидентами безпеки використовується також класична модель безперервного поліпшення процесів - модель PDCA.

Стандарт ISO 27001 описує модель PDCA як основу функціонування всіх процесів СУІБ. Природно, що і процедура управління інцидентами (реалізація процесного підходу) також підпорядковується цієї моделі PDCA (рис.2.32).

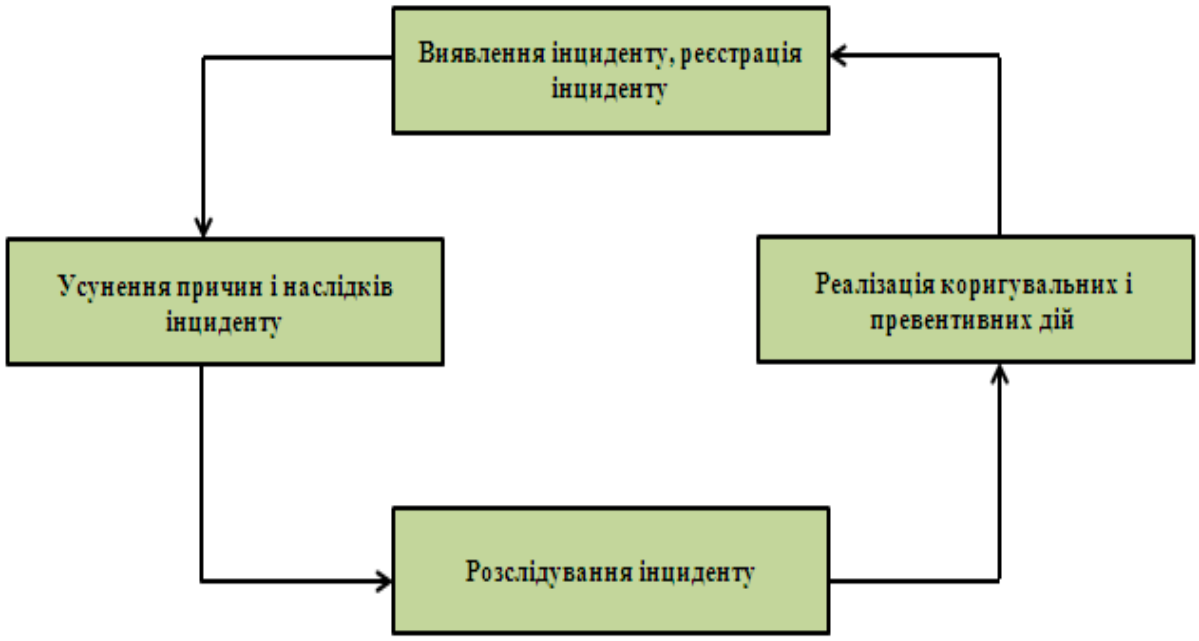


Рис.2.32. Система менеджменту (управління) інцидентів (ами) ІБ (варіант)

Стратегія управління інцидентами інформаційної безпеки пропонується відповідно до основних етапів функціонування самої системи: підготовка, виявлення, аналіз, покращення (рис.2.33).

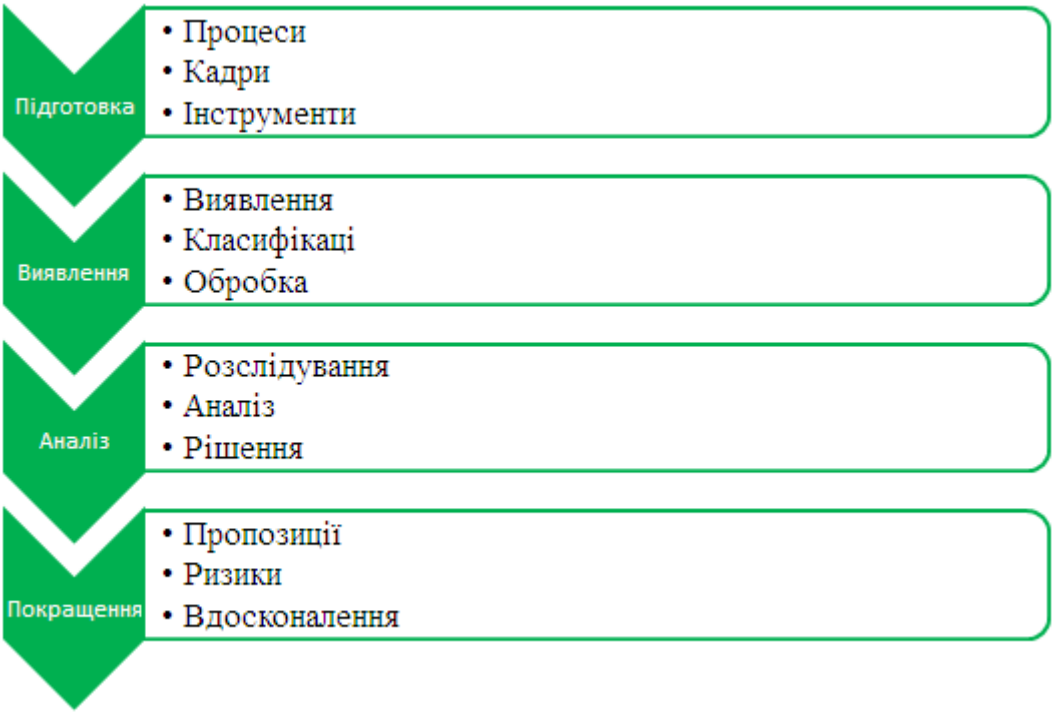


Рис.2.33. Стратегія управління інцидентами інформаційної безпеки

Виявлення і реєстрація інциденту

Інцидент ІБ може помітити користувач або адміністратор системи. Для користувачів слід розробити інструкцію, яка, як правило, містить опис, в якому вигляді співробітник повинен повідомити про виникнення інциденту, координати відповідальних осіб, а також перелік дій, які співробітник може виконати самостійно (або попередити про те, що виконувати будь-які дії самостійно заборонено). Такий звіт повинен містити докладний опис інциденту, перерахування співробітників, залучених в інцидент, прізвище співробітника, який зафіксував інцидент і дату виникнення та реєстрації інциденту.

Потрібно розробити інструкцію для фахівця, в обов'язки якого входить реєстрація інциденту. Співробітник, який знайшов інцидент, зв'язується зі співробітником, відповідальним за реєстрацію інциденту і виконання подальших дій (він може усунути наслідки і причини.

Така інструкція може містити, наприклад, правила і термін реєстрації інциденту, перелік необхідних первинних інструкцій для співробітника, який знайшов інцидент, крім того, опис порядку передачі інформації про інцидент

відповідного фахівця, порядок контролю за усуненням наслідків і причин інциденту.

Для ефективного виявлення інцидентів (рис.2.34) необхідно збирати і аналізувати події ІБ на всіх рівнях середовища обробки інформації, що захищається - в DBMS, NETWORK (мережі) і OS (ОС).

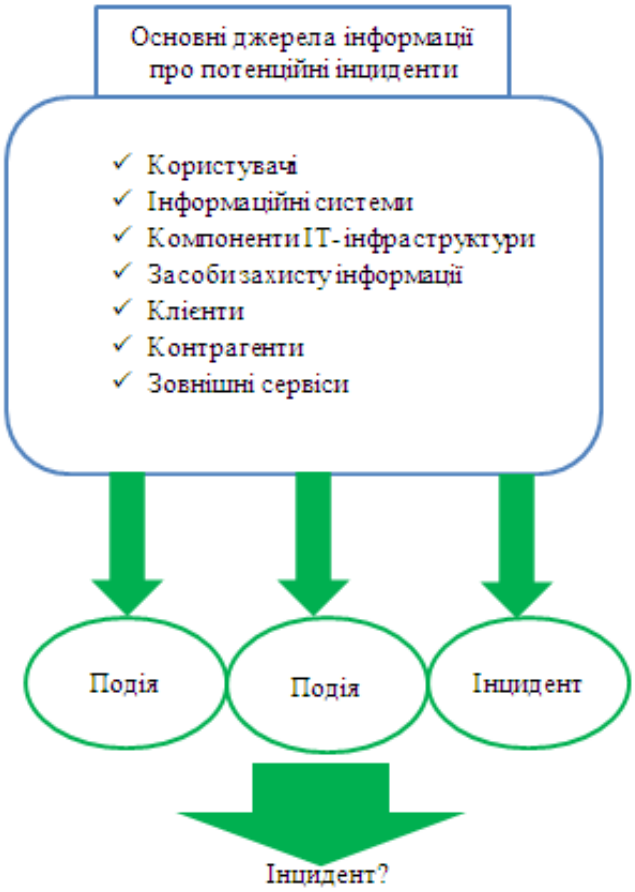


Рис.2.34. Виявлення інцидентів

Нижче розкриті практики використання основних дій з управління інцидентами ІБ.

Практика

Інформація про інциденти ІБ може надходити за наступними каналами:

- журнали реєстрації мережевого і міжмережевого обладнання;

- журнали реєстрації загальносистемного програмного забезпечення;

- журнали реєстрації інфраструктурного програмного забезпечення; журнали реєстрації прикладного програмного забезпечення;

- оповіщення антивірусних підсистем; оповіщення підсистем виявлення атак;

- оповіщення підсистем моніторингу про події ІБ

- оповіщення підсистем кореляції про події ІБ

- оповіщення підсистем запобігання (контролю) витоків ІБ

- оповіщення інших підсистем,

- інформація, що отримується від співробітників по будь-яких каналах зв'язку (телефон, електронна пошта, КІС, мовний канал, ін.).

Всі процеси виявлення інцидентів ІБ повинні підлягати обов'язковому документуванню. Всі процедури з необхідним ступенем деталізації описуються у відповідних регламентах та інструкціях

Практика

Аналіз інциденту ІБ

• Факт спроби НСД

• Чи продовжується НСД зараз

• Хто є джерелом НСД

• Що є об'єктом НСД

• Коли відбувалася спроба НСД

• Як і за яких обставин була зроблена спроба НСД

• Точка входу порушника в систему

• Чи була спроба НСД успішної

• Визначити системні ресурси, безпека яких була порушена

• Яка мотивація спроби несанкціонованого доступу (отримання прибутку, саботаж, шпигунство, і т.д.

Реєстрація інцидентів ІБ

• опис характеру інциденту і його наслідків;

• місце, дата і час виникнення та вжиті заходи щодо інциденту;

• опис подальших дій і поточний статус розслідування;

• коментарі учасників розслідування;

• причини виникнення інциденту і результати розслідування, включно із залученням винних до відповідальності;

• перелік свідоцтв (з обов'язковим зазначенням джерел), зібраних в ході обробки інциденту;

• планувалися і впроваджені контрзаходи, оцінка результатів їх впровадження.

Для реагування на інциденти ІБ в компанії повинна бути створена спеціальна група реагування на інциденти ІБ (ГРРІБ), що складається з менеджерів і фахівців.

Всі процеси реагування на інциденти, типізовані за ознакою приналежності порушення будь-якої політики ІБ, повинні обов'язково документуватися. Документування сценаріїв реагування на кожен можливий інцидент ІБ проводиться експертним шляхом і оформляється у вигляді набору відповідних регламентів і правил.

Першочерговим завданням ІБ є стримування інциденту ІБ, тобто прийняття всіх необхідних заходів для локалізації інциденту ІБ і перешкоджають його поширенню.

ГРРІБ повинна мати виділене захищене приміщення для переговорів, в якому проводяться зустрічі, аналіз матеріалів, координуються дії з розслідування інцидентів ІБ.

Метою розслідування інциденту ІБ є розкриття всіх причинно-наслідкових зв'язків і отримання такої інформації:

- джерела інциденту ІБ (порушники);

- цілі інциденту ІБ (активи, репутація, ін.) І способи здійснення інциденту ІБ.

У разі інциденту ІБ політика безпеки ЗАБОРОНЯЄ повідомлення партнерів, засобів масової інформації, а також третіх осіб, які не беруть участі в бізнес процесах компанії.

Якщо в Компанії використовується **CMDB** і описана сервісно -ресурсний модель інформаційних систем, то можлива розробка комплексних сценаріїв виявлення інцидентів ІБ.(Концепція CMDB, пропонована ITIL і передбачає створення комплексного всеохоплюючого сховища інформації про IT-середовищі компанії. Інвентаризація всіх IT-активів компанії трудомістке і дороге заняття, але ще складніше підтримувати CMDB в актуальному стані цілими відділами).

Важливо! Необхідна прив'язка до реальних бізнес-процесів з метою мінімізації наслідків для основної діяльності компанії!

В єдиному **каталозі бази даних управління конфігураціями (Configuration Management Data Base - CMDB)** міститься інформація про всі IT-об'єктах компанії і зв'язки між ними, включаючи:

• Сервера і робочі станції;

• Всі периферійні пристрої та комплектуючі;

• Програмне забезпечення;

• IT-сервіси, а також сервіси одержувані з хмари;

• Мережеве обладнання;

• Принтери, сканери та інше обладнання.

Необхідно проводити регулярне **підвищення обізнаності персоналу в питаннях забезпечення ІБ і оповіщення про потенційні інциденти:**

- Розробка пам'ятки

- Проведення навчальних семінарів

- Тренінги (наприклад, у формі тестування на проникнення.

Практика

Звіт за результатами обробки інциденту може містити:

• Основні відомості

• інформацію про об'єкт інциденту

• інформацію про джерело інциденту

• опис хронології інциденту

• вжиті заходи по реагуванню

• рішення щодо інциденту

• інформацію про залучених осіб

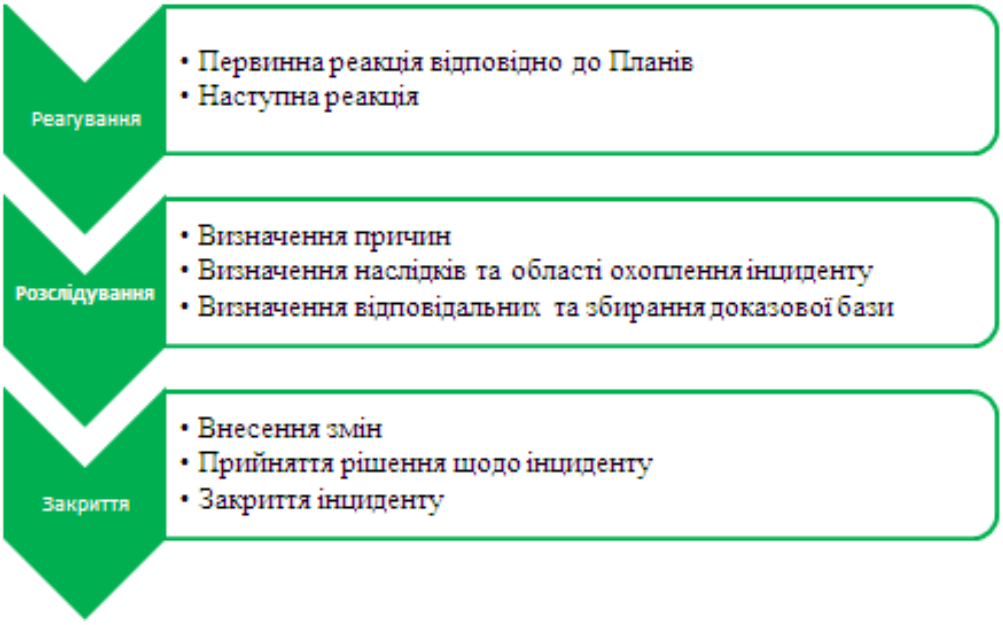


Рис.2.35. Обробка інцидентів

Ухвалення рішення про подальші дії щодо усунення інцидентів може бути реалізовано за наступним принципом алгоритму обробки інциденту (рис.2.36):

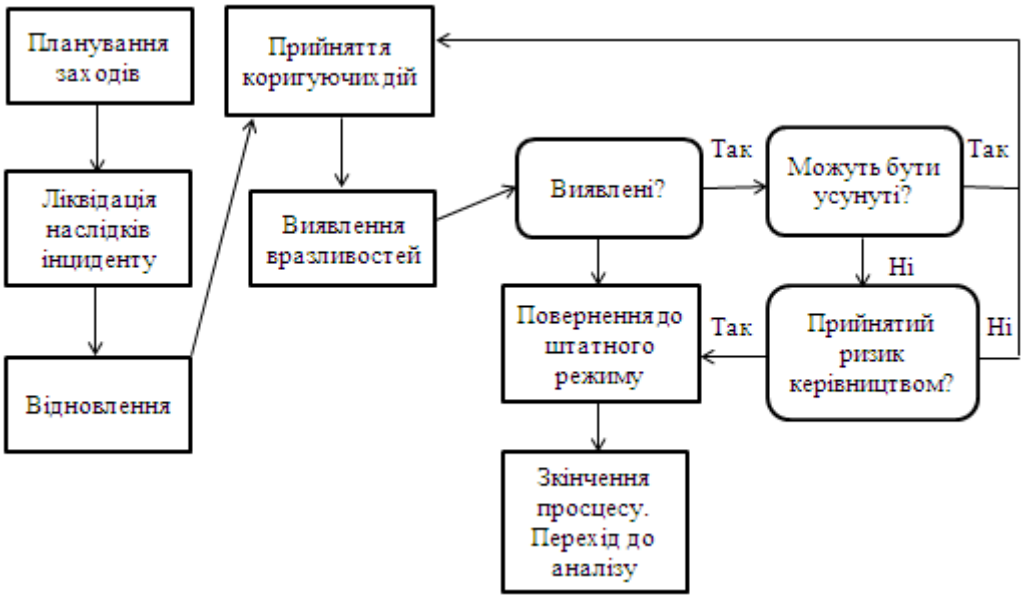


Рис.2.36. Алгоритм обробки інциденту

Приклад Плану реагування на інцидент (обробка інцидентів) певного типу: «Компрометація облікового запису».

Таблиця 2.5

Компрометація облікового запису

№	Етап	Вхід	Дії	Вихід	Відповідальний	Тер-мін
1	Виявлення	Інцидент ІБ	Інформування Адміністратора АС Адміністратора AD	-	Оператор системи моніторинга	5 хв
2	Блокування	Обліковий запис АС/AD	Блокування облікового запису	-	Адміністратора АС Адміністратора AD	
3	Розслідування	Журнали реєстрації подій ІБ	Виявлення фактів несанкціонованого використання облікового запису	Інформація про використан-ня облікового запису . Наслідки інциденту ІБ	Адміністратор АБС Адміністратор AD	
4	Створення нового облікового запису	-	Активація нового облікового запису (заміна пароля)		Адміністратора АС Адміністратора AD	

Примітка: АС-адміністратор сайтів; АД-адміністратор доменів.

Усунення причин, наслідків інциденту і його розслідування

Інструкція щодо усунення причин і наслідків інциденту включає опис загальних дій, які необхідно вжити (конкретні дії для кожного виду інциденту визначати занадто багато роботи і не завжди доцільно), а також терміни, протягом яких слід усунути наслідки і причини інциденту. Терміни усунення наслідків і причин інциденту залежать від рівня інциденту. Слід розробити класифікацію інцидентів - визначити кількість рівнів критичності інцидентів, описати інциденти кожного рівня і терміни їх усунення. Документ, який визначає, які події в компанії слід вважати інцидентом, також може описувати і рівні інцидентів.

Розслідування інциденту включає в себе визначення винних в його виникненні, збір доказів і доказів інциденту, визначення відповідних дисциплінарних стягнень. У великих компаніях, як правило, виділяють комісію з розслідування інцидентів інформаційної безпеки (до складу якої може входити співробітник, який реєструє інциденти).

Інструкція по розслідуванню інцидентів повинна описувати: дії з розслідування інциденту (в тому числі визначення винних в його виникненні), правила збору і зберігання доказів (особливо в разі, якщо може знадобитися використання доказів у судових органах) і правила внесення дисциплінарних стягнень.

Практика

Технічні заходи з розслідування інциденту

• Виявлення активних користувачів

• Виявлення підозрілих процесів

• Аналіз системних журналів

• Аналіз журналів мережевого обладнання

• Аналіз конфігурації системного програмного забезпечення, обладнання та мережевих адаптерів

• Пошук підозрілих файлів і інших слідів атаки (антивірусне сканування, контроль цілісності, контроль змін)

Ліквідація наслідків інциденту

• Планування відновлювальних робіт і розподіл обов'язків

• Антивірусні заходи

• Відновлення даних з резервних копій

• Зміна паролів на скомпрометовані системи

• Аналіз виявлених вразливостей і причин інциденту

• Ліквідація вразливостей, установка програмних корекцій

• Відтворення картини подій і документування інциденту

• Підготовка свідоцтв про порушення, залучення правоохоронних органів.

Практика

Розслідування інцидентів

З метою розвитку процесів розслідування інцидентів ІБ і формування доказової бази повинні бути виконані наступні основні дії:

1. Визначити і описати типи інцидентів (сценарії), що вимагають формування доказової бази.

2. Визначити доступні джерела і типи інформації, яка може використовуватися в якості доказової бази.

3. Визначити вимоги до збору доказів з цих джерел.

4. Організувати можливість для коректного (з юридичної точки зору) збору доказової бази відповідно до певних вимог.

5. Встановити політику зберігання і використання (обробки) потенційних доказів.

6. Забезпечити моніторинг подій, що вказують на інцидент ІБ

7. Визначити події, при настанні яких повинні бути запущені процеси збору доказової бази (вказано це в типових планах)

8. Описати все ролі в рамках даного процесу і провести необхідне навчання залучених працівників.

9. Описати основні плани реагування на інциденти, що вимагають збору доказової бази (юридично значимої).

10. Забезпечити правову експертизу.

Коригувальні та превентивні дії

Після усунення наслідків інциденту і відновлення нормального функціонування бізнес-процесів компанії, можливо, буде потрібно виконати дії щодо запобігання повторного виникнення інциденту. Для визначення необхідності реалізації таких дій слід провести аналіз ризиків, в рамках якого визначається доцільність коригувальних і запобіжних дій. У деяких випадках наслідки інциденту незначні в порівнянні з коригуючими і превентивними діями, і тоді доцільно не робити подальших кроків після усунення наслідків інциденту.

Процедури циклу управління інцидентами безпеки повинні безперервно і послідовно повторюватися - через певний час (як правило, через півроку або рік). Необхідно заново переглянути перелік подій, які називаються інцидентами, форму звіту та ін., впровадити оновлену процедуру в інформаційну систему, перевірити її функціонування і ефективність, реалізувати превентивні дії.

Оцінка ефективності процесу управління інцидентами ІБ

(Відповідно до метрик безпеки)

Після проведення розслідування інциденту ІБ проводиться аналіз причин і оцінка результату:

- переоцінка ризиків, що призвели до виникнення інциденту ІБ;
- підготовка переліку захисних заходів для мінімізації виявлених ризиків і в разі повторення інциденту ІБ;
- актуалізація необхідних політик, регламентів, правил ІБ;
- навчання персоналу (співробітників) компанії, для підвищення його обізнаності в частині ІБ.

Оцінка ефективності процесу управління інцидентами ІБ спрямована на коригування (вдосконалення):

• процесу управління інцидентами;
• реалізованих заходів забезпечення ІБ;
• підходу і результатів оцінки ризиків;
• області моніторингу та контролю;
• політики (підходів).

Оцінка ефективності (у вигляді показників) повинна бути спрямована на:

• загальні вимоги і підхід до управління інцидентами
• захист інформації (превентивні заходи)
• виявлення і обробку інцидентів
• прийняття рішень по інцидентах

2-й варіант РДСА процесів управління інцидентами

Рис.2.37. Етапи менеджменту (управління) інцидентів (ами) ІБ (варіант)

А. Планування і підготовка

Ефективний менеджмент інцидентів ІБ потребує належної плануванні та підготовці. Для забезпечення ефективності реакції на інциденти ІБ необхідно:

- Розробити і документувати політики менеджменту інцидентів ІБ. а також отримати очевидну підтримку цієї політики зацікавленими сторонами і, особливо, вищого керівництва;

- Розробити і в повному обсязі документувати систему менеджменту інцидентів ІБ для підтримки політики менеджменту інцидентів ІБ.

- Форми, процедури та інструменти підтримки виявлення, оповіщення, оцінки та реагування на інциденти ІБ, а також градації шкали серйозності інцидентів повинні бути відображені в документації на конкретну систему (в

деяких організаціях така система може називатися «Планом реагування на інциденти ІБ»);

- обновіть політики менеджменту ІБ і ризиків на всіх рівнях, тобто на корпоративному і для кожної системи, сервісу і мережі окремо з урахуванням системи менеджменту інцидентів ІБ.

Б. Використання системи менеджменту інцидентів інформаційної безпеки

При використанні системи менеджменту інцидентів ІБ необхідно здійснити наступні процеси:

- Виявлення і оповіщення про виникнення подій ІБ (людиною або автоматичними засобами);
- збір інформації, пов'язаної з подіями ІБ і оцінка цієї інформації з ланцюгом визначення, які події можна віднести до категорії інцидентів ІБ;
- реагування на інциденти ІБ: негайно, в реальному або майже реальному масштабі часу;
- якщо інциденти ІБ знаходяться під контролем, виконати менш термінові дії (наприклад, що сприяють повному відновленню після катастрофи):
- якщо інциденти ІБ не перебувають під контролем, то виконати «антикризові» дії (наприклад, викликати пожежну команду / підрозділ або ініціювати виконання плану безперервності бізнесу)

С. Аналіз

Після дозволу і закриття інцидентів ІБ необхідно зробити наступні дії з аналізу стану ІБ:

- Провести додаткову правову експертизу (при необхідності);
- -Вивчити уроки, витягнуті з інцидентів ІБ;
- визначити поліпшення для впровадження захисних заходів ІБ, отримані з уроків, витягнутих з одного або декількох інцидентів ІБ;
- визначити поліпшення для системи менеджменту інцидентів ІБ б ціпом, враховуючи уроки, витягнуті з результатів аналізу якості проведеного підходу

(наприклад, з аналізу результативності процесів, процедур, форм звіту і (або) організації.

Д. Поліпшення

Необхідно підкреслити, що процеси менеджменту інцидентів ІБ є ітеративними, з постійним внесенням поліпшень з плином часу в ряд елементів ІБ. Ці поліпшення пропонується на основі даних про інциденти ІБ і реагуванні на них. а також даних про динаміку тенденцій. Етап «Поліпшення» включає в себе:

-перегляд наявних результатів аналізу ризиків ІБ і аналіз менеджменту організації;

- Поліпшення системи менеджменту інцидентів ІБ і її документації;

- ініціювання поліпшень в області безпеки, включаючи впровадження нових і (або) оновлених захисних заходів ІБ.

Будь-яка організація, яка використовує **системно-структурний підхід до менеджменту інцидентів ІБ**, може витягти з нього значні переваги, які можна об'єднати в такі групи:

- поліпшення ІБ;

- зниження негативних впливів на бізнес, наприклад, переривання бізнесу і фінансові збитки як наслідки інцидентів ІБ;

- посилення уваги до питань запобігання інцидентів;

- посилення уваги до встановлення пріоритетів та збору доказів;

- обгрунтування бюджету і ресурсів;

- оновлення результатів менеджменту і аналізу ризиків;

- надання матеріалу для програм підвищення обізнаності та навчання в області ІБ;

- надання вхідних даних для аналізу політики ІБ і відповідної документації.

Основною метою забезпечення ІБ організації є зниження ризиків, які діють щодо інформаційних ресурсів, і в кінцевому рахунку запобігання або мінімізація шкоди від можливих інцидентів ІБ.

Для досягнення цієї мети в більшості великих і середніх компаній створені підрозділи ІБ, які планують і реалізують комплекс заходів щодо захисту своїх інформаційних ресурсів в складі СУІБ (рис.2.38 і 39).

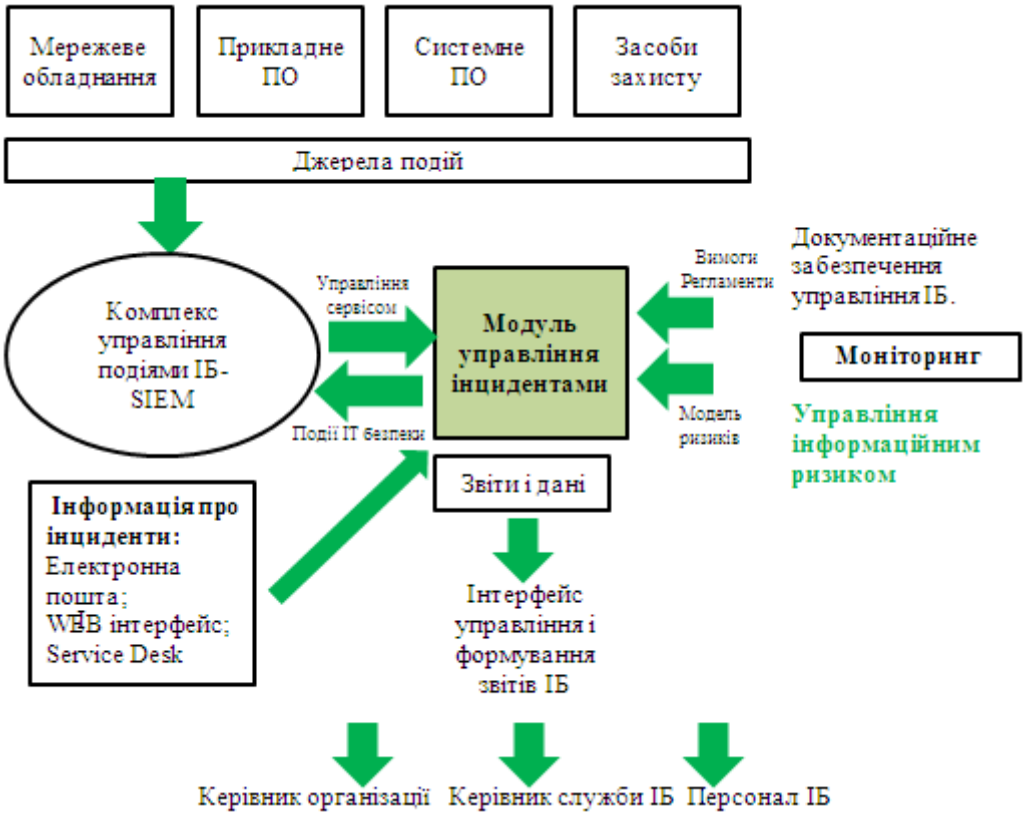


Рис.2.38. Місце модуля управління інцидентами (в складі СУІБ)

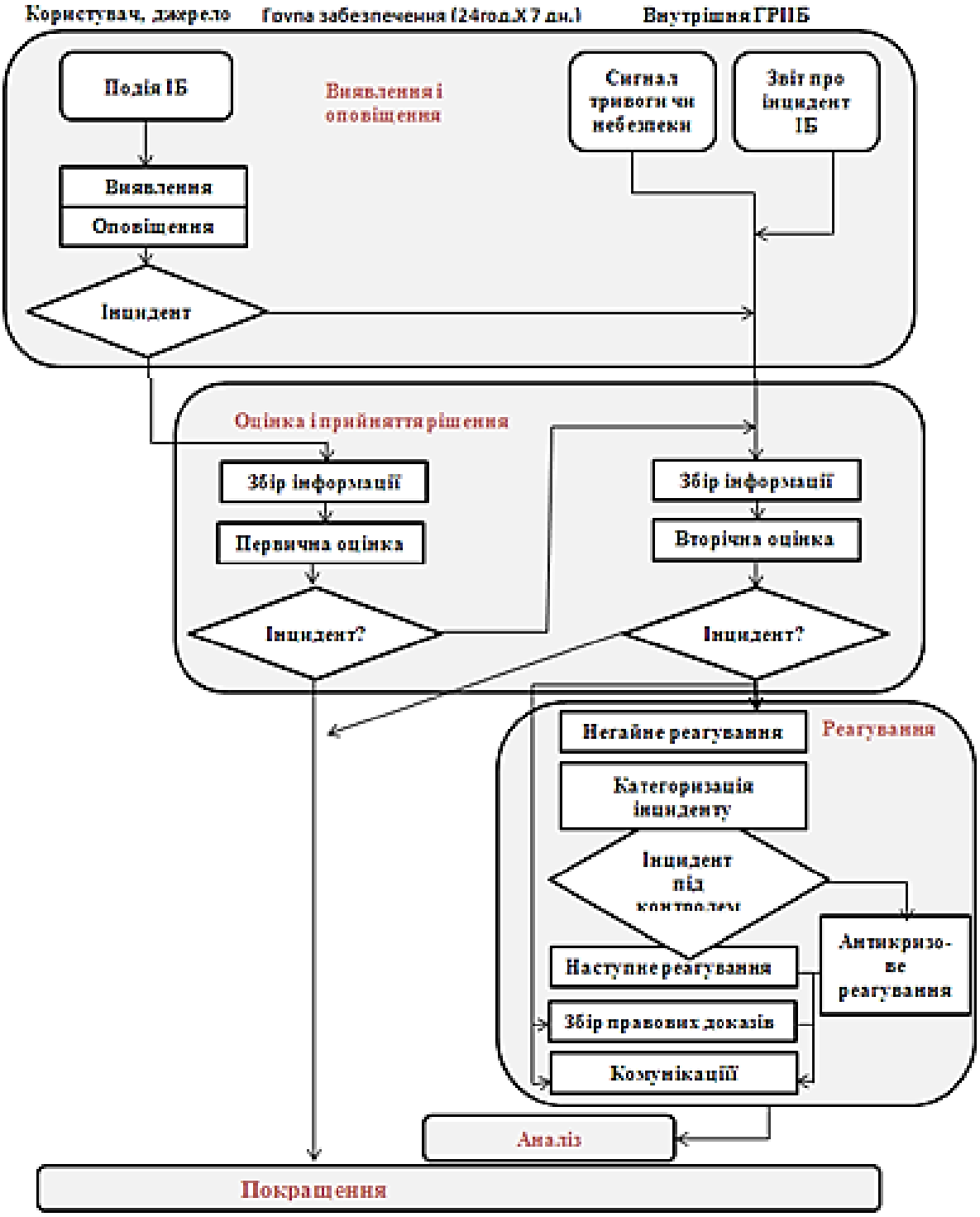


Рис.2.39. Алгоритм менеджменту інцидентів ІБ в процесі експлуатації

Архітектура системи управління інцидентами ІБ (реалізація системно - структурного методу побудови) представлена на рис.2.40.

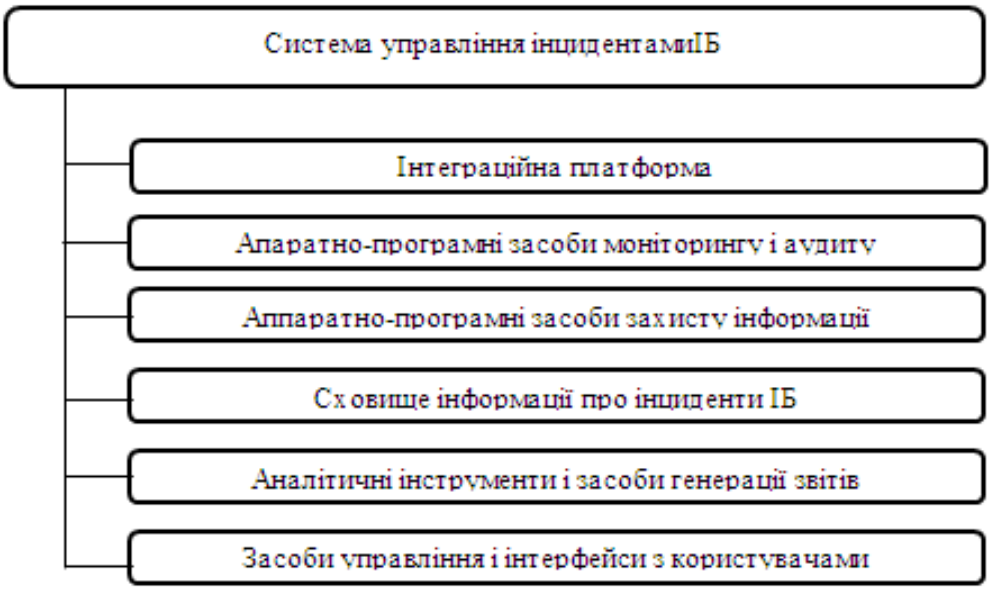


Рис. 2.40. Архітектура системи управління інцидентами ІБ.

Інтеграційна платформа є ядром системи. Вона реалізує функції по інтеграції та взаємодії всіх компонент, що складають систему. Інтеграційна платформа надає:

- інтерфейси для інтеграції засобів моніторингу та аудиту, забезпечуючи збір даних;

- інтерфейси до засобів захисту інформації для оперативного зміни їх конфігурації з метою локалізації наслідків інцидентів ІБ;

- інтерфейс до сховища даних;

- послуги з використання аналітичних функцій і засобів генерації звітів.

Основна мета інтеграційної платформи полягає в забезпеченні чіткої і оперативної координації і взаємодії осіб, які відповідають за реагування на події, пов'язані з комп'ютерними інцидентами.

Такими особами можуть бути:

- **користувачі** інформаційних систем організації - оповіщення про комп'ютерні інциденти;

-**адміністратори і персонал** підрозділів автоматизації -оповіщення, реагування, локалізація, розбір інцидентів і т. п .;

- **співробітники підрозділів безпеки** - реагування, контроль, координація дій по усуненню, розслідування причин, вироблення пропозицій щодо недопущення повторення інцидентів.

Апаратно-програмні засоби моніторингу та аудиту -засоби, що реалізують функції з протоколювання, збору, накопичення та обробки інформації про функціонування інформаційних систем організації. До таких засобів відносяться як **вбудовані** (штатні засоби операційних систем, додатків, мережевих пристроїв, засобів захисту та автоматизованих систем), так і **спеціалізовані засоби** (які розроблені за технічними завданнями підрозділу ІБ, а також спеціалізовані засоби аудиту: сканери безпеки, програмні агенти, сенсори, збирають інформацію та ін.). Результатом роботи всіх перерахованих засобів є дані, на основі яких системою автоматично або після їх аналізу експертом приймається рішення про настання комп'ютерного інциденту. Дані кошти складають підсистему збору інформації про комп'ютерні інциденти. На діяльності цієї підсистеми і заснований контроль за забезпеченням безпеки ІТ в організації.

Апаратно-програмні засоби захисту в контексті системи управління інцидентами ІБ –це засоби, які забезпечують локалізацію інцидентів або зниження шкоди. Ці засоби мають механізми, що дозволяють проводити швидке та дистанційне зміна своєї конфігурації або мати в своєму складі заздалегідь розроблені автоматизовані сценарії дій по мінімізації можливих збитків від комп'ютерних інцидентів.

Питання для самоконтролю

1. Що таке інцидент і наведіть приклади.
2. Які основні властивості інциденту ІБ ?
3. Наведіть логічний ланцюг появи інциденту інформаційної безпеки в СУІБ (у відповідності зі стандартом ISO/IEC 27035).

4. Приведіть варіант схеми системи менеджменту (управління) інцидентів(ами) ІБ (СУІБ) - у відповідності зі стандартом ISO/IEC 27035.

5. У чому полягає стратегія управління інцидентами інформаційної безпеки?

6. Які основні джерела прояви інцидентів ІБ?

7. Який алгоритм обробки інциденту?

8. Яка архітектура системи управління інцидентами ИБ?

9. Розкрийте місце модуля управління інцидентами (у складі СУІБ).

10. Приведіть алгоритм менеджменту інцидентів ІБ в організації.

2.6. Практика проходження перевірки СУІБ на відповідність вимогам стандартів ISO

Безпека даних забезпечується комплексом технічних засобів і організаційних заходів. Серед них - впровадження, експлуатація, оцінка ефективності і вдосконалення системи управління (менеджменту) інформаційної безпеки (СУІБ), яка дозволяє контролювати і мінімізувати ризики в області захисту інформаційних активів. Стандарт ISO 27001 містить в собі загальні принципи і кращу практику впровадження, забезпечення і оптимізації управління інформаційною безпекою на всіх етапах життєвого циклу інформаційних систем організації.

З точки зору процесів управління СУІБ входить в загальну систему менеджменту організації і надає додаткові механізми управління в частині забезпечення захисту інформації.

Для успішного функціонування і виконання завдань СУІБ повинна відповідати вимогам нормативно-методичних документів і, перш за все, стандарту ISO / IEC 27001. Ступінь відповідності цих вимог можна визначити тільки за результатом проведення аудиту ІБ організації. Саме аудит допомагає виявити області, які потребують удосконалення. Існують фірми, що надають послуги по проведенню аудиту - за допомогою експертів провести оцінку

безпеки на якісному рівні. При цьому необхідно, щоб цю оцінку визнавали і інші фірми - перш за все, партнери.

2.6.1. Організація аудиту на відповідність СУІБ вимогам стандартів ISO

Причини проведення аудиту на відповідність стандартам ІБ можна умовно розділити за ступенем обов'язковості даної послуги по відношенню до компанії:

- обов'язкова сертифікація;
- сертифікація, викликана «зовнішніми» об'єктивними причинами;
- сертифікація, яка дає змогу отримати вигоди в довгостроковій перспективі;
- добровільна сертифікація.

При проведенні даного виду аудиту стан інформаційної безпеки порівнюється з якимсь абстрактним описом, що приводиться в стандартах.

Результатом аудиту повинен стати перелік невідповідностей вимогам стандарту і план робіт зі створенням чи удосконаленням СУІБ організації.

Вимоги стандарту ISO 27001 дозволяють організувати оцінку інформаційної безпеки. Цей процес оцінки настільки формалізований, що вже існує програмне забезпечення, за допомогою якого можна самостійно організації теж виконати оцінку інформаційної безпеки. Саме програмне забезпечення в даний час вже дозволяє пов'язувати в єдиний процес процедури первинного збору інформації про підприємство, аналізу фактичного рівня організаційного забезпечення інформаційної безпеки, розробки документації, адаптації методів управління до певних вимог і підходи щодо проведення аудитів інформаційної безпеки. **Як програмні засоби перевірки СУІБ на відповідність вимогам ISO 27001** на практиці використовуються програми - британський програмний комплекс Cobra і російський КОНДОР+. **Для цілей сертифікації СУІБ на відповідність стандарту ISO 27001 використовують методику проведення сертифікаційного аудиту.** При цьому поняття інформаційна безпека визначається як система заходів, які повинні забезпечувати захист

інформації та інформаційних технологій – забезпечувати їх конфіденційність, цілісність і доступність (рис.2.41 і 2.42). В той же час стандарт ISO 27001 є основним керівництвом по створенню СУІБ, а самі засоби управління ІБ детально описані в стандарті ISO 27002. Стандарт ISO 27002 регламентує те, «що необхідно робити» (представляє перелік засобів управління), а стандарт ISO 27001 визначає «як робити» (визначає процедури створення і підтримки СУІБ).

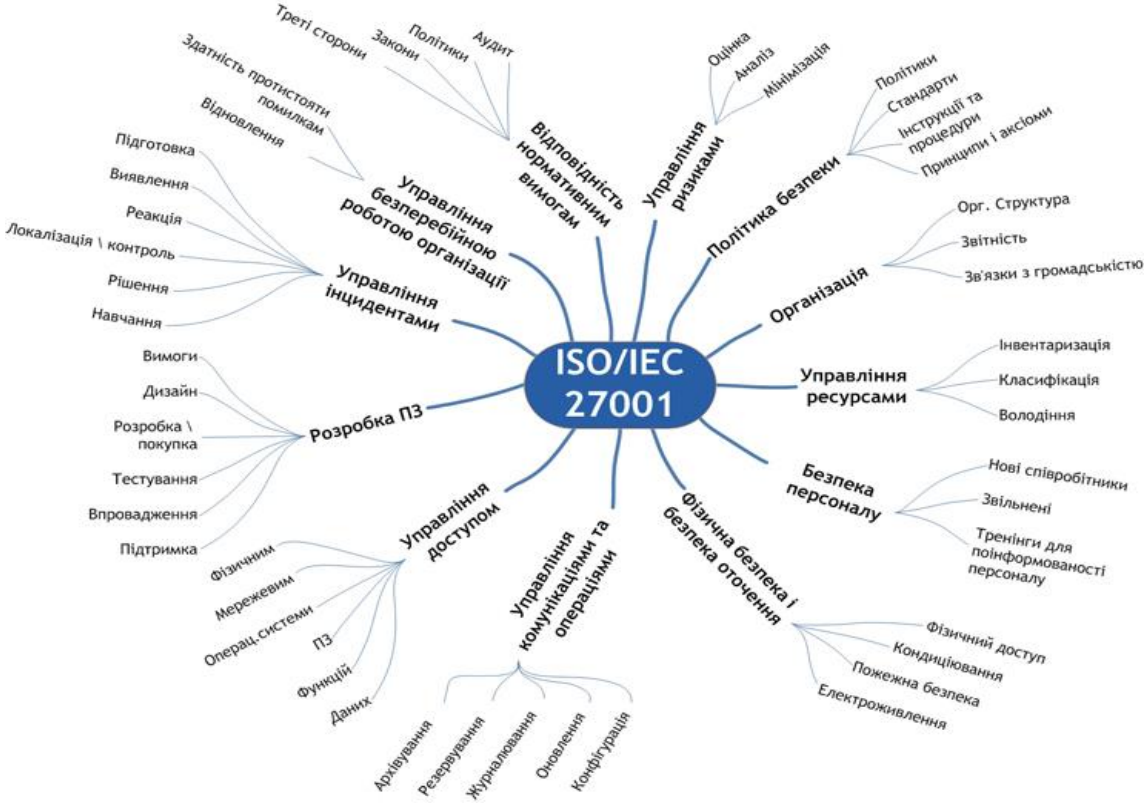


Рис. 2.41. Схема функцій і задач, визначених у стандарті ISO 27001

Сертифікація на відповідність стандарту ISO 27002 не проводиться, в той же час механізми проведення загального аудиту організації присутні і в ньому (рис. 2.42).

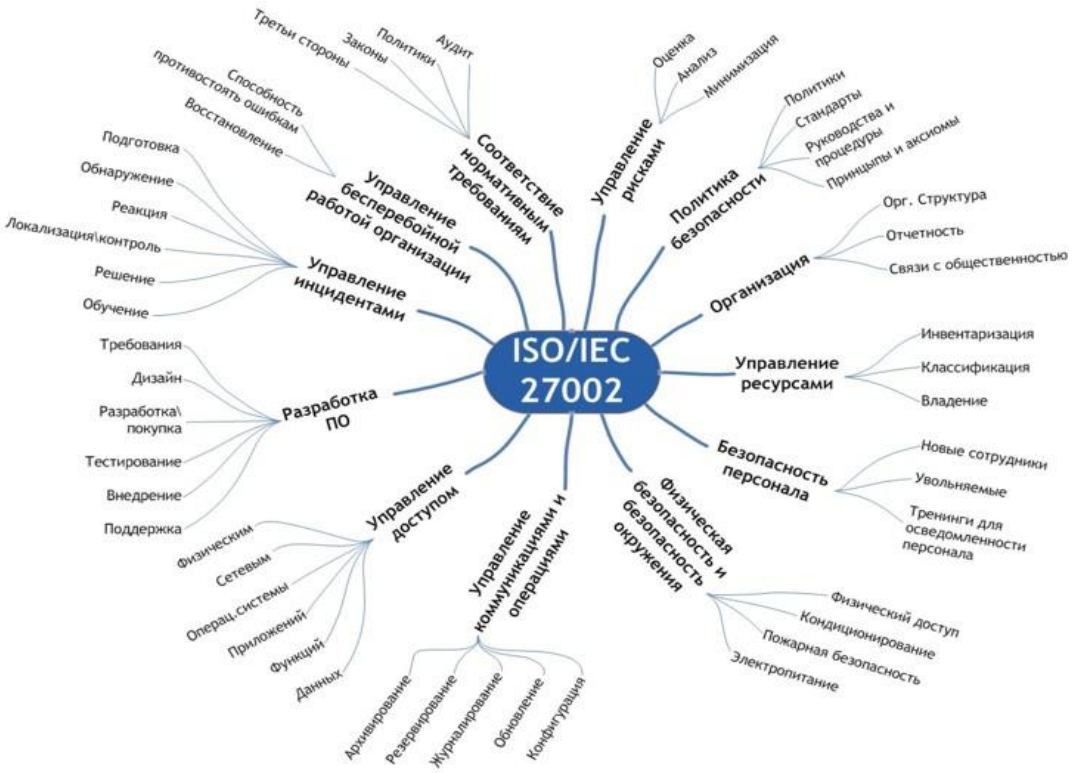


Рис. 2.42. Схема функцій і задач, визначених у стандарті ISO 27002

Аудит на відповідність СУІБ вимогам стандартів ISO може знадобитися організації в наступних випадках:

- Якщо організація вирішила впровадити СУІБ. У цьому випадку проведення аудиту допоможе коректно вибрати область дії, скоротивши тим Самим витрати НЕ реалізацію СУІБ. Так само за результатами робіт покаже, в яких областях в організації необхідно буде вживати заходів щодо підвищення рівня інформаційної безпеки.
- Якщо організація проводила реалізацію СУІБ самостійно, то незалежна оцінка відповідності допоможе організації, при необхідності, внести потрібні корективи в СУІБ.
- Якщо організація проводила реалізацію СУІБ самостійно і планує отримання сертифіката на СУІБ. У цьому випадку перед проведенням сертифікаційного аудиту, можливе проведення так званого аудиту, Який допоможе усунути критичні і некритичні недоліки СУІБ (при їх наявності).

• Якщо в організації вже діє СУІБ, то організація може для проведення необхідних періодичних аудитів звертатися до зовнішніх організацій.

Аудит на відповідність міжнародному стандарту з інформаційної безпеки ISO 27001 (раніше - ISO 17799: 2005) повинен також **проводиться під час другого етапу спільного аудиту безпеки організації** (рис.2.43). Аудит на відповідність стандартам найчастіше має на увазі **проведення активного і експертного аудиту.**

Рис.2.43. Місце сертифікаційного аудиту СУІБ

Стандарт ISO 27001 є переліком вимог, обов'язкових для сертифікації, в додатку ISO 27001 наведено перелік основних вимог, що перевіряються при сертифікації. Тому **ISO 27001 є стандартом, за яким проводиться офіційна сертифікація системи менеджменту інформаційної безпеки СУІБ (СМІБ)**.

Сертифікація на відповідність вимогам стандарту ISO 27001 є підтвердженням того, що в організації добре побудована СУІБ, приділяється належна увага управління ризиками, пов'язаними з інформацією та інформаційними технологіями.

Сертифікат відповідності ISO 27001 - офіційний документ, який підтверджує, що в компанії впроваджена СУІБ, вона забезпечує високий

рівень захисту конфіденційної інформації та управління ризиками, пов'язаними з витоком такої інформації.

Загальний аудит системи менеджменту інформаційної безпеки, як правило, включає в себе:

- аудит архітектури системи (організація системи,яка втілена в її елементах, їх взаємини один з одним і з середовищем),
- тестування програм фільтрації спаму, захисту від троянів,
- аудит внутрішньої безпеки (загрози, які виходять від працівників, віддалених працівників, відвідувачів),
- аудит забезпечення безпеки при доступі до системи і управління правами доступу,
- аудит центрів архівування та системи архівації даних,
- аудит планування готовності до надзвичайних ситуацій та аварійного відновлення,
- тест на проникнення (внутрішнього, зовнішнього) з метою перевірки системи захисту.

В перелік документів на сертифікацію СМІБ входять:

- Керівництво з інформаційної безпеки (або інший документ, що встановлює управління інформаційною безпекою).
- Політика інформаційної безпеки (якщо вона виконана у вигляді окремого документа і не включена в Керівництво з управління інформаційною безпекою).
- Область функціонування систем менеджменту інформаційної безпеки (СМІБ) (якщо вона виконана у вигляді окремого документа і не включена в Керівництво з управління інформаційною безпекою).
- Процедури і заходи управління, які підтримують СМІБ.
- Методологія оцінки і критерії прийняття ризиків.
- Організаційна структура організації, яка перевіряється.
- Структура служби, яка відповідає за інформаційну безпеку в організації (якщо вона не включена в загальну організаційну структуру).

- Задокументовані методики щодо управління документацією та записами, вимірювання, аналізу і поліпшення.
- Звіт з оцінки ризиків План обробки ризиків.
- Записи за результатами внутрішніх аудитів системи менеджменту інформаційної безпеки (СМІБ).
- Протокол аналізу функціонування системи менеджменту інформаційної безпеки, з боку керівництва.

Аудит СУІБ дає об'єктивну оцінку її поточного стану, визначає рівень відповідності ІС заданим критеріям і стандартам. Аудит дозволяє оцінити існуючий рівень захищеності ІС і вплив інформаційних ризиків на бізнес (планування та прийняття рішень).

Регулярне проведення аудиту СУІБ необхідно, тому що негативні наслідки проломів в функціонуванні ІС можуть привести до серйозних подій, починаючи від фінансових втрат, втрати довіри з боку клієнтів і партнерів і закінчуючи втратою ліцензії або повною зупинкою діяльності бізнесу.

Аудит СУІБ дасть можливість вирішити безліч проблем і відповісти на питання щодо функціонування ІС організації (організація служби ІБ, рекомендації з розробки політики інформаційної безпеки).

Проведення аудиту та подальше впровадження стандарту **дозволить вирішити цілу групу проблем, пов'язаних як з поточною роботою, так і з подальшим розвитком** підприємства:

- прихованість інвестицій в ІТ, відсутність економічних показників роботи підрозділів ІТ організації;
- неадекватний захист інформації (ресурси кинуті на захист інформації, що не представляє реальної цінності організації, в той час, як справді цінна інформація не захищена адекватно);
- фінансові та репутаційні втрати внаслідок слабкої організації ІБ підприємства;
- постійні штрафні санкції з боку регуляторів;
- придбання, розробка та обслуговування інформаційних систем;

• відсутність об'єктивної інформації про стан інформаційної системи для вірного прийняття рішень.

Роботи по проведенню оцінки відповідності проводяться, як правило, в один етап і полягають в наступному:

• Проводиться **вступна нарада** за участю представників Замовника і Компанії з метою визначення складу і порядку проведення робіт. Основне завдання наради полягає у визначенні регламенту проведення робіт.

• Проводиться **документальний аудит**. При цьому здійснюється збір документів і документальних свідчень, які можуть бути джерелами для оцінки відповідності СУІБ. Перелік цих документів формується при проведенні наради. За результатами аналізу наданої документації та за погодженням із Замовником розробляється «План проведення аудиту на місці» і визначається область дії СУІБ (якщо вона не визначена).

• Проводиться оцінка на місці. Дані роботи включають в себе оцінювання - оцінку виконання основних вимог стандарту ISO / IEC 27000 (Додатки А).

• Формуються звітні матеріали. При цьому здійснюється:

- розробка звіту про обстеженні;

- розробка рекомендацій щодо усунення виявлених невідповідностей та підвищення рівня відповідності вимогам стандарту.

2.6.2. Особливості проведення ресертифікаційного видів аудиту

Проведення ресертифікаційного аудиту за міжнародними стандартами ISO здійснюється через три роки з дати оформлення сертифіката відповідності системи менеджменту.

Ресертифікаційний аудит за процедурою проведення **схожий з сертифікаційним аудитом**, так як через три роки система менеджменту підприємства може сильно змінитися у зв'язку приходом нових людей, розвитку нових проектів і відділів, розширенню бізнесу підприємства в інші галузі або

регіони, а отже потрібно провести повний аудит системи менеджменту для оцінки відповідності системи менеджменту вимогам стандартів.

Ресертифікаційний аудит покликаний підтвердити, що вся система менеджменту як єдине ціле зберігає своє відповідність і результативність, залишаючись актуальною і застосовується до області сертифікації.

Ресертифікаційний аудит покликаний розглянути роботу системи менеджменту на протязі періоду сертифікації, включаючи аналіз звітів попередніх йому наглядових аудитів.

Ресертифікаційний аудит проводиться в кінці терміну дії сертифіката, на третій рік. **Сертифікувати систему відповідно до ISO 27001 необхідно**:

1. Для участі в тендерах, закупівлі.

2. Щоб отримати доступ до державної таємниці.

3. Для роботи з державними організаціями.

4. Роботи з серйозними структурами і холдингами (+ входження в їх склад).

5. Для виходу на міжнародний ринок.

6. Обов'язково при експорті продукції.

Заходи щодо вдосконалення СУІБ і ресертифікації за стандартом ISO / IEC 27001 проводяться в три етапи:

- обстеження поточного стану СУІБ;

- вдосконалення СУІБ;

- ресертифікаційний аудит СУІБ.

На етапі 1. Обстеження поточного стану СУІБ виконується:

• збір відомостей про бізнес-процесах Замовника (підприємства), на захист яких спрямована СУІБ;

• аналіз діючої у підприємства документації в сфері ІБ;

• ідентифікація типів захищаються активів, що входять в зону дії СУІБ;

• визначення зовнішнього і внутрішнього контексту організації;

• визначення зацікавлених зовнішніх і внутрішніх сторін, які мають відношення до СУІБ, і їх вимог;

• збір відомостей про областях ІБ і ІТ;

• виявлення слабких місць СУІБ;

• оцінка відповідності СУІБ вимогам Стандарту;

• розробка рекомендацій щодо усунення виявлених невідповідностей Стандарту і слабких місць СУІБ

Збір відомостей про наступні області ІБ і ІТ включає :

- політика та цілі СУІБ;

- організація діяльності в області ІТ та ІБ;

- управління документацією та записами СУІБ;

- процес оцінки ризиків;

- заяву про застосування, план обробки ризиків, процес обробки ризиків;

- свідоцтва компетенцій;

- методологія вимірювання результативності СУІБ;

- документована інформація зовнішнього походження;

- результати оцінки ризиків;

- результати обробки ризиків;

- прихильність і залученість керівництва підприємства, забезпечення ресурсами;

- бюджетування та облік витрат для роботи ІТ-сервісів;

- аналіз СУІБ з боку керівництва підприємства і Результати аналізу з боку керівництва;

- програма аудитів, плани аудитів, звіти про аудити;

- плани коригувальних дій і результати їх виконання;

- результати моніторингу процесів СУІБ;

- компетенції, навчання і підвищення обізнаності працівників в області ІТ та ІБ;

- управління рівнем ІТ-сервісу і звітність з надання ІТ сервісів

- управління взаємодією зі споживачами і постачальниками;

- управління активами;

- питання безпеки, пов'язані з персоналом;

- фізична безпека, безпека «навколишнього середовища» та обладнання;

- контроль і управління доступом;

- придбання і прийняття інформаційних систем;

- планування та впровадження нових або змінених ІТ-сервісів;

- безпеку ІБ- інфраструктури;

- забезпечення захисту каналів зв'язку;

- управління потужностями;

- управління конфігураціями;

- управління змінами;

- управління мобільними пристроями;

- забезпечення антивірусного захисту;

- здійснення резервного копіювання;

- управління безперервністю і доступністю ІБ - сервісів і залежних від них ІТ-сервісів;

- управління інцидентами і проблемами ІБ; - моніторинг подій ІБ;

- виявлення і реєстрація інцидентів ІБ, реагування і витяг уроків з інцидентів ІБ;

- забезпечення безпеки при взаємодії з третіми сторонами;

- відповідність вимогам законодавства у сфері захисту інформації.

За результатами першого етапу повинні бути відпрацьовані наступні **документи:**

• **«Звіт про обстеження поточного стану СУІБ»**, що містить:

- оцінку виконання вимог Стандарту;

- опис виявлених невідповідностей вимогам Стандарту;

- опис виявлених слабких місць СУІБ;

- рекомендації щодо виправлення виявлених невідповідностей і слабких місць СУІБ;

- план реалізації рекомендацій щодо усунення виявлених невідповідностей вимогам Стандарту;

- дорожня карта розвитку ІБ на 2019-2022 роки.

• **«Область дії системи управління інформаційною безпекою»**.

- документальне фіксування області дії системи управління інформаційною безпекою;

- реєстрація відповідностей вимогам ресертифікаційного аудиту.

На другому етапі Удосконалення виконуються:

- Розробка та (або) актуалізація комплекту документів, що регламентує процеси управління ІБ, перелік яких визначається відповідно до вимог Стандарту;

- доопрацювання політики управління активами підприємства;

- проведення інвентаризації активів і складання реєстру активів відповідно до раніше доопрацьованій і узгодженої з підприємством політикою управління активами;

- доопрацювання діючої на підприємстві методики оцінки ризиків ІБ. Для визначення ймовірності настання ризику ІБ і тяжкості наслідків від його реалізації повинні використовуватися інформативні шкали, що забезпечують порівняльні та відтворювані результати оцінки ризиків;

- проведення оцінки ризиків ІБ відповідно до раніше доопрацьованій і узгодженої з підприємством методикою оцінки ризиків ІБ;

- розробка захисних заходів, що забезпечують мінімізацію виявлених раніше ризиків ІБ до рівня, узгодженого з підприємством;

- актуалізація Процесу безперервності бізнесу і відновлення після збоїв для процесів ІБ;

- консультації працівників підприємства з питань виконання вимог Стандарту, щодо необхідних змін СУІБ, щодо виконання виданих рекомендацій, по проходженню процедури ресертифікації, по процесам управління і забезпечення ІБ (управління змінами, інцидентами ІБ ...; перевірка результатів надання послуг щодо усунення невідповідностей вимогам Стандарту;

- навчання і підвищення обізнаності персоналу Замовника в області ІБ;

- проведення передсертифікаційного аудиту СУІБ;

- підготовка матеріалів і супровід аналізу поліпшеною СУІБ керівництвом Замовника;

- вимір ефективності СУІБ на основі розроблених / доопрацьованих метрик.

За результатами другого етапу повинні бути розроблені і доопрацьовані наступні **документи**:

• комплект документів, що регламентують процеси управління ІБ, відповідно до вимог Стандарту;

• «реєстр активів в області дії СУІБ» з позначенням відповідальних за активи з боку Бізнесу та ІТ супровід;

• «Звіт про оцінку ризиків інформаційної безпеки в області дії СУІБ»;

• план обробки ризиків ІБ, і проведено схвалення плану від власників ризику і підтвердження прийняття остаточних ризиків ІБ:

• «заяву про застосування контролів інформаційної безпеки»;

• комплект проектів, актуалізованих розроблених внутрішніх нормативних і організаційно-розпорядчих документів щодо реалізації організаційних заходів, що забезпечують мінімізацію ризиків ІБ і / або усунення виявлених невідповідностей вимогам Стандарту;

• звіти про оцінку результатів впровадження змін в діючих процесах ІБ;

• записи за результатами впровадження змін в процеси управління і забезпечення ІБ:

• матрицю ролей в рамках кожного процесу управління і забезпечення ІБ з переліком функцій і повноважень для кожної ідентифікованої ролі кожного процесу ІБ;

• накази про закріплення відповідальності за процеси управління і забезпечення ІБ.

М**етодики проведення внутрішнього аудиту за процесами управління і забезпечення ІБ повинні включати**:

- цілі, завдання, принципи і критерії перевірки процесу ІБ в рамках внутрішнього аудиту;

- методи і техніки збору інформації в рамках проведення аудиту;

- чек-листи для збору інформації в рамках аудиту;

- методи інтерпретації та аналізу зібраної інформації.

Документація по процесам безперервності і відновлення після збоїв інфраструктури ІБ хмарної платформи (ХП):

- актуальна карта ІБ-сервісів з прив'язкою до ІТ-ресурсів;
- актуальна логічна і фізична схеми поточної інфраструктури для ІБ-сервісів;
- прийнятні (узгодженими з власниками) показники RPO і RTO для резервуються ІБ-сервісів;
- технічне завдання на актуалізовану систему резервування ІБ-сервісів;
- проект на актуалізовану систему резервування ІБ-сервісів ХП;
- категорування типових інцидентів за рівнями критичності ІБ;
- процедура реагування на інциденти ІБ в ХП;
- схема взаємодії ІТ та ІБ в надзвичайній ситуації;
- список постачальників ІБ і ІТ-послуг в СУІБ;
- детальний план дій в режимі нормального функціонування для ІБ сервісів;
- детальний план дій в режимі надзвичайних ситуацій для ІБ сервісів;
- детальний план дій в режимі відновлення після надзвичайної ситуації для кожного ІБ Сервісу;
- планування тестових випробувань.

Етап 3. Супровід при ресертифікаційному аудиті СУІБ.

В рамках даного етапу повинна бути надана **консультаційна підтримка працівників підприємства з питань проходження ресертифікаційного аудиту і щодо усунення невідповідностей, виявлених в ході ресертифікаційного аудиту СУІБ**.

За результатами послуг третього етапу: виконавцем повинен бути розроблений Звіт за результатами ресертифікаційного аудиту, в якому будуть описані результати проведеного аудиту.

Вимоги до документування:

1. Звітні документи повинні подаватися на паперовому носії та в електронному вигляді на машинних носіях.

2. Електронні документи, що подаються на машинних носіях, повинні бути в форматі редакторів Microsoft Word, Microsoft Visio (DOC, VSD).

2.6.3. Практика проходження перевірки за допомогою програми Кондор+

У стандарті ISO / IEC 27001 містяться до 150 вимог до ІБ організацій. З них 132 пункту є обов'язковими до виконання. Ці вимоги передбачають області ІБ, представлені на рис.2.44, першої і найбільш важливою є **ПОЛІТИКА БЕЗПЕКИ**.

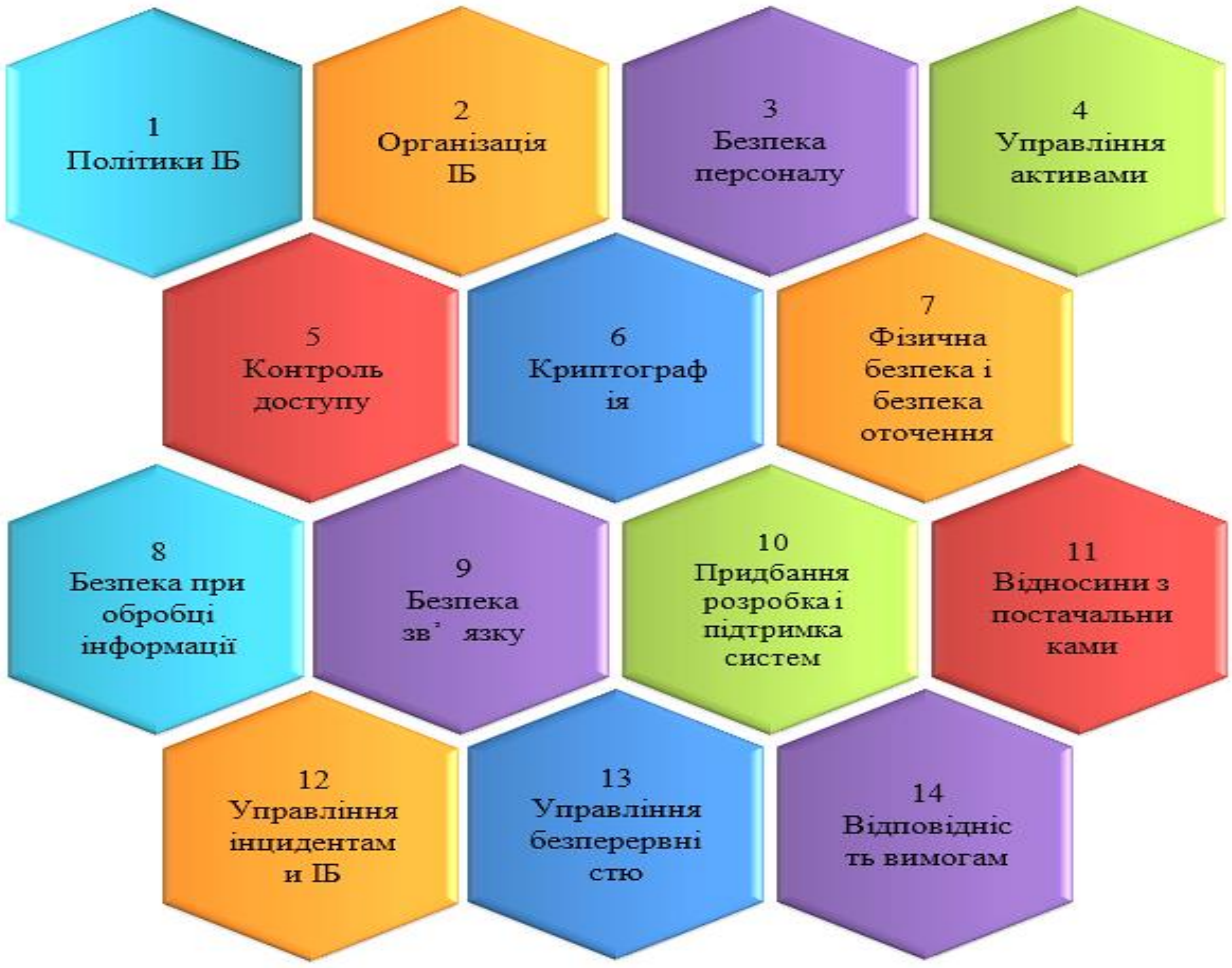


Рис.2.44. Області інформаційної безпеки

Програмний продукт КОНДОР + призначений для перевірки відповідності політики інформаційної безпеки компанії вимогам стандартів ISO 27001.

КОНДОР + включає в себе більше двохсот питань, відповівши на які, фахівець отримує звіт про стан політики безпеки, а також модуль оцінки рівня ризиків відповідності вимогам стандартів ISO. Основні модулі Програмного комплексу КОНДОР + показані на рис. 2.45.

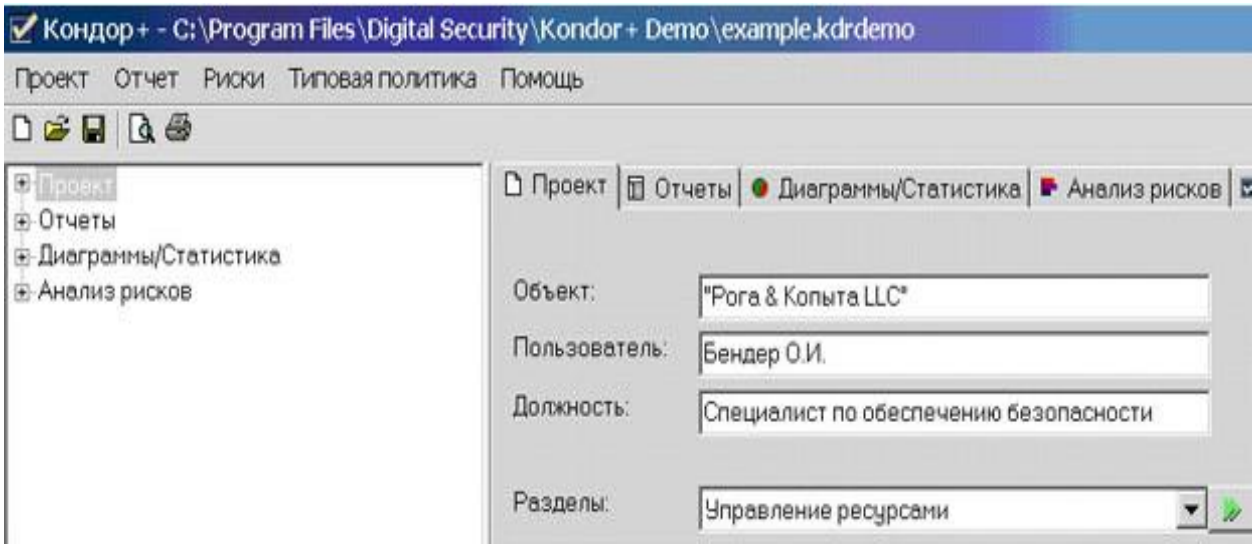


Рис.2.45. Головне вікно програми КОНДОР +

Після реєстрації користувач (відповідальний менеджер) отримує можливість вибрати відповідний розділ стандарту і повинен відповісти на питання, згруповані відповідно до його структури (по розділах стандарту ISO 27001) і які мають певні варіанти відповідей.

У звіті (рис.2.46) відображаються всі положення політики безпеки (ПБ) організації, які відповідають і не відповідають стандарту, а також відображається існуючий рівень ризику невиконання вимог ПБ.

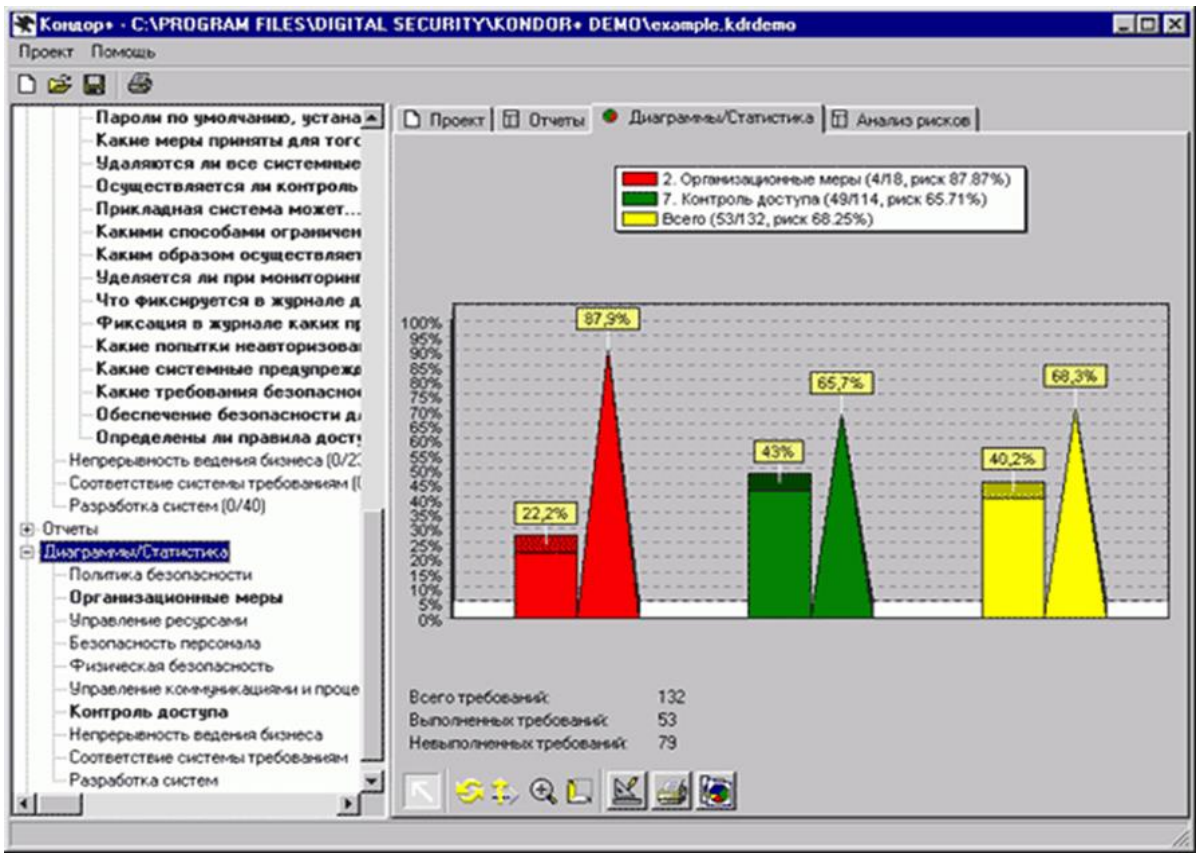


Рис.2.46. Положення політики безпеки організації - в звіті

До найбільш важливих елементів ПБ звіту даються коментарі та рекомендації експертів у вигляді опису окремих невідповідностей - в модулі "Звіти" - користувач має можливість за допомогою довідкової підсистеми звернутися додатково до коментарів і рекомендацій експертів, що описує окремі питання практичного застосування стандарту ISO.

Крім того, КОНДОР + дає можливість фахівцеві відстежувати вносяться на основі виданих рекомендацій зміни в ПБ, поступово приводячи її в повну відповідність з вимогами стандарту.

Таким чином, програмний комплекс "Кондор +" з модулем аналізу ризиків базового рівня дозволяє провести весь комплекс робіт по збору відомостей про стан ІБ і організації захисних заходів на підприємстві, порівняно фактичного стану справ з вимогами стандартів ISO (як укрупнено, так і детально) та визначенню пріоритетних напрямків подальшого розвитку СУІБ.

До недоліків КОНДОР + можна віднести:

• відсутність можливості установки користувачем ваги на кожну вимогу;

• відсутність можливості внесення користувачем коментарів.

Питання для самоконтролю

1.Що таке аудит?

2. Які функції й завдання по організації керування ИБ позначені в стандартах ISO 27001 і 27002?

3. Які основні програмні продукти використовуються як програмні засоби перевірки СУИБ на відповідність вимогам ISO 27001?

4. Покажіть місце сертифікаційного аудита СУИБ (на відповідність стандарту ISO 27001) у послідовності проведення загального аудита безпеки організації.

5. Що таке сертифікат відповідності ISO 27001?

6. Які роботи проводяться при оцінці відповідності ISO 27001?

7. Які проводяться заходи щодо вдосконалювання СУИБ і ресертифікації у відповідності зі стандартом ISO/IEC 27001?

8. У чому особливість проходження перевірки відповідності ISO 27001 за допомогою програми КОНДОР+?

ТЕМА 3. Застосування методів в системному аналізі інформаційної безпеки

3.1. Системний аналіз інформаційних систем

Застосування методів системного аналізу до дослідження проблеми захисту інформації (ЗІ) диктується вимогами практики, яка поставила фахівців перед необхідністю:

- проектувати складні системи захисту інформації,
- вивчати протікають в них процеси,
- управляти ними в умовах невизначеності, неповноти інформації, дефіциту часу і обмеженості ресурсів.

Специфічною особливістю розглянутих в літературі методик системного аналізу є те, що вони використовують закономірності побудови, функціонування і розвитку систем, формування варіантів структури системи і вибір найкращого варіанту.

Методи системного аналізу - це декомпозиція, аналіз і синтез системи, що знімає або послаблює проблему практики. Будь-яке системне дослідження пов'язане з різними альтернативами розвитку системи. Завдання системних аналітиків вибрати і обгрунтувати найкращу альтернативу розвитку. На етапі вироблення і прийняття рішень необхідно враховувати взаємодію системи з її підсистемами, поєднувати цілі системи з цілями її підсистем, виділяти глобальні і другорядні цілі.

3.1.1. Характеристика задач системного аналізу

Лідируюча роль системного аналізу обумовлена тим, що розвиток науки призвело до постановки тих завдань, які покликаний вирішувати саме системний аналіз.

Особливість поточного етапу полягає в тому, що системний аналіз, ще не встигнувши сформуватися в повноцінну наукову дисципліну, змушений

існувати і розвиватися в умовах, коли суспільство починає відчувати потребу в застосуванні ще недостатньо розроблених і апробованих методів і результатів і не в змозі відкласти вирішення пов'язаних з ними завдань на завтра.

У цьому джерело як сили, так і слабкості системного аналізу:

- постійно відчуває вплив потреби практики, змушений безперервно розширювати коло об'єктів дослідження і не має можливості абстрагуватися від реальних потреб суспільства;

- нерідко застосування «сирих», недостатньо опрацьованих методів системних досліджень веде до прийняття скоростиглих неефективних рішень.

Основні завдання, на вирішення яких спрямовані зусилля фахівців і які потребують подальшої розробки. По-перше, це завдання дослідження системи взаємодій аналізованих об'єктів з навколишнім середовищем. Рішення завдання передбачає:

• проведення кордону між досліджуваної системою і навколишнім середовищем;

• визначення реальних ресурсів такої взаємодії;

• розгляд взаємодій досліджуваної системи з системою більш високого рівня.

Завдання, пов'язані з конструюванням альтернатив взаємодії аналізованих об'єктів - альтернатив розвитку системи в часі і в просторі. Важливий напрямок розвитку методів системного аналізу пов'язано зі спробами створення нових можливостей конструювання оригінальних альтернативних рішень, несподіваних стратегій, незвичних уявлень і прихованих структур. Розробкою методів і засобів посилення індуктивних можливостей людського мислення. Дослідження в цьому напрямку розпочато лише зовсім недавно, і єдиний концептуальний апарат в них поки відсутній. Проте, і тут можна виділити **кілька важливих напрямків** ,таких, як:

- розробка формального апарату індуктивної логіки,

- розробка методів морфологічного аналізу та інших структурно-синтаксичних методів конструювання нових альтернатив,

- розробка методів організації групової взаємодії при вирішенні творчих завдань, а також вивчення основних парадигм пошукового мислення.

Завдання третього типу полягають в конструюванні безлічі імітаційних моделей, що описують вплив того чи іншого взаємодії на поведінку об'єкта дослідження.

У системних дослідженнях не мають на меті створення якоїсь супермоделі. Ставиться завдання по розробці приватних моделей, кожна з яких вирішує свої специфічні питання.

Навіть після того як подібні імітаційні моделі створені і досліджені, питання про зведення різних аспектів поведінки системи в якусь єдину схему залишається відкритим. Однак вирішити його можна і потрібно не за допомогою побудови супермоделі, а аналізуючи реакції на спостереження поведінки інших взаємодіючих об'єктів, шляхом дослідження поведінки об'єктів-аналогів і перенесення результатів цих досліджень на об'єкт системного аналізу. Таке дослідження дає підставу для змістовного розуміння ситуацій взаємодії і структури взаємозв'язків, що визначають місце досліджуваної системи в структурі суперсистеми.

Завдання четвертого типу пов'язані з конструюванням моделей прийняття рішень. Будь-яке системне дослідження пов'язане з різними альтернативами розвитку системи. Завдання системних аналітиків вибрати і обгрунтувати найкращу альтернативу розвитку. На етапі вироблення і прийняття рішень необхідно враховувати взаємодію системи з її підсистемами, поєднувати цілі системи з цілями її підсистем, виділяти глобальні і другорядні цілі.

Найбільш розвинена і в той же час найбільш специфічна область наукової творчості пов'язана з розвитком теорії прийняття рішень і формуванням цільових структур, програм і планів. Тут не відчувається нестачі і в роботах, в які працюють дослідники. Однак і в даному випадку занадто багато результати знаходяться на рівні непідтвердженого винахідництва і різночитань в розумінні як змісту поставлених завдань, так і засобів їх вирішення. Дослідження в цій області включають:

а) побудову теорії оцінки ефективності прийнятих рішень або сформованих планів і програм;

б) рішення проблеми багатокритеріальності в оцінках альтернатив рішення або планування;

в) дослідження проблеми невизначеності, особливо пов'язаної ні з факторами статистичного характеру, а з невизначеністю експертних суджень і навмисно створюваної невизначеністю поведінки системи;

г) розробку проблеми агрегування індивідуальних переваг на рішеннях, які зачіпають інтереси сторін, що впливають на поведінку системи;

д) вивчення специфічних особливостей соціально-економічних критеріїв ефективності;

е) створення методів перевірки логічної узгодженості цільових структур і планів і встановлення необхідного балансу між зумовленістю програми дій і її підготовленістю до перебудови, при надходженні нової інформації про зовнішні події та інших змінах.

Розглянуті завдання системного аналізу не охоплюють повного переліку завдань. Тут вказано конкретно, які є найбільш складними при їх вирішенні.

Слід зазначити, що всі завдання системних досліджень тісно взаємопов'язані між собою, не можуть бути ізольовані і вирішуватися окремо як за часом, так і за складом виконавців. Більш того, щоб вирішувати всі ці завдання, дослідник повинен володіти широким кругозором і володіти багатим арсеналом методів і засобів наукового дослідження.

Кінцевою метою системного аналізу є вирішення проблемної ситуації, що виникла перед об'єктом проведеного системного дослідження (зазвичай це конкретна організація, колектив, підприємство, окремий регіон, соціальна структура і т. п.). Системний аналіз займається вивченням проблемної ситуації, з'ясуванням її причин, виробленням варіантів її усунення, прийняттям рішення і організацією подальшого функціонування системи, щоб не допускати проблемної ситуації

3.1.2. Методи дослідження інформаційних систем в системному аналізі

Всю сукупність методів дослідження можна розбити на три великі групи: методи, засновані на використанні знань і інтуїції фахівців; методи формалізованого представлення систем управління (методи формального моделювання досліджуваних процесів) і комплексні методи.

Перша група - методи, засновані на виявленні та узагальненні думок досвідчених фахівців-експертів, використанні їхнього досвіду і нетрадиційних підходів до аналізу діяльності організації включають: метод «мозкової атаки», метод типу «сценаріїв», метод експертних оцінок, метод типу «Дельфі», методи типу «дерева цілей», «ділової гри», морфологічні методи, SWOT-аналіз і ряд інших методів.

Друга група - методи формалізованого представлення систем управління, засновані на використанні математичних, економіко-математичних методів і моделей дослідження систем управління. Серед них класи: аналітичні; теоретико-множинні, логічні, лінгвістичні, подання; графічні.

До третьої групи відносяться комплексні методи: комбінаторика, ситуаційне моделювання, топологія, і ін. Вони сформувалися шляхом інтеграції експертних і формалізованих методів.

Схема структуризації методів дослідження ІС наведена на рис.3.1.

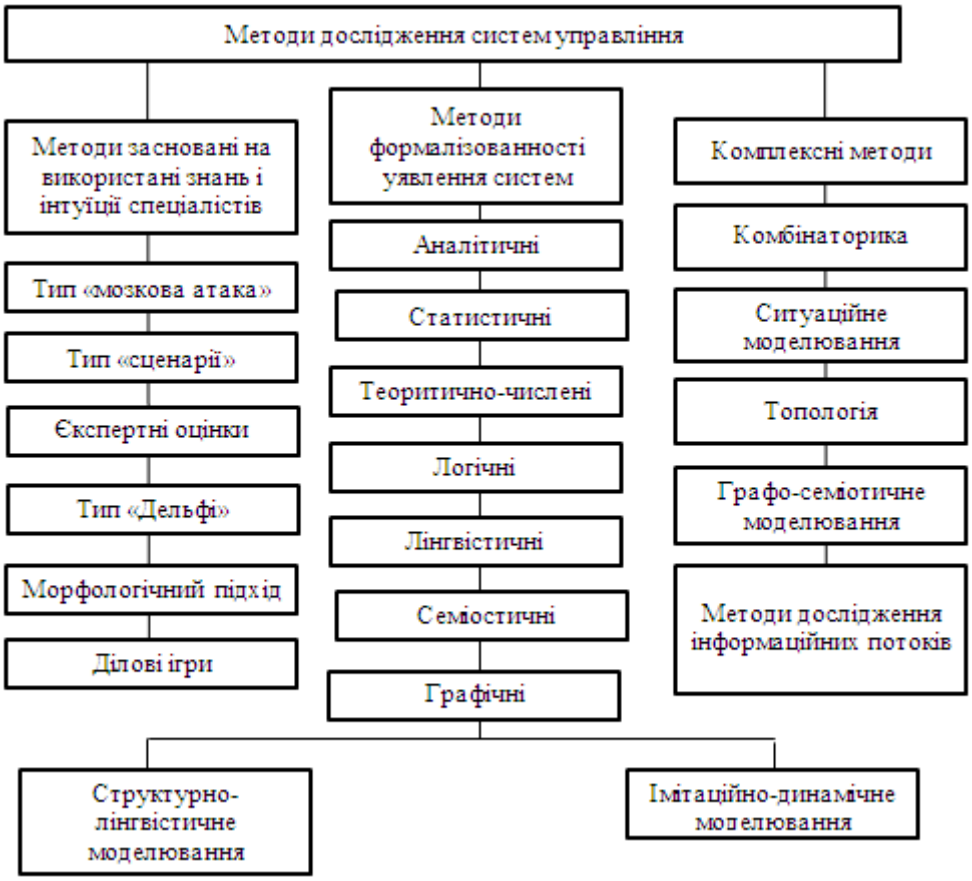


Рис.3.1. Структуризація методів дослідження систем управління (ІС)

Слід зазначити, що будь-яка класифікація умовна. Вона лише засіб, що допомагає орієнтуватися у величезному числі різноманітних методів і моделей. Тому розробляти класифікацію потрібно з урахуванням конкретних умов дослідження і особливостей модельованих систем (процесів прийняття рішень).

З практичної точки зору методика проведення досліджень, як правило, включає три основні розділи: теоретичний, методичний, організаційний.

У **теоретичному розділі** визначаються основні цілі, завдання, предмет і об'єкт дослідження.

Методичний розділ містить обгрунтування вибору методу проведення досліджень, збору і обробки даних, аналіз отриманих результатів, способи їх оформлення.

Організаційний розділ представляє, план проведення досліджень, формування команди виконавців, розподіл трудових і фінансових ресурсів. Тут же визначається і організаційна форма проведення досліджень, тобто

індивідуальні або колективні дослідження, дослідження, проведені внутрішніми або зовнішніми фахівцями. Виділяються спеціальні відділи, служби управління змінами, цільові проектні підрозділи, які будуть задіяні в проведенні дослідження систем управління.

Збір даних є основним етапом дослідження. Для цих цілей використовується ряд методів, серед яких найбільш ефективними є:

• бесіди з фахівцями апарату управління;

• вивчення техніко-економічних і статистичних відомостей про розвиток виробництва даного підприємства;

• вивчення досвіду розвитку однотипних підприємств.

Особливе значення в дослідженні мають бесіди з персоналом апарату управління, які в короткі терміни дозволяють отримати відомості про позитивні і негативні фактори в розвитку об'єкта, проаналізувати і узагальнити ці дані, а також намітити конкретні напрямки робіт.

У більшості випадків відомості по певній групі чинників легше і швидше отримати в ході бесіди з працівниками підприємства.

Ефективність дослідження систем багато в чому визначається обраними і використаними методами дослідження.

Методи дослідження являють собою способи, прийоми проведення досліджень. Їх грамотне застосування сприяє отриманню достовірних і, повних результатів дослідження виникли в організації проблем. Вибір методів дослідження, інтеграція різних методів при проведенні дослідження визначається знаннями, досвідом і інтуїцією фахівців, які проводять дослідження.

3.1.3 Застосування методів системного аналізу на практиці

У системному аналізі акцентується увага на труднощі формулювань

задач, на способах подолання цих труднощів. З практичного боку системний аналіз є теорія і практика втручання в проблемну ситуацію.

Застосування методів системного аналізу до дослідження проблеми захисту інформації диктується вимогами практики, яка поставила фахівців перед необхідністю:

- проектувати складні системи захисту інформації,

- вивчати процеси, які протікають в них,

- управляти процесами в умовах невизначеності, неповноти інформації, дефіциту часу і обмеженості ресурсів.

Специфічною особливістю розглянутих в літературі методик системного аналізу є те, що вони використовують закономірності побудови,

функціонування і розвитку систем, формування варіантів структури системи і вибір найкращого варіанту.

Методи системного аналізу - ***це декомпозиція, аналіз і синтез системи***, що знімає або послаблює проблему практики.

В процесі дослідження використовуються основні принципи системного аналізу, сформульовані стосовно захисту інформації.

Аналіз різних варіантів декомпозиції життєвого циклу ІС і проблем показує, що, стосовно до проблеми розв'язання наявних протиріч в області забезпечення безпеки інформації, можливо формування наступного варіанта декомпозиції:

- виявлення проблеми забезпечення безпеки інформації та оцінка її актуальності;

- визначення мети організації, формулювання загальної мети і завдань системи забезпечення ІБ, декомпозиція цілей;

- розробка моделі системи забезпечення ІБ і її декомпозиція, аналіз об'єкта дослідження;

- пошук можливостей підвищення ефективності захисту інформації: розробка моделі керуючої системи і її деталізація;

- прогнозування показника ефективності системи захисту інформації - рівня захищеності інформації.

Застосування системного підходу до вирішення проблеми забезпечення повноти і ефективності реалізації функцій системи забезпечення ІБ на різних етапах її життєвого циклу викликає необхідність розробки керуючої системи, покликаної не тільки забезпечити раціональні ресурсні, фінансові та часові характеристики, а й підвищити ступінь наукової обгрунтованості та оперативності прийнятих управлінських рішень.

Робоче формулювання проблеми забезпечення ІБ:

Як підвищити ефективність системи забезпечення ІБ?

Як сформувати раціональний комплекс засобів захисту інформації в інформаційній системі?

Як реагувати на небезпечні події в мережі, щоб мінімізувати збиток?

Модель проблемної ситуації щодо захисту інформації містить сукупність трьох взаємодіючих систем (див. рис.3.2):

- проблемозмістовної (проблемовмісної) системи забезпечення ІБ;

- проблемодозвільної (проблемовирішуючої) системи, тобто системи, яка розробляється для того, щоб вплинути на процеси захисту інформації таким чином, щоб проблема зникла або ослабла;

- навколишнього, або істотної середовища, в умовах якої функціонує системи забезпечення ІБ.

Так як функціонування системи забезпечення ІБ пов'язано з процесами інформаційного протиборства, яке спрямоване на протидію зовнішнім і внутрішнім загрозам, то під навколишним середовищем розуміється безліч потенційно можливих зовнішніх і внутрішніх загроз інформації в інформаційній системі.

- проблемозмістовна система забезпечення ІБ є об'єктом дослідження, а в якості цільової виступає керуюча проблемодозвільна система.

Дана модель дозволяє не тільки підвищити повноту набору цілей, а й структурувати їх сукупність, що згодом дозволить здійснити постановку завдань по прийняттю раціональних рішень з управління захистом інформації.

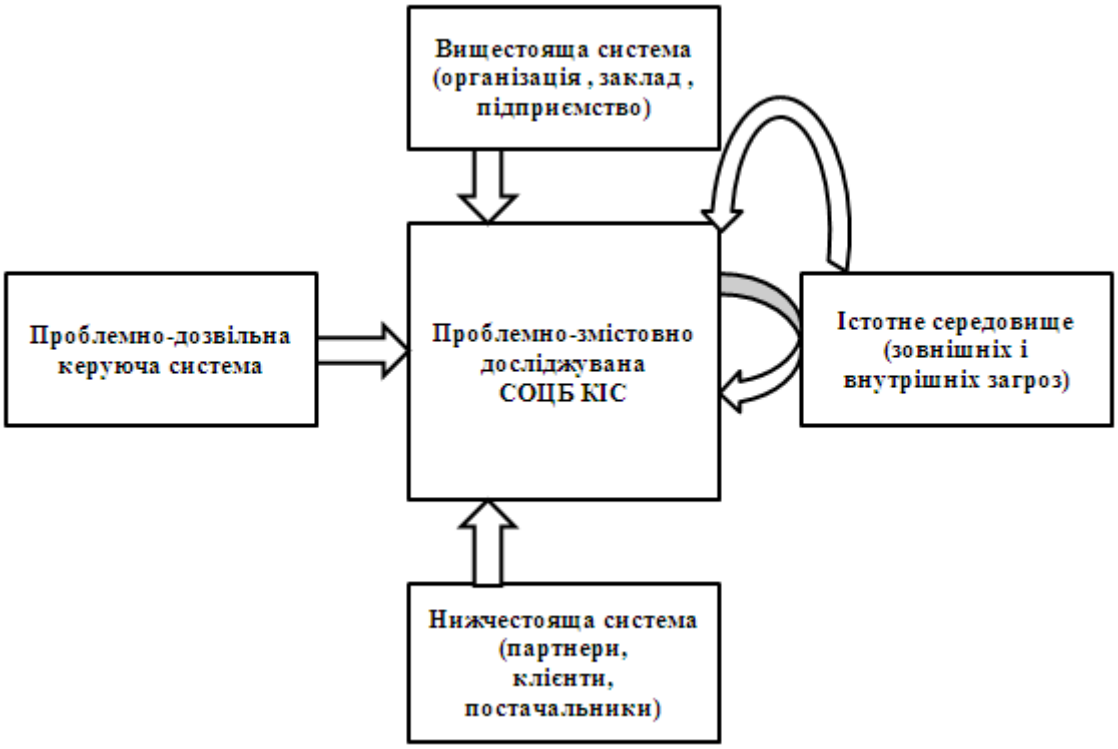


Рис.3.2. Схема системи забезпечення ІБ КІС, як об'єкта дослідження при реалізації системного підходу до вирішення проблеми

Метою вищестоящої системи є підвищення ефективності процесу інформатизації, яка в даний час є недостатньою через щорічне шкоди від злочинів в сфері ІТ, що здійснюються з використанням засобів обчислювальної техніки.

Для **проблемозмістовної системи** головне - **вирішити проблему**, мети **проблемодозвільної системи** пов'язані з раціональним **витрачанням ресурсів на вирішення проблеми**.

Цілі істотної середовища (зовнішні і внутрішні загрози) і системи забезпечення ІБ протилежні.

Загальною метою захисту інформації в ІС є запобігання або зниження шкоди, яка завдається власнику, власнику чи користувачу системи внаслідок реалізації загроз безпеці інформації.

Приватними цілями захисту інформації, що забезпечують досягнення загальної мети, є:

- забезпечення правового режиму використання масивів даних і програм обробки інформації;

- запобігання несанкціонованого знищення, перекручення, копіювання інформації, блокування доступу до інформації;

- збереження можливості управління процесом обробки та використання інформації в умовах несанкціонованих (програмно-технічних) впливів на захищається інформацію;

- запобігання витоку інформації технічними каналами.

Мета захисту інформації повинна включати, крім формулювання, кількісну оцінку характеристик систем - показник ефективності досягнення мети і його необхідне значення, а також час актуальності мети на етапах життєвого циклу, протягом яких мета повинна досягатися.

Показником ефективності досягнення мети ЗІ зазвичай вважається ***рівень захищеності інформації на об'єкті захисту, або відносний ризик порушення ІБ***. Значення рівня захищеності інформації задається замовником в залежності від максимального рівня критичності оброблюваної на об'єкті захисту інформації, і може приймати ймовірні значення від 0,9 до 1, які визначаються планами обробки інформації на об'єкті захисту.

У практиці системного аналізу в якості глобального об'єкта декомпозиції береться **досліджувана проблема** і **проблемозмістовна система**.

Для цілей аналізу проблеми захисту інформації необхідна модель системи забезпечення ІБ. Для цього можна використовувати модель діяльності, надавши відповідну інтерпретацію компонентам, які входять в цю модель (рис.3.3).

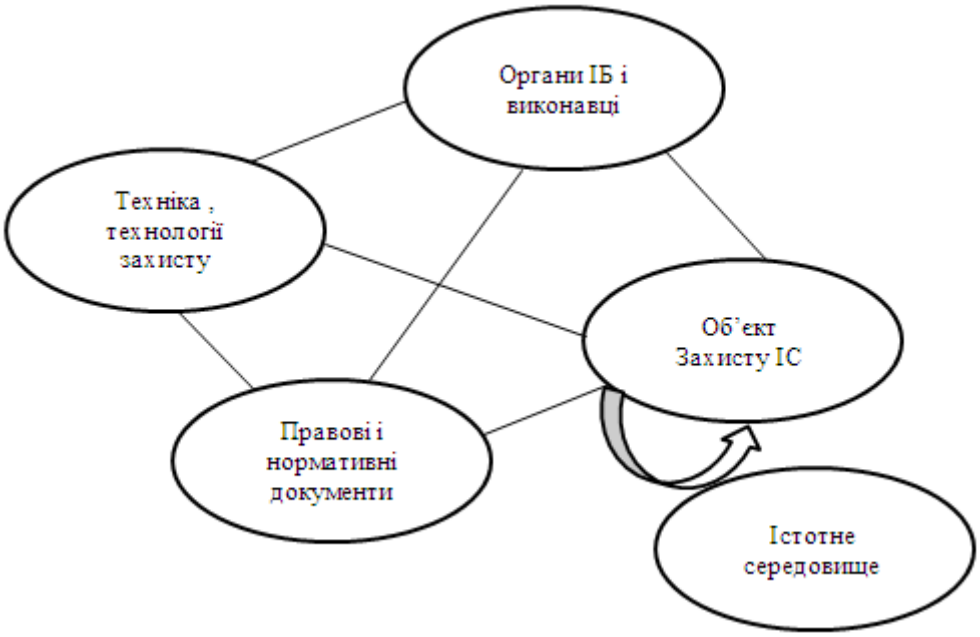


Рис.3.3. Схема компонентів, що входять в модель діяльності системи забезпечення ІБ

Одна з важливих завдань інформаційного забезпечення в процесі системного аналізу полягає в розробці і накопиченні моделей.

Для аналізу процесів ЗІ необхідні моделі, які деталізують компоненти: об'єкт захисту, істотну середу, техніку і технології захисту.

Метод декомпозиції є одним із способів спрощення складної системи забезпечення ІБ. Він складається в постійно наростаючою деталізації базових моделей системи захисту, в розкладанні складного цілого на все більш дрібні і прості частини.

Після розробки спрощеної моделі діяльності необхідно відповідно до методу декомпозиції системного аналізу здійснити багатоступінчастий процес від початкової декомпозиції до завершального рівня.

Об'єкт захисту - інформаційна система є складною організаційно-технічною системою, що складається з двох компонентів: інформаційної інфраструктури та інформаційних сервісів.

Інформаційна інфраструктура є середовищем, в якій функціонують інформаційні сервіси. Якість інформаційних сервісів безпосередньо залежить від

якості інформаційної інфраструктури та управління нею. Інформаційна інфраструктура сучасних

ІС - це телекомунікаційна система (ТКС). **ТКС** - це носії і засоби обробки інформаційних ресурсів, а також середа, яка забезпечує виробництво і споживання інформаційних продуктів і послуг.

Найважливішим системним властивістю ТКС є можливість здійснення комунікаційних функцій через стандартизовані уніфіковані інтерфейси. Це дозволяє прикладним системам розглядати ТКС як «Чорний ящик» і будувати свою реалізацію без урахування специфічних особливостей конкретної ТКС.

Модель складу об'єкта захисту інформації з декомпозицією компонента «інформаційна інфраструктура» приведена на рис.3. 4.

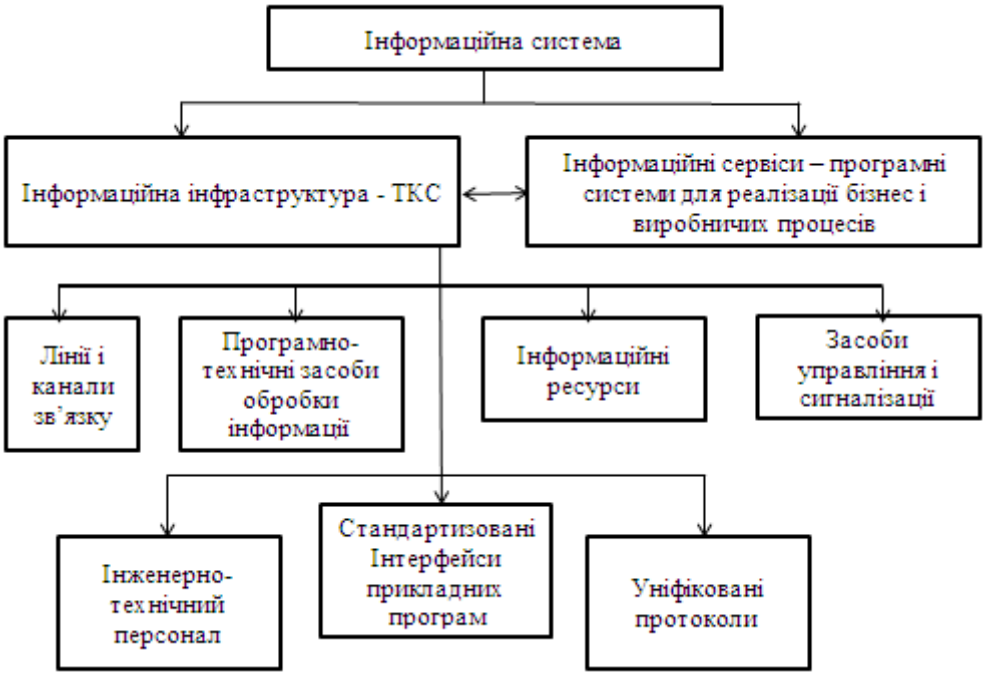


Рис.3.4. Модель складу об'єкта захисту інформації з декомпозицією компоненти «інформаційна інфраструктура»

Програмні системи можуть бути представлені у вигляді сукупності взаємодіючих програмних модулів. Однак кожна конкретна програмна система має свій склад модулів, певний специфічними завданнями, на вирішення яких спрямована дана система в залежності від реалізованих бізнес-процесів.

Щодо модуля системи забезпечення ІБ «техніка, технології захисту» (див. рис.2) - захист інформації на рівні інформаційної інфраструктури здійснюється на чотирьох рівнях моделі OSI: фізичному, канальному, мережевому і транспортному.

Моделювання загроз порушення безпеки інформації дозволяє спеціалісту по захисту інформації отримати досить переконливі доводи про

наявності потенційних загроз на конкретному об'єкті захисту, що сприяє

фінансування проекту системи забезпечення ІБ в необхідному обсязі.

На рис.3.5 наведена модель складу істотної середовища - навмисних загроз об'єкту захисту.

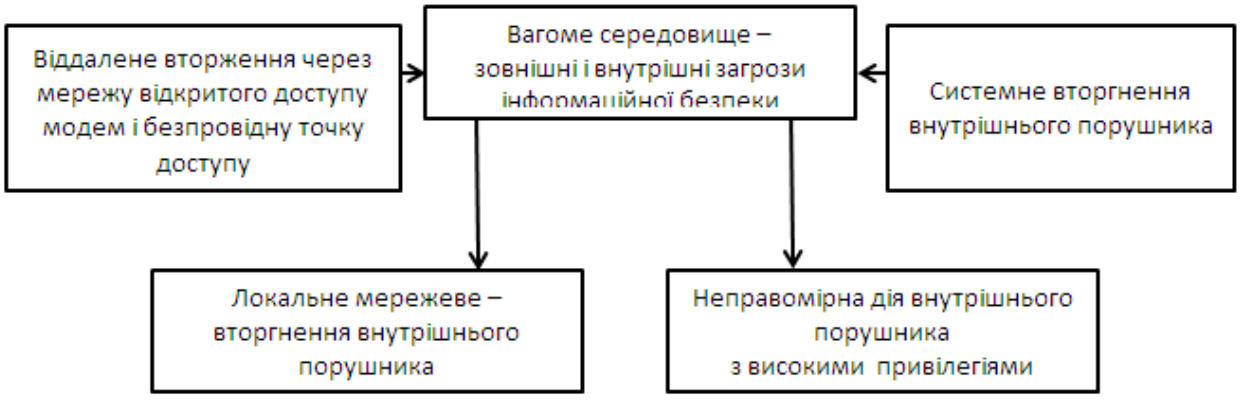


Рис.3.5. Модель складу навмисних загроз об'єкту захисту

Захист на рівні ТКС включає в себе наступні аспекти:

• забезпечення доступності за рахунок виключення точок збою;

• врахування вимог безпеки в структурі самої мережі: організація впровадження внутрішніх захищених підмереж і зовнішніх екрануючих сегментів;

• вдосконалення інформаційної взаємодії за рахунок модернізації існуючих протоколів та використання таких механізмів захисту як аутентифікація і криптографія;

• віртуалізація каналів інформаційної взаємодії шляхом використання VLAN на канальному рівні і MPLS при міжмережевої взаємодії;

• використання автономних засобів захисту, таких як міжмережеві екрани, системи запобігання вторгнень, антивіруси, сканери безпеки, системи управління інформаційною безпекою та ін.

Забезпечення безпеки ІС вимагає необхідності комплексного підходу.

Сервери реляційних баз даних ІС підтримують значний масив різних типів додатків і прав користувачів. Тому для забезпечення конфіденційності, цілісності та доступності, необхідно застосовувати політику безпеки на декількох рівнях: транспортний рівень, рівень мережі, системний рівень, рівень операційної системи, рівень системи управління базами даних (СУБД), рівень баз даних, рівень таблиць, рівень об'єктів.

На прикладі аналізу істотної середовища особливу увагу слід приділити ***рівню додатків і мережевого рівня***.

На рівні додатків найбільш небезпечні загрози підміни ідентифікатора

і підвищення привілеїв. Якщо парольна інформація передається у відкритому вигляді, то вона може бути переглянута в локальних мережах. Вона також може бути перехоплена при її передачі по мережі Інтернет.

Зловмисник може скористатися перехопленими іменами і паролями для легального входу в операційну систему, наприклад, сервер ІС. Якщо за умовчанням вся інформація на рівні web-служб і додатків також передається у відкритому вигляді, то вона легко може бути перехоплена.

Загроза витоку інформації високого рівня критичності пов'язана з можливим неконтрольованим поширенням інформації легальним користувачем, що має доступ до неї і таким, що порушує свої привілеї після отримання доступу.

На мережевому рівні в результаті сканування мережі ІС, виявлення вразливостей міжмережевих екранів, використання недоліків протоколів маршрутизації, віддаленого пошуку і управління мережею, зловмисник може підмінити мережеві маршрути або об'єкти, наприклад сервер ІС.

На мережевому рівні за рахунок можливості віддаленого запуску додатків можуть реалізовуватися загрози, які приведуть до підміни ідентифікаційної інформації, спотворення даних, порушення конфіденційності інформації.

При проектуванні програмних систем для реалізації бізнес-процесів доцільно використовувати вбудовані засоби захисту. Але вбудовані в програмні системи засоби захисту часто мають недоліки:

• неможливо вирішити і заборонити доступ тільки до певних верств даних;

• користувач, який має доступ до WEB-додатком, отримує дані від всіх його WEB -служб навіть без дозволу доступу до них;

• неможливо розмежовувати права щодо виконання різних видів операцій для різних користувачів;

• користувачам корпоративної мережі сервера ІС надається або не надається повний доступ до даних сервера без можливості більш детального розмежування доступу.

Застосування технології системного аналізу до побудови моделі керуючої системи дозволить:

- визначити її підсистеми, компоненти і способи їх з'єднання,

- задати обмеження, при яких система повинна функціонувати,

- вибрати найбільш ефективне поєднання людей (експертів, фахівців ІБ, аналітиків), ЕОМ і програмного забезпечення.

Якщо для підвищення рівня захищеності йти по шляху використання вбудованих в програмну систему засобів захисту, то на прикладному рівні захисту можна запропонувати наступні заходи:

• введення в рольову модель елементів мандатної доступу (роль, пов'язана з доступом тільки до несекретної інформації; роль, що має доступ як до несекретної, так і до інформації обмеженого доступу; роль, що має повний доступ);

• створення служб, пов'язаних з одним ресурсом, що мають схожі назви, але різний набір операцій;

• виключити локальних користувачів сервера ІС з груп admin (використовувати WEB-доступ до сервера через розмежування доступу до служб і додатків);

• встановити при розміщенні секретної інформації дозвіл на рівні окремих стовпців таблиці (відфільтровування непотрібних);

• запобігти безконтрольний доступ до кешу зображень, минаючи систему безпеки;

• використовувати нові криптографічні технології, що з'явилися в MS SQL Server, що забезпечують прозоре шифрування всієї бази даних.

Запропоновані рішення, проведені на основі методів системного аналізу, дозволяють значно підвищити рівень захищеності ІС.

Питання для самоконтролю

1. Перерахуйте основні завдання системного аналізу в наукових дослідженнях?

2. Перерахуйте основні методи дослідження систем управління ІС.

3. Які основні розділи, з практичної точки зору, включає в себе методика проведення досліджень в системному аналізі?

4. Наведіть варіант декомпозиції ІС в області забезпечення безпеки інформації.

5. Наведіть модель проблемної ситуації щодо захисту інформації (варіант).

6. Наведіть варіант розробки моделі системи забезпечення ІБ і її декомпозиції.

3.2. Аналіз та синтез як методи дослідження і проектування організацій

Аналіз і синтез - це загальнонаукові методи, які застосовуються і в емпіричному, і в теоретичному пізнанні. Аналіз і синтез — це комплексний метод дослідження, сукупність прийомів, операцій і дій з розумового роз'єднання об'єктів на складові, елементи, властивості (аналіз) і об'єднання їх у єдине ціле (синтез) під час вирішення пізнавального завдання. Аналіз і синтез — це складова будь-якого наукового дослідження. Аналіз має створити основу для

синтезу, тобто доказовості, визначення, вирішення проблеми. Синтезоване знання у цілому є якісно новим порівняно з аналітичним. Аналіз і синтез у процесі проектування (і пізнання взагалі) постають у діалектичній єдності. Аналіз без синтезу і синтез без аналізу у пізнанні не застосовуються. систему не можна вивчити за допомогою аналізу, так як при діленні на частини вона втрачає свої суттєві властивості. Синтез завжди націлений на побудову такої нової структури системи, при якій будуть найкращим чином реалізовані її функції (функція від лат. - виконання, здійснення – це діяльність, обов'язок, робота). Отже, аналіз сконцентрований на структурі, а синтез - на функціях системи; аналіз спрямований всередину системи, а синтез – зсередини; аналіз дасть знання, а синтез - розуміння. У теорії організації аналіз включає дві основні процедури: поділ цілого на частини і поліпшення функціонування кожної з цих частин. Синтез також складається з двох процедур: узгодження характеристик виділених частин і об'єднання їх в одне ціле.

3.2.1.Закон єдності аналізу і синтезу

Вивчення організацій як соціально-економічних, так і технічних систем і об'єктів передбачає обов'язкове використання операцій аналізу і синтезу (рис.3.6).

Можна сказати, що аналіз дає знання, а синтез - розуміння.

Аналіз або декомпозиція - це поділ цілого на частини або подання складного об'єкта у вигляді простих складових. Аналіз причинно-наслідкових зв'язків між виділеними частинами зводиться до знаходження необхідних і достатніх умов для підтримки необхідного взаємодії між цими частинами цілого.

Синтез – зворотній процес, від об'єднання простих складових об'єкта в єдине ціле. Об'єднання в рамках синтезу здійснюється на основі взаємної необхідності і взаємозв'язку.

Аналіз і синтез, подібно індукції (умови від часткового до загального, коли на підставі знання частини предметів або властивостей класу робиться висновок про клас в цілому) і дедукції (висновок про властивості деякого елемента безлічі

на підставі знання про загальні властивості всієї множини), можна розглядати з точки зору логіки у вигляді протилежних, але в той же час тісно пов'язаних методів пізнання або двох різних процесів. Якщо йти від причини до дії, від заснування до висновку, то такий шлях називається прогресивним або синтетичним.

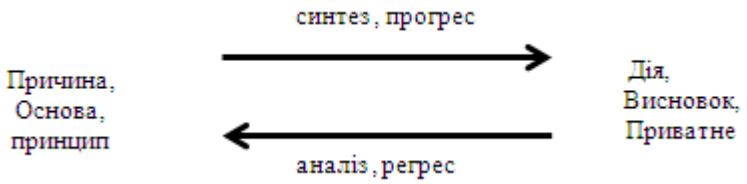


Рис.3.6. Схема відносин між аналізом і синтезом

Прогресивним він називається тому, що відповідає реальному ходу природи, дійсному ходу речей, так як в природі причина раніше, ніж дія.

Дорога назад, саме від дії до причини, від висновків до принципів, називається регресивним, аналітичним.

Будь-яке пізнання (після попереднього загального ознайомлення) зазвичай починається з аналізу, а не з синтезу. Щоб об'єднати частини в ціле, необхідно спочатку мати ці частини перед собою. Тому аналіз завжди передує синтезу.

Метод аналізу і синтезу (рис.3.7 і 3.8) передбачає вивчення соціально-економічних явищ і об'єктів як по частинах (аналіз), так і в цілому (синтез). Таким чином, аналіз - це метод пізнання, змістом якого є сукупність прийомів і закономірностей розчленування предмета дослідження на його складові частини, а синтез - це метод пізнання, змістом якого є сукупність прийомів і закономірностей з'єднання окремих частин предмета в єдине ціле.

Рис.3.7. Призначення методу аналізу і синтезу

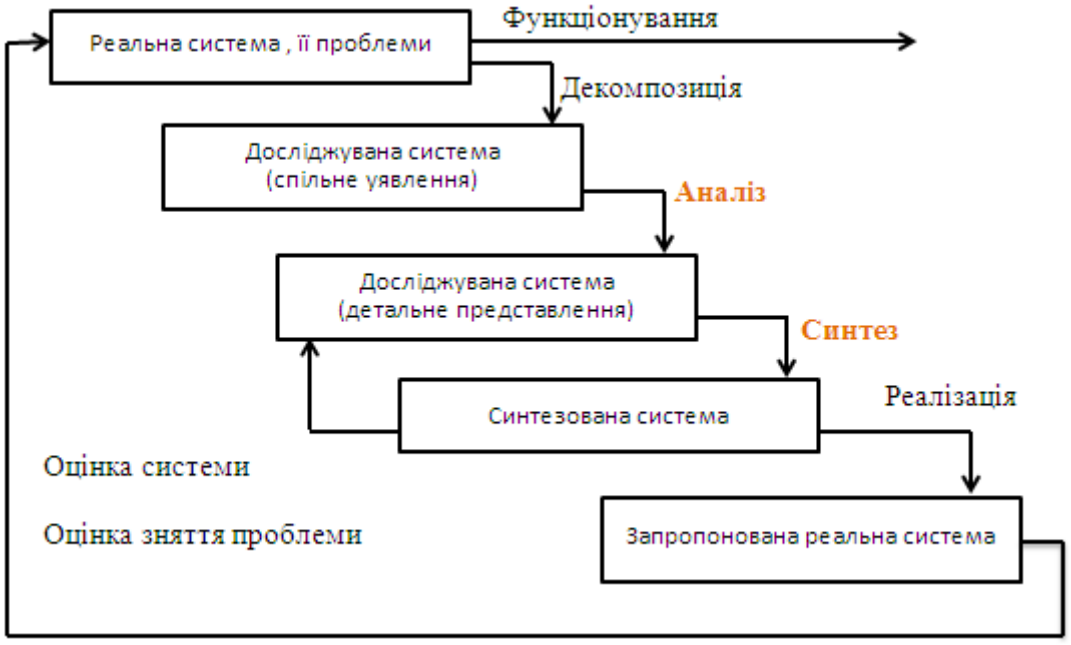


Рис.3.8. Місце аналізу і синтезу в процесах системного підходу

З точки зору основ методології, аналіз являє собою особливий інструмент дослідження, за допомогою якого виявляється, наскільки відповідає система управління організації тим навколишнім соціально-економічним умовам, в яких здійснюється її діяльність. Синтез ж необхідний для того, щоб дати

характеристику основних структурних компонентів організації, виявити основні шляхи та механізми їх взаємодії.

Аналіз і синтез розглядаються як методи оцінки сьогодення і майбутнього компанії (організації).

Під законом єдності аналізу і синтезу мається на увазі нерозривність і постійна взаємодія його складових, здійснюване в рамках діалектичного принципу єдності і боротьби протилежностей.

Управляюча система будь-якої організації прагне до найбільш ефективної функціональної та організаційної структури за рахунок постійного циклічного процесу аналізу - синтезу (дедукції - індукції).

Іншими словами, кожна матеріальна система: живий організм, соціальна організація (підприємство, навчальний заклад) - прагне налаштуватися на найбільш економний режим функціонування в результаті постійної зміни своєї структури або функцій. Ці зміни відбуваються в наступному циклі: поділ - перетворення - об'єднання - перетворення.

Для забезпечення цієї успішної діяльності керівник організації повинен:

- прагнути до постійного моніторингу внутрішніх та зовнішніх сильних і слабких сторін організації;

- ретельно планувати діяльність як всієї організації, так і окремих підрозділів;

- прагнути до мінімізації виробництва по ресурсах;

- застосовувати сучасну інформаційну технологію.

Аналіз і синтез в своєму єднанні складають основу системного підходу до вивчення діяльності організації, як науково-методологічну основу, яка сприяє знаходженню найбільш вигідних шляхів вирішення виникаючих проблем.

Закон єдності аналізу і синтезу тісно взаємодіє з законами розвитку, інформованості-впорядкованості, самозбереження і синергії (рис.3.9). Найважливішу роль закон відіграє при прагненні системи до досягнення відповідності, пропорційності елементів між собою і в співвідношенні до цілого, з його допомогою реалізуються принципи композиції і пропорційності.

Рис.3.9. Взаємодія закону єдності аналізу та синтезу з іншими законами організації

Закон єдності аналізу і синтезу має суттєві відмінності від інших законів:

- він не відображає специфіки історично визначених відносин, а описує зв'язки і відносини в соціальному середовищі взагалі;
- грає роль каталізатора суспільного прогресу;
- з розвитком суспільства його значення зростає.

Закон єдності аналізу і синтезу має слідства:

Слідство 1. При відсутності зовнішніх впливів, що обурюють всі творчі ресурси організації витрачаються на внутрішні потреби організації, що веде до переродження господарської організації в суспільну.

Слідство 2. При відсутності зовнішніх і внутрішніх впливів, що обурюють всі творчі ресурси організації виявляються не затребувані. Це веде організацію до деградації.

Слідство 3. При відсутності внутрішніх збурюючих впливів всі творчі ресурси організації витрачаються на зовнішні потреби, що, з одного боку, здатне згуртувати колектив навколо спільних проблем, а з іншого боку, з огляду на некритичну внутрішню атмосферу, веде до застою і неефективній роботі.

З наслідків 2 і 3 слідств випливає парадоксальний висновок про те, що для організації та людини необхідні зовнішні потрясіння і внутрішні протиріччя, які звичайно, не доводять до патологічних проблем.

Закон єдності аналізу і синтезу може бути реалізований в трьох варіантах:

Відповідно **до першого варіанту** ні керівник, ні підлеглі нічого про нього не знають. В організації відбуваються формальні і неформальні зміни в структурі, виконуваних функціях, персоналі. Такі зміни можна вважати рутинними. Якщо такі зміни відбуваються вчасно, тоді вони непомітні, то закон єдності аналізу і синтезу реалізується ефективно. У разі невідповідності швидкості перетворень потребам організації виникають проблеми з прибутковістю, конкурентоспроможністю та іншими характеристиками. Згодом проблеми будуть виявлені, але час реакції буде вже упущено.

У **другому варіанті** керівник знає про закон, а його підлеглі не знають. У разі невідповідності поточних організаційних змін вимог зовнішнього і внутрішнього середовища, керівник оцінює тільки неповноту такої відповідності.

Підлеглі не прагнуть ні до яких перетворень, і керівнику доводиться переконувати людей в необхідності конкретних змін. Якщо ж виявлені великі невідповідності, персонал буде активно брати участь у перетвореннях, але реакція також буде запізнілою.

Третій варіант є найбільш сприятливим, так як керівник і підлеглі знають про існування закону єдності аналізу та синтезу. Свій внесок в дію закону вносять всі працівники в межах своїх повноважень і відповідальності.

Аналіз і синтез організацій можна проводити як закон на практиці (що дуже важливо для будь-якого керівника) - за допомогою методу поступового наближення, що включає **чотири рівні**:

1. Попередній аналіз з позицій стороннього спостерігача.

2. Мозкова атака на нараді основних фахівців організації.

3. Створення групи розвитку підприємства і формування стратегії розвитку організації.

4. Постійна робота групи розвитку.

Завдання керівника: забезпечити якісне планування реорганізації діяльності окремих підрозділів і повинна полягати: в забезпеченні новими джерелами інформації, організації навчання своїх співробітників, впровадження найбільш досконалих технологій.

Процеси аналізу і синтезу є основою управління будь-якої організаційної системою і передбачають вироблення і реалізацію конкретних рішень.

Рішення - це засіб комунікації між ланками і елементами організації, в тому числі і між людьми. За допомогою управлінських рішень реалізується зв'язок між окремими ланками системи управління.

Використання процесів аналізу і синтезу є обов'язковою складовою будь-якої процедури прийняття рішення з управління організацією, так як першим етапом прийняття рішення є визначення мети, на досягнення якої спрямоване це рішення.

Наступним етапом є процес аналізу, який забезпечить знаннями про можливості організації для виконання поставленої мети, про її зовнішніх і внутрішніх умовах, що впливають на її діяльність.

Аналіз впливу кожного окремого ланки зовнішніх і внутрішніх умов проводиться з використанням математичних і формально-логічних методів.

Аналіз внутрішнього середовища досліджуваного об'єкта проводиться з використанням методів декомпозиції, заснованих на принципах незалежності, повноти відображення і слабкого впливу. Елементи внутрішнього середовища показані на рис.3.10.

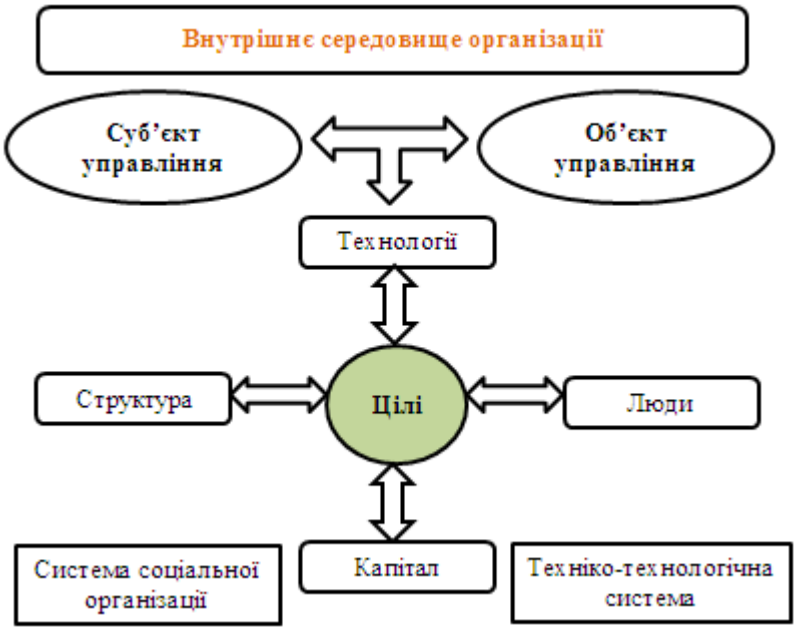


Рис.3.10. Елементи внутрішнього середовища

Незалежність передбачає можливість самостійного аналізу роботи кожного підрозділу організації: бухгалтерії, відділу кадрів, комерційного відділу, виробничих підрозділів і т. д.

Повнота відображення має на увазі, що подальше об'єднання елементів за встановленим правилом призводить до вихідної системи. Це означає, що процес декомпозиції досліджуваної системи має будуватися так, щоб можна було здійснити зворотний процес відновлення вихідної системи по її окремих елементах, ланкам і підсистем.

Слабкий вплив. Цей принцип заснований на тому, що внутрішні процеси, що відбуваються в одному виділеному елементі, не повинні надавати значного впливу на функціонування інших елементів системи.

У наукових дослідженнях використовують такі види аналізу і синтезу:

Прямий або емпіричний -застосовується на стадії поверхового ознайомлення з об'єктом дослідження і дає можливість пізнати явище, але для проникнення в сутність речі він недостатній (можливий як експериментальне об'єкта на елементи).

Поворотний або елементарно-теоретичний -застосовується для розуміння суті досліджуваного об'єкта -дає можливість пізнати причинно-наслідковий зв'язок, закономірність.

Структурно-генетичний - застосовується для виокремлення в складному утворенні таких елементів, які представляють найголовніше в них.

3.2.2. Цілі, завдання аналізу і синтезу систем управління

Під аналізом систем управління (СУ) розуміється процес дослідження системи управління, заснований на її декомпозиції з подальшим визначенням статичних і динамічних характеристик складових елементів, що розглядаються у взаємозв'язку з іншими елементами системи і навколишнім середовищем. **Цілі аналізу системи управління**:

• детальне вивчення системи управління для більш ефективного використання та прийняття рішення щодо її подальшого вдосконалення або заміни;

• дослідження альтернативних варіантів новостворюваної системи управління з метою вибору найкращого варіанту.

До завдань аналізу системи управління відносяться:

• визначення об'єкта аналізу і структурування системи;

• визначення функціональних особливостей системи управління;

• дослідження інформаційних характеристик системи;

• визначення кількісних і якісних показників системи управління;

• оцінка ефективності системи управління;

• узагальнення та оформлення результатів аналізу.

Визначення об'єкта аналізу. При вирішенні цього завдання потрібно виконати наступні дії:

• виділити аналізовану систему управління;

• визначити цілі і завдання управління;

• провести первинну декомпозицію системи з виділенням керуючої підсистеми (органів управління), об'єктів управління (виконавців) і навколишнього середовища.

Структурування системи. Метою структурування є детальне вивчення системи управління, встановлення зв'язків і відносин між її елементами. Під завданням аналізу структури розуміється визначення основних характеристик системи при деякій обраної (фіксованою) структурі.

Основні характеристики структури системи розбивають на групи.

До першої відносяться характеристики, пов'язані з ієрархічністю систем: число підсистем даної системи, характер взаємозв'язків між рівнями (підсистемами), ступінь централізації і децентралізації в управлінні, ознаки розбиття системи на підсистеми.

До другої - ефективність (в широкому сенсі) функціонування системи тієї чи іншої структури: ефективність (вартісна), надійність, живучість, швидкодія, пропускна здатність, здатність до перебудови і ін.

Визначення функціональних особливостей системи. Завдання визначення функціональних особливостей системи строго пов'язана з завданням структурування. З урахуванням структурування визначаються перелік приватних завдань і функції кожного елемента системи, порядок їх взаємодії, необхідні вхідні і вихідні дані.

Дослідження інформаційних характеристик системи. У процесі дослідження інформаційних характеристик визначаються:

• сутність і якість інформації, що використовуються для вироблення управляючих впливів;

• достатність інформації для вироблення управляючих впливів;

• сумарні обсяги надходить і що виходить інформації в одиницю часу в цілому по системі і окремо по основних елементів;

• обсяг інформації, постійно зберігається в системі;

• одиничні обсяги переданої інформації;

• способи передачі або доставки інформації;

• основні напрямки інформаційних потоків та ін.

Визначення кількісних і якісних показників системи. Після з'ясування поставленого завдання, визначення об'єкта аналізу і складання його багаторівневого опису виробляються:

- попередній вибір переліку показників кожного рівня;

- розробка моделей і методів визначення показників різних рівнів;

- уточнення умов визначення показників, що включають передбачувані дії над системою, можливість інтегрування з іншими системами управління і наявність дублюючих систем.

В результаті рішення даної задачі:

систематизуються приватні якісні і кількісні показники структур, процесів функціонування та інформації;

визначаються узагальнені показники, що характеризують зовнішні властивості аналізованої системи і її окремих елементів.

Оцінка ефективності. Дане завдання вирішується з метою визначення досягнутих в процесі функціонування системи управління результатів і витрачених на досягнення цих результатів матеріальних і часових ресурсів.

Це експериментальні показники функціонування - вимірюють ті чи інші результати реального (або імітаційного) функціонування системи.

Це теоретичні показники функціонування - оцінки можливих значень експериментально визначених показників.

Точність теоретичних оцінок являє собою "міру відповідності" оцінок.

Узагальнення та оформлення результатів аналізу. Завдання документального узагальнення і оформлення результатів аналізу включає:

- короткий опис структури, процесів функціонування та інформаційних потоків системи;

- узагальнене значення показників і результатів оцінки ефективності системи (наводяться значення показників);

- узагальнені виявлені недоліки і попередні рекомендації щодо подальшого використання системи, вдосконалення або її заміні.

Узагальнений алгоритм системного аналізу об'єкта представлен на рис.3.11.

Різновиди аналізу. Сутністю ***структурного аналізу*** є визначення статичних характеристик систем за відомою її структури. Структурний аналіз проводиться з метою дослідження статичних характеристик системи шляхом виділення в ній підсистем і елементів різного рівня і зв'язків між ними. Об'єктами дослідження структурного аналізу є різні варіанти структур системи управління, які формуються в процесі її декомпозиції.

Рис. 3.11. Узагальнений алгоритм системного аналізу об'єкта

Сутністю ***функціонального аналізу*** є визначення динамічних характеристик систем на підставі прийнятих алгоритмів її функціонування. Загальна схема функціонального аналізу систем представлена на рис.3.12. Функціональний аналіз проводиться з метою визначення динамічних характеристик системи шляхом дослідження процесів зміни її станів з плином часу на основі прийнятих алгоритмів (способів, методів, принципів, концепцій) управління. Об'єктами дослідження функціонального аналізу є реалізовані системою методи і алгоритми управління, включаючи загальний алгоритм функціонування, що містить всі основні етапи (фази, функції) управління, і приватні методи і алгоритми, спрямовані на виконання окремих етапів

управління (формування мети управління, збір і обробка необхідної інформації , прийняття рішень, планування, організація, контроль, виконання рішень та ін.).

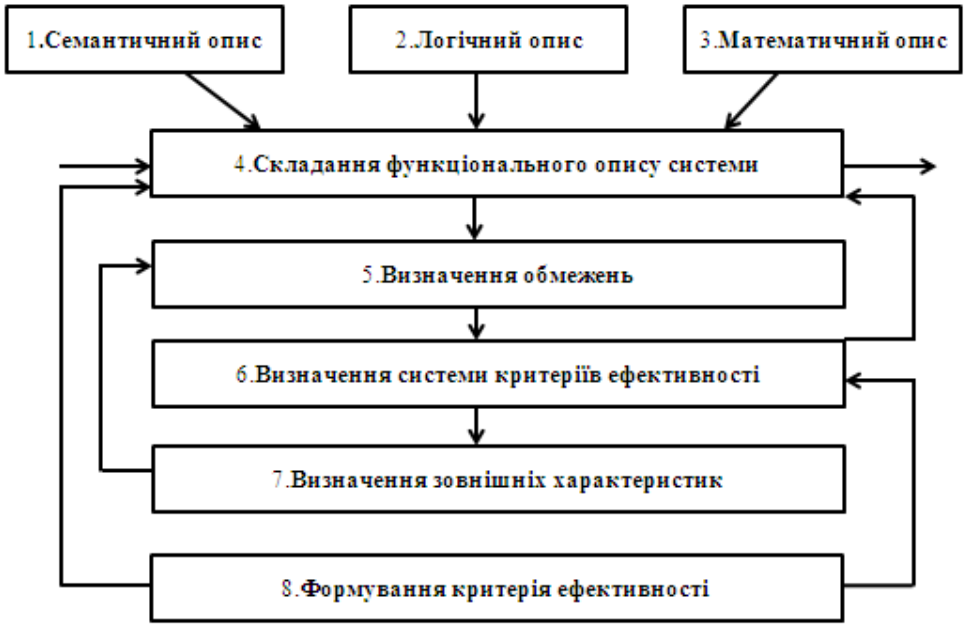


Рис. 3.12. Загальна схема функціонального аналізу систем

Сутністю ***інформаційного аналізу*** є визначення об'єкта і форм подання інформації, методів і засобів її передачі, обробки, зберігання, введення і виведення для відомої структури і алгоритму функціонування системи управління. Інформаційний аналіз проводиться з метою дослідження кількісних і якісних характеристик інформації, використовуваної в системі управління. Об'єктами дослідження виступають інформаційні процеси, що протікають в системі управління.

У системах управління виділяють наступні інформаційні процеси:

- збір, прийом, сприйняття інформації (ці процеси відображають взаємодію системи із зовнішнім середовищем);
- передача інформації між окремими підсистемами системи; переробка, аналіз, відбір інформації, створення нової інформації;
- використання інформації; передача інформації з системи у зовнішнє середовище.

Сутністю **параметричного аналізу** є визначення необхідної і достатньої сукупності показників, що характеризують всі досліджувані властивості системи і формування залежностей, що характеризують сумарний ефект від застосування системи або її елементів. Мета параметричного аналізу - оцінка ефективності системи управління на основі визначення кількісних значень її показників. Об'єкти дослідження параметричного аналізу - це приватні та узагальнені показники системи, що утворюють ієрархічну структуру.

Цілі і завдання синтезу систем управління. На відміну від аналізу дослідження заданої системи управління, під синтезом розуміється процес створення нової системи шляхом визначення її раціональних або оптимальних властивостей і відповідних показників.

Цілі синтезу системи управління:

• створення нової системи управління на основі нових досягнення науки і техніки;

• вдосконалення існуючої системи управління на основі виявлених недоліків, а також появи нових завдань і вимог.

У загальному вигляді завдання синтезу систем управління полягають у визначенні структури і параметрів системи виходячи із заданих вимог до значень показників ефективності її функціонування, а також способів забезпечення цілей функціонування системи.

Синтез, або ***структурний синтез, є центральною ланкою створення системи управління. Він включає наступні компоненти:***

1. *Синтез структури управляємої системи;*

2. Синтез структури управляючої системи;

3. Синтез структури системи передачі та обробки інформації.

1. ***Синтез структури управляємої системи***, тобто визначення оптимального складу і взаємозв'язків елементів системи, оптимальна розбивка безлічі управляємих об'єктів на окремі підмножини, що володіють заданими характеристиками зв'язків.

2. ***Синтез структури управляючої системи***:

а) вибір числа рівнів і підсистем (ієрархії системи);

б) вибір принципів організації управління, тобто встановлення між рівнями правильних взаємин (це пов'язано з узгодженням цілей підсистем різних рівнів і оптимальним стимулюванням їх роботи, розподілом прав і відповідальності, створенням контурів прийняття рішень);

в) оптимальний розподіл виконуваних функцій між людьми і засобами обчислювальної техніки;

г) вибір організаційної ієрархії.

3. ***Синтез структури системи передачі та обробки інформації*** - це:

а) синтез структури системи передачі та обробки інформації;

б) синтез структури інформаційно-керуючого комплексу (в тому числі розміщення пунктів обслуговування).

Синтез структури системи передачі та обробки інформації є відповідальний багатокроковий процес, що включає послідовне вирішення таких основних завдань:

• формування задуму і цілі створення системи управління;

• формування варіантів нової системи;

• приведення описів варіантів системи у взаємне відповідність;

• оцінка ефективності варіантів і прийняття рішення про вибір варіанта нової системи;

• розробка вимог до системи управління;

• розробка програм реалізації вимог до системи управління;

• реалізація розроблених вимог до системи управління.

Формування задуму і цілі створення системи управління. Задум виникає на підставі отриманого завдання, виділення недоліків існуючої системи управління, появи практичної потреби або нових наукових досягнень.

Результатами виконання завдання формування задуму і цілі створення системи повинні бути:

• визначення призначення системи управління;

• визначення мети (цільової функції);

• визначення завдань системи;

• формулювання основної ідеї створення системи;

• визначення напрямків розробки системи.

Формування варіантів нової системи. Варіанти системи формуються на основі аналізу загальної мети створення системи, вивчення суспільних потреб, передбачуваного обсягу задоволення цих потреб, вивчення стану та перспектив розвитку аналогічних вітчизняних і зарубіжних систем.

Процес формування кожного варіанта нової системи може бути описаний *концептуальною і математичною моделями*.

При побудові концептуальної моделі можна виділити кілька етапів:

1. Визначення рівня деталізації концептуальної моделі варіанту системи;

2. Локалізація концептуальної моделі (встановлення меж взаємодії зі іншою системою) шляхом подання зовнішнього середовища у вигляді генераторів зовнішніх впливів, причому ці генератори включаються до складу системи в якості її елементів;

3. Завершення побудови структури моделі із зазначенням зв'язків між складовими її елементами (зв'язку можуть бути розділені на речові та інформаційні). Кожен варіант формування системи включає **різні види описів**: ***структурний (морфологічний), функціональний, інформаційний та параметричний***.

Структурний опис включає опис структури і видів забезпечення системи управління, призначення, складу і розміщення її елементів.

Функціональний опис включає завдання, які вирішуються системою і порядок функціонування системи.

Інформаційний опис включає опис вхідної та вихідної інформації, потоків інформації, що циркулює в системі, способів їх подання і передачі.

Параметричний опис включає перелік кількісних показників (параметрів), що характеризують окремі властивості системи, які необхідно забезпечити в процесі її створення.

Вимоги до показників у вигляді різних обмежень формуються в процесі оцінки ефективності кожного досліджуваного варіанту системи і уточнюються при її проектуванні (розробці, поліпшенню).

4. Визначення управляємих характеристик, тобто в модель повинні увійти ті параметри (показники) системи, що допускають варіювання своїх значень в процесі моделювання. забезпечать перебування (цікавлять розробника) моделей характеристик при конкретних зовнішніх впливах на заданому часовому інтервалі функціонування системи. Інші параметри необхідно ввести в обмеження. Бажано, щоб в концептуальної моделі були конкретизовані всі вирішальні правила або алгоритми управління елементами і (або) процесами моделі, які відображають статику системи.

5. Опис динаміки системи. Отриману раніше модель необхідно доповнити описом функціонування системи. Слід зазначити, що в складних системах часто протікає кілька процесів одночасно. Кожен процес являє собою певну послідовність окремих елементарних операцій, частина яких може виконуватися паралельно різними елементами (ресурсами) системи.

Приведення описів варіантів системи у взаємну відповідність включає;

• *зіставлення описів (структурного, функціонального, інформаційного, параметричного);*

• *усунення протиріч;*

• *об'єднання названих описів.*

- ***Зіставлення описів***. Виконання вимог інформаційного опису забезпечується морфологічно (структурно) і функціонально. Всі блоки структурного опису повинні бути охоплені функціональним описом, містити способи і формули для обчислення всіх вихідних і проміжних параметрів.

На підставі морфологічного і функціонального опису обчислюються параметри, що входять в параметричне опис.

- ***Усунення протиріч***. Виявлення сутності протиріччя вимагає аналізу морфологічних та інформаційних властивостей системи. Усунення протиріччя шляхом компромісу, щоб загальна їх поєднання було задовільним. Включення

нових ідей, тобто включення в систему підсистем або елементів з принципово новими властивостями, радикальна перебудова структури і зв'язків, створення нових процесів і т. д. Етап є багатокроковим і закінчується новим описом системи.

- ***Складання єдиного опису***, що охоплює морфологічні, функціональні, інформаційні властивості і параметри.

Оцінка ефективності варіантів і прийняття рішення про вибір варіанта нової системи. Рішення даного завдання включає:

• визначення значень обраних показників ефективності кожного досліджуваного варіанту створюваної системи;

• порівняльну оцінку ефективності, яка проводиться відповідно до заданого правилом переваг і встановленим критерієм;

• прийняття рішення про вибір найкращого варіанту системи.

Після вибору остаточного варіанту системи уточнюється критерій ефективності системи, формується вихідний варіант значень показників системи управління і проводиться повторний синтез системи який набуває щораз більшої визначеності.

Розробка вимог до системи управління. Вимоги формуються у вигляді кількісно-якісних показників до істотних властивостей системи, що визначає ситуацію або область ситуації в n-вимірному просторі, яка повинна бути досягнута при функціонуванні системи (її величина обумовлюється кількістю виділених істотних властивостей об'єкта). Як правило, вимоги задаються у вигляді обмеження на допустимі межі значень показників.

Розробка вимог проводиться в процесі вирішення всіх перерахованих вище завдань. Загальні вимоги до системи управління документально оформляються, а потім уточнюються окремі вимоги до її елементів, включаючи елементи, що виділяються при морфологічному (структурному), функціональному, інформаційному і параметричної описі системи.

Розробка програм реалізації вимог до системи управління. Зазвичай програма або план реалізації вимог включає:

• перелік цілей і завдань (завдань) виконавцям (відповідальним за створення системи управління), розгорнутих у часі, взаємопов'язаних по відношенню до загальної мети створення нової системи і збалансованих за ресурсами і відношенню до загальної мети створення нової системи;

• графік (порядок) забезпечення виконавців ресурсами (інформаційними, матеріальними, енергетичними та ін.).

Збалансованість по ресурсах означає, що немає завдань, які не забезпечені ресурсами, і що обмежені ресурси раціонально розподілені між усіма виконавцями.

Реалізація розроблених вимог до системи управління. Метою завдання є реалізація розроблених вимог до системи управління в задані терміни, відповідно до розробленої програми.

Умовні етапи реалізації розроблених вимог до людино-машинної (ергатичної) системи управління:

- моделювання (математичне, фізичне, сценарна) підсистем та системи в цілому;
- макетування системи;
- проектування системи;
- конструювання системи;
- виготовлення системи;
- випробування системи;
- оцінка шляхів модернізації;
- повернення до аналізу задуму створення системи та перспектив його розвитку в зв'язку зі створенням нової системи.

Оцінка шляхів модернізації. Основою продовження життєвого циклу системи є її своєчасна і неодноразова модернізація, ідеї якої закладаються на етапі створення системи.

Виявлення сукупності цих відносин, встановлення взаємозв'язків властивостей системи і процесів, їх показників є найважливішим завданням дослідження систем управління.

Різновиди синтезу. Сутністю інформаційного синтезу є обґрунтування необхідного обсягу і форм подання інформації, методів і засобів її передачі, обробки, зберігання, введення і виведення для розроблюваної структури і алгоритму функціонування СУ. Інформаційний синтез доповнює завдання функціонального аналізу, що здійснюється з метою визначення необхідних якісних і кількісних характеристик інформації в СУ.

Сутністю параметричного синтезу є обґрунтування необхідної і достатньої сукупності показників, що дозволяють оцінювати бажані властивості розроблюваної системи та її сумарний ефект. Мета параметричного синтезу - комплексне визначення узгоджених і збалансованих за рівнями дослідження системи необхідних значень її показників, включаючи загальні показники ефективності управління, а також приватні показники структури, процесів функціонування інформації.

Сутністю структурного синтезу є розробка (створення, вдосконалення, реорганізація та організація системи), яка повинна володіти бажаними властивостями. Він проводиться з метою обґрунтування безлічі елементів структури, відносин і зв'язків, що забезпечують в сукупності максимальну відповідність заданим вимогам. Об'єктами дослідження структурного синтезу є різні варіанти розробки (вдосконалення) структур системи управління.

Сутністю функціонального синтезу є обґрунтування динамічних характеристик СУ, які повинні володіти бажаними властивостями. Метою функціонального синтезу є обґрунтування оптимальних або раціональних характеристик процесів функціонування системи управління, тобто процесів зміни її станів з плином часу відповідно до поставленої мети.

Основні принципи, види, рівні аналізу і синтезу.В основу дослідження, використання і створення складних систем управління покладені **три основних принципа аналізу і синтезу**: ***принцип фізичності; принцип моделювання; принцип цілеспрямованості.***

Виділяють наступні **види аналізу і синтезу систем управління**:

- **структурний аналіз і синтез систем управління;**

- **функціональний аналіз і синтез систем управління;**
- **інформаційний аналіз і синтез систем управління;**
- **параметричний аналіз і синтез систем управління.**

Системний підхід вимагає багаторівневого вивчення системи управління. Виділяються такі **рівні аналізу і синтезу систем управління**: ***зовнішній, вихідний, загальносистемний, системний.***

На зовнішньому рівні аналізується система організації , до складу якої входить досліджувана система управління (СУ). В процесі дослідження системи: визначаються цілі та завдання системи; виділяються підсистеми (функції, завдання), в інтересах яких застосовується СУ; уточнюються показники і критерії даних підсистем системи організації; визначаються зовнішні властивості і відповідні показники системи управління, які можуть вплинути на ефективність системи організації в цілому.

На початковому рівні досліджувана СУ виділяється як окремий елемент системи, яка включає різні, в тому числі і протилежні за інтересами, підсистеми. Основні завдання дослідження на початковому рівні, це: виділення досліджуваної системи у вигляді окремого цілеспрямованого елемента; виявлення вхідних напрямів забезпечення і помехових впливів від різних підсистем; встановлення показників і критеріїв ефективності, які характеризують зовнішні властивості СУ і її вплив на систему.

На загальносистемному рівні основними завданнями дослідження є: декомпозиція СУ на управляючу систему і об'єкт управління; формування управлінських впливів; визначення показників, які розкривають структуру системи і ефективність цих впливів.

Питання для самоконтролю

1. У чому полягає кінцева мета системного аналізу?
2. Перелічіть основні завдання, які вирішуються системним аналізом.

3. Які існують групи методів системного аналізу при дослідженні систем управління (ІС)?

4. Покажіть варіант моделі проблемної ситуації щодо захисту інформації.

5. Наведіть схему компонентів, що входять в модель діяльності СОІБ.

6. У чому полягає сутність і зміст інформаційного аналізу систем управління?

7. У чому полягає сутність і зміст інформаційного синтезу систем управління?

8. Які цілі синтезу систем управління?

9. Опишіть завдання синтезу систем управління.

3.3. Застосування методу аналізу ієрархій в системному аналізі

У сучасних умовах вже неможливо вирішувати складні політичні та організаційні проблеми простим перебором безлічі доступних вхідних даних за допомогою математичних моделей або обчислювальної техніки.

У 1970-х рр. для вирішення цих проблемних завдань Сааті був розроблений метод аналізу ієрархій (МАІ).

Цей метод являє собою теорію, яка базується на експертних оцінках і судженнях індивідуальних учасників або груп.

МАІ дозволяє особі, що приймає рішення (ОПР), структурувати складну проблему у вигляді ієрархії і виконувати кількісну оцінку наявних варіантів вирішення (альтернатив).

Широке застосування в світовій практиці МАІ знайшов при вирішенні завдань: професійний відбір, планування ефективного навчання, розподіл кадрів, атестація фахівців і просування персоналу по службі.

3.3.1. Особливості застосування методу аналізу ієрархій

МАІ доцільно також застосовувати і в сфері інформаційної безпеки.

В основі МАІ лежать використовувані людиною в процесі пізнання декомпозиція і синтез, за допомогою яких створюється структура завдання прийняття рішення (ПР) - ієрархія. У вершині ієрархії в МАІ розташовується основна мета, далі, на рівень нижче - підцілі, і, нарешті, на самому нижньому рівні - альтернативи, серед яких проводиться вибір або ранжування. Для процесу парного зважування експертом елементів ієрархії в МАІ використовується інтуїтивно обґрунтована якісна шкала.

Завдання, для вирішення яких може бути застосований МАІ:

- Проблема багатокритеріального вибору. Вибір однієї альтернативи з наявного набору альтернатив на основі деяких критеріїв.
- Ранжування. Багатокритеріальне упорядкування заданої множини альтернатив.
- Визначення пріоритетів альтернатив і критеріїв в задачах багатокритеріального вибору.
- Розподіл ресурсів. Розподіл ресурсів між альтернативами із заданої множини.
- Порівняльний аналіз. Розробка рекомендацій щодо оптимізації внутрішніх процесів організації на основі успішного досвіду конкурентів.
- Управління якістю. Аналіз різних аспектів якості та шляхи поліпшення якості.
- Рішення складних проблем:
- Вибір спеціалізації при навчанні в університеті.
- Прийняття рішення про місце розташування підприємств
- Оцінка ризиків, пов'язаних з функціонуванням компаній.
- Сфера освіти та наукових досліджень.

Основне застосування методу - підтримка прийняття рішень за допомогою ієрархічної композиції завдання і рейтингування альтернативних рішень.

Метод аналізу ієрархій під час прийняття рішень включає:

1. Подання завдання в ієрархічній формі. Завдання формалізується у вигляді ієрархічної структури з кількома рівнями: цілі-критерії-альтернативи (див. Рис.).

2. Парні порівняння і складання матриці порівнянь. Особа, яка приймає рішення (ОПР) порівнює попарно елементи кожного рівня. Результати порівнянь переводяться в числа.

3.Нормалізація матриці порівнянь.

4.Оцінка переваг (привабливості) і обчислення вектора пріоритетів для елементів кожного рівня.

5. Підрахунок кількісного індикатора переваг (привабливості) кожної з альтернатив і визначається найкраща альтернатива.

6. Перевірка узгодженості оцінок (результатів).

1. Подання завдання в ієрархічній формі.

Визначення кількості та змісту рівнів ієрархії.

- 0-й - цілі аналізу.
- 1-й - критерії оцінки (можна додати ще кілька рівнів, оскільки кожен критерій може складатися з підкритеріїв - більш приватних і конкретних).
- 2-й - це альтернативи, з яких робиться вибір.

Приклад варіанту побудови ієрархічної структури вибору системи, найбільш підходящою для зберігання великих обсягів інформації (для вирішення МАІ)- на рис.3.13.

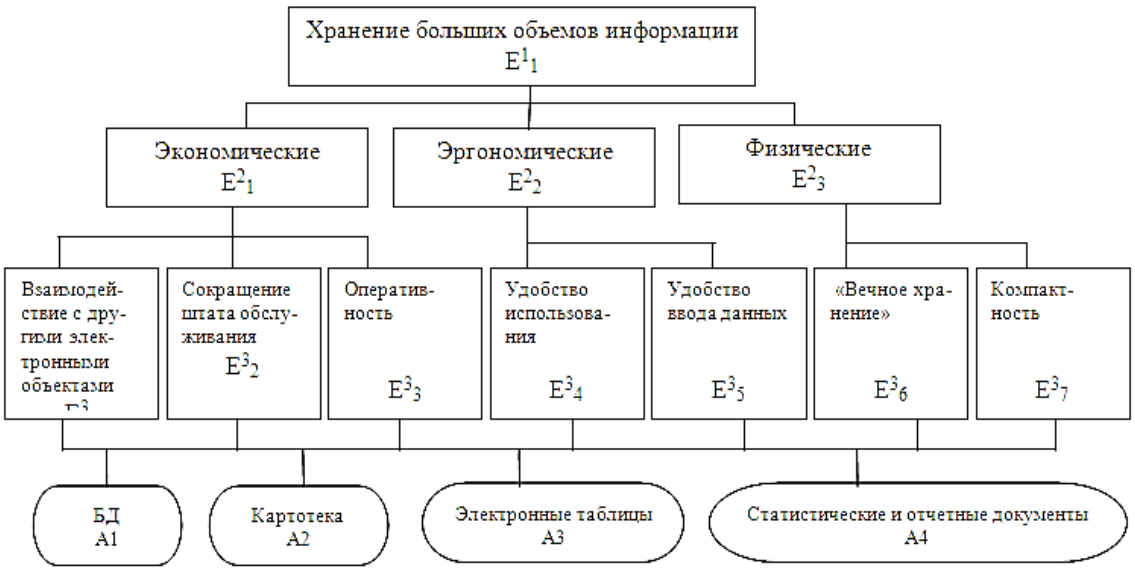
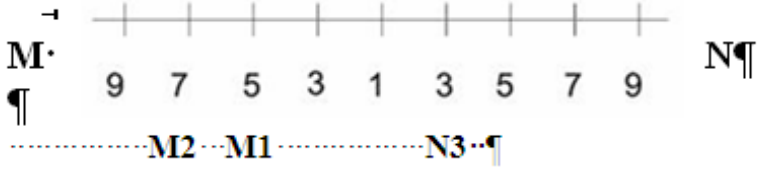


Рис.3.13. Структура критеріїв, показників і альтернатив оцінки зберігання інформації

Е - критерії оцінки завдання. А - можливі альтернативи.

2. Парні порівняння. Це порівняння між собою пари альтернатив, які призначені для вибору в якості прийнятного рішення.

Вибирається шкала для оцінки альтернатив, як правило, від 1 до 10



Кожній альтернативі визначається оцінка переваг.

Для двох альтернатив при порівнянні один з одним виставляються оцінки у вигляді чисел:

- при однаковому високому оцінюванні альтернатив М і N - 1;
- при незначному перевазі М до N - 3;
- при значному перевазі М до N - 5;
- при явно кращому перевагу М до N - 7;
- при абсолютній перевазі М до N - 9.

Можуть бути і проміжні - парні оцінки, що враховують особливості альтернатив.

Зі збільшенням числа альтернатив зростає і число порівнянь, які необхідно провести. Для двох - 1, для трьох - 3. Таблиця нижче показує залежність числа порівнянь від кількості порівнюваних альтернатив.

Кількість альтернатив	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**n**
Кількість порівнянь	**0**	**1**	**3**	**6**	**10**	**15**	**21**	$\frac{n(n-1)}{2}$

Зауваження

• Звичайно, шкала не обов'язково повинна бути від 1 до 9. Важливо, однак, щоб шкала оцінок була, по можливості, простий, інакше це може призвести до плутанини.

• Тут важлива саме парність порівняння. Те, що використовується відносна шкала замість абсолютної - набагато менше шансів допустити помилку.

При визначенні важливостей використовують поснення щодо їх Інтенсивностей , представлених в табл.3.1.

Таблиця 3.1

Визначення важливостей щодо їх Інтенсивностей

Інтенсивності важливості	Визначення	Пояснення
1	Рівна важливість	Досвід та міркування надають легку перевагу одного елемента над другим
3	Незначна перевага одного елемента над другим	Одному елементу надається настільки велике nремайно, що він виявляється практично значущим
5	Важлива чи велика перевага	Очевидність переваги одного елемента над іншим підтверджується досить сильно
7	Значна перевага	Застосовуються у компромісному випадку
9	Дуже велика перевага	Застосовуються у разі зворотного порівняння
2,4,6,8	Проміжні рішення	Досвід та міркування надають легку перевагу одного елемента над другим

Продовження табл. 3.1.

1 /2, 1 /3, 1 /4 1/ 5, 1 /6, 1/ 7, 1 /8, 1 /9	Утримуються при зворотному порівнянні	Одному елементу надається настільки велике премайно, що він виявляється практично значущим

3. Складання матриці порівнянь А. Наприклад, для 3-х альтернатив розмірність матриці буде 3х3. Елементами матриці будуть оцінки, які виставляються при парному порівнянні. Елемент матриці а12 говорить про те, що порівнюються 1 і 2 альтернативи. На головній діагоналі завжди стоятимуть одиниці, оскільки її елементи означають, що альтернатива порівнюється з самим собою.

Для заповнення верхньої трикутної матриці встановлені правила:

• Якщо оцінка знаходиться в лівій частині шкали, то її значення поміщається у відповідний елемент матриці порівнянь без зміни.

• Якщо оцінка знаходиться в правій частині шкали, то її значення поміщається у відповідний елемент матриці порівнянь у вигляді зворотної величини.

Для прикладу трьох альтернатив - дві альтернативи М (зліва шкали) мають оцінки 5 і 7 і одна альтернатива N (праворуч шкали) має оцінку 1/3. При перевагах М1> N3> М2 і наочності за вищенаведеною шкалою.

$$A = \begin{array}{c} \begin{matrix} N3 & M1 & M2 \end{matrix} \\ \begin{bmatrix} 1 & \frac{1}{3} & 5 \\ & 1 & 7 \\ & & 1 \end{bmatrix} \end{array}$$

Для отримання елементів нижньої частини матриці використовується формула. Повністю, матриця порівнянь записується так:

$$A = \begin{array}{c} \begin{matrix} & N3 & M1 & M2 \end{matrix} \\ \begin{matrix} N3 \\ M1 \\ M2 \end{matrix} \begin{bmatrix} 1 & \frac{1}{3} & 5 \\ 3 & 1 & 7 \\ \frac{1}{5} & \frac{1}{7} & 1 \end{bmatrix} \end{array}$$

Всі елементи матриці порівнянь позитивні: $a_{ij} > 0$.

Елементи рядків матриці порівнянь говорять про переваги однієї альтернативи перед іншими. Сума елементів рядка могла б дати оцінку переваг. Але цього робити передчасно, тому що стовпці мають різні ваги.

Обчислення суми елементів кожного стовпця матриці порівнянь:

$$A = \begin{array}{c} \\ N3 \\ M1 \\ M2 \\ Sum \end{array} \begin{array}{c} \begin{array}{ccc} N3 & M1 & M2 \end{array} \\ \begin{bmatrix} 1 & \frac{1}{3} & 5 \\ 3 & 1 & 7 \\ \frac{1}{5} & \frac{1}{7} & 1 \end{bmatrix} \\ \begin{array}{ccc} \frac{23}{5} & \frac{31}{21} & 13 \end{array} \end{array}$$

З матриці видно, що найбільшу вагу при оцінці матимуть елементи 3-го стовпця.

4. Нормалізація матриці порівнянь - шляхом ділення кожного елемента матриці на суму елементів відповідного стовпця.

$$A = \begin{array}{c} \\ N3 \\ M1 \\ M2 \\ Sum \end{array} \begin{array}{c} \begin{array}{ccc} N3 & M1 & M2 \end{array} \\ \begin{bmatrix} \frac{5}{21} & \frac{7}{31} & \frac{5}{13} \\ \frac{15}{21} & \frac{21}{31} & \frac{7}{13} \\ \frac{1}{21} & \frac{3}{31} & \frac{1}{13} \end{bmatrix} \\ \begin{array}{ccc} 1 & 1 & 1 \end{array} \end{array}$$

5.Оценка переваг (привабливості) - Вектор пріоритетів - обчислюється як середнє арифметичне елементів рядків матриці порівнянь.

$$A = \frac{1}{3}\begin{bmatrix} \frac{5}{21} + \frac{7}{31} + \frac{5}{13} \\ \frac{15}{21} + \frac{21}{31} + \frac{7}{13} \\ \frac{1}{21} + \frac{3}{31} + \frac{1}{13} \end{bmatrix} = \begin{bmatrix} 0.2828 \\ 0.6434 \\ 0.0738 \end{bmatrix}$$

Оскільки вектор пріоритетів нормалізований, то сума його елементів дорівнює 1. Вектор пріоритетів показує відносні ваги альтернатив, які порівнюються - що саме краще.

У прикладі найбільш переважними є: **альтернатива М1**, далі - N3 і М2. Можна відзначити, що альтернатива М1 в 2.27 рази (= 64.34 / 28.28) більш привабливим, ніж N3 і в 8.72 (= 64.34 / 7.38) більш, ніж М2.

6. Перевірка узгодженості оцінок.

Про матрицю порівнянь А кажуть, що вона узгоджена, якщо $a_{ij}a_{jk} = a_{ik}$ для будь-яких i, j, k. Однак ідеальною узгодженості домогтися вдається не завжди.

Вважаються узгодженими рішення, які незначно відхиляються від розрахованих за формулою значень $a_{ij}a_{jk} = a_{ik}$.

Індекс узгодженості матриці **А** визначається: $CI = \frac{\lambda_{\max} - n}{n-1}$

У випадку ідеальної узгодженості CI = 0, коли $\lambda_{\max} = n$

де: n - число альтернатив;

$\lambda_{\max}$ - показник узгодження.

Для прикладу визначається множенням суми стовпців початкової матриці А на елементи вектора пріоритетів і складанням їх між собою.

$$\lambda_{max} = \frac{21}{5}(0.2828) + \frac{31}{21}(0.6434) + 13(0.0738) = 3.0967$$

$$CI = \frac{3.0967 - 3}{2} = 0.0484$$

Саати запропонував середнє значення індексу узгодженості для всієї множини матриць, назвавши його **<u>індексом рандомізації</u>** RI і звів в таблицю:

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

і коефіцієнт узгодженості: $CR = \frac{CI}{RI}$.

Якщо коефіцієнт узгодженості не перевищує 10%, то така неузгодженість вважається прийнятною. Якщо ж CR> 10%, то пропонується «переоцінка цінностей», перегляд оцінки переваг ...

В нашем примере $CI = 0.0484$ и RI для $n = 3$ равен 0.58, тогда

$$CR = \frac{CI}{RI} = \frac{0.0484}{0.58} = 8.3\% < 10\%$$.

Тобто всі отримані оцінки можна вважати узгодженими.

3.3.2. Метод аналізу ієрархій у вірішенні завдань

Вирішення завдань за допомогою Excel (додаток Microsoft)

Задача 1 - для двох рівнів ієрархії: за вибором з трьох альтернатив за вісьмома критеріями порівняння

За MAI обґрунтуйте вибір одного найкращого засобу вимірювання з трьох варіантів:

• варіант 1 - високочастотний аналоговий прилад з візуальним відліком (В1);

• варіант 2 - цифровий прилад (В2);

• варіант 3 - багатофункціональна напівавтоматична установка з виведенням інформації на екран (В3).

Кожна альтернатива оцінюється по безлічі критеріїв:

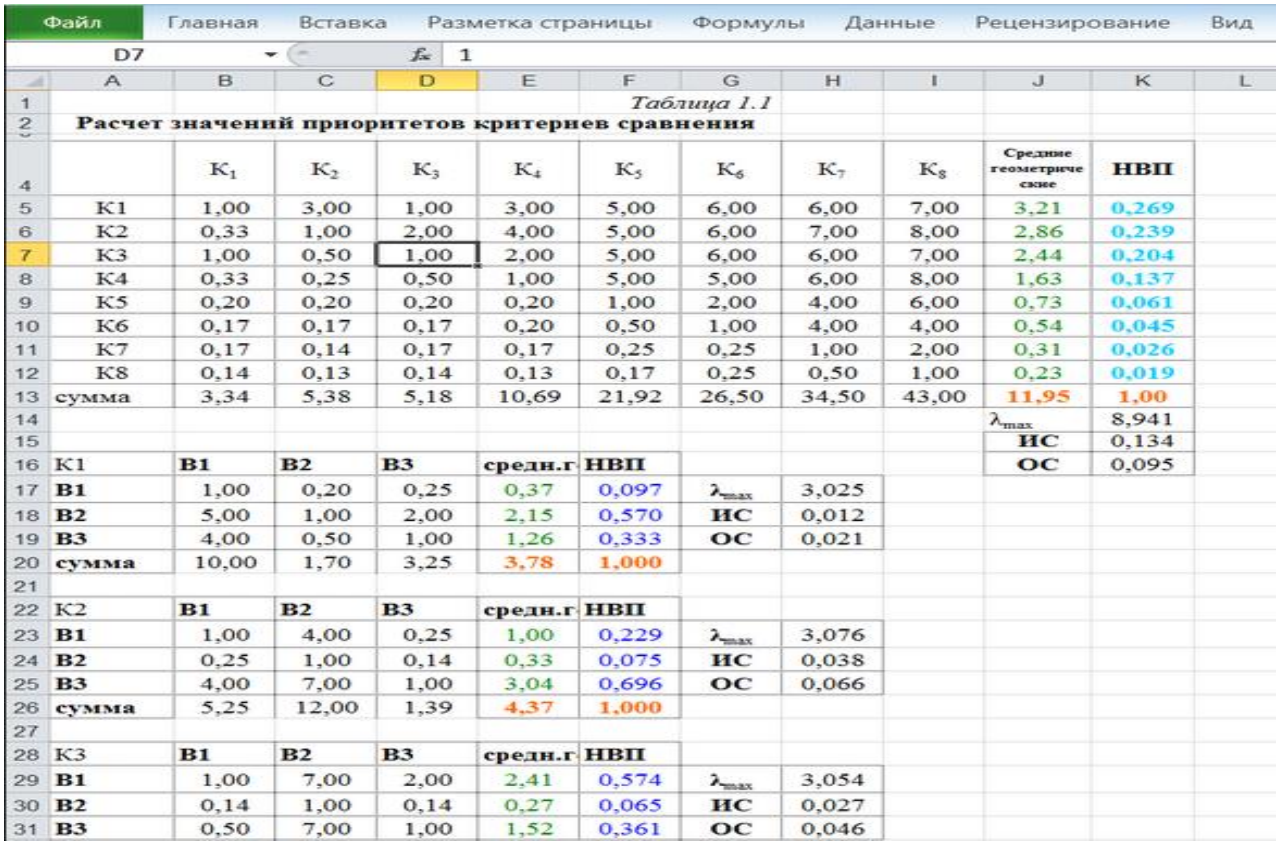
• точність (К1), діапазон (К2),

• швидкодія (К3), універсальність (К4),

• інтенсивність експлуатації (К5), вартість (К6),

• простота і зручність експлуатації (К7), габарити (К8).

Відповідь по задачі 1 - для двох рівнів ієрархії: за вибором з трьох альтернатив за вісьмома критеріями порівняння (http://vamocenka.ru/metod-analiza-ierarxij-primer-rascheta-excel/).



Файл | Главная | Вставка | Разметка страницы | Формулы | Данные | Рецензирование | Вид

D7 | 1

Таблица 1.1

Расчет значений приоритетов критериев сравнения

		K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	Средние геометрические	НВП
5	К1	1,00	3,00	1,00	3,00	5,00	6,00	6,00	7,00	3,21	0,269
6	К2	0,33	1,00	2,00	4,00	5,00	6,00	7,00	8,00	2,86	0,239
7	К3	1,00	0,50	1,00	2,00	5,00	6,00	6,00	7,00	2,44	0,204
8	К4	0,33	0,25	0,50	1,00	5,00	5,00	6,00	8,00	1,63	0,137
9	К5	0,20	0,20	0,20	0,20	1,00	2,00	4,00	6,00	0,73	0,061
10	К6	0,17	0,17	0,17	0,20	0,50	1,00	4,00	4,00	0,54	0,045
11	К7	0,17	0,14	0,17	0,17	0,25	0,25	1,00	2,00	0,31	0,026
12	К8	0,14	0,13	0,14	0,13	0,17	0,25	0,50	1,00	0,23	0,019
13	сумма	3,34	5,38	5,18	10,69	21,92	26,50	34,50	43,00	11,95	1,00
14										λ_{max}	8,941
15										ИС	0,134
16	К1	В1	В2	В3	средн.г	НВП				ОС	0,095
17	В1	1,00	0,20	0,25	0,37	0,097	λ_{max}	3,025			
18	В2	5,00	1,00	2,00	2,15	0,570	ИС	0,012			
19	В3	4,00	0,50	1,00	1,26	0,333	ОС	0,021			
20	сумма	10,00	1,70	3,25	3,78	1,000					
21											
22	К2	В1	В2	В3	средн.г	НВП					
23	В1	1,00	4,00	0,25	1,00	0,229	λ_{max}	3,076			
24	В2	0,25	1,00	0,14	0,33	0,075	ИС	0,038			
25	В3	4,00	7,00	1,00	3,04	0,696	ОС	0,066			
26	сумма	5,25	12,00	1,39	4,37	1,000					
27											
28	К3	В1	В2	В3	средн.г	НВП					
29	В1	1,00	7,00	2,00	2,41	0,574	λ_{max}	3,054			
30	В2	0,14	1,00	0,14	0,27	0,065	ИС	0,027			
31	В3	0,50	7,00	1,00	1,52	0,361	ОС	0,046			

Відповідь задачі 1 (для самоперевірки): Найкращим засобом вимірювання є багатофункціональна напівавтоматична установка з виведенням інформації на екран (варіант 3) з підсумковим значенням пріоритетів альтернатив, рівним 0,397; менш кращий високочастотний аналоговий прилад з візуальним відліком (варіант 1) з підсумковим значенням пріоритетів альтернатив, рівним 0,338; найменш кращий цифровий прилад з підсумковим значенням пріоритетів альтернатив, рівним 0,265.

Питання для самоконтролю

1. Ким і коли був розроблений метод аналізу ієрархій (MAI)

2. Де застосовується МАІ в світовій практиці ?

3. Для вирішення яких завдань може бути застосований МАІ?

4. Яка послідовність дій при використанні МАІ під час прийняття рішень?

5. За якими програмними засобами можна використовувати МАІ в дослідженнях на практиці?

6. Приведіть порядок рішення задачі за допомогою програми MPRIORITY 1.0.

Завдання на самостійну роботу

Вирішити задачу. Необхідно вибрати один з варіантів програмного забезпечення (ПЗ) для підвищення безпеки комп'ютерної системи. Нехай існують два варіанти такого ПЗ: А і Б. Як критерії відбору ПЗ приймаються:

1. Вартість.
2. Супровід розробниками.
3. Інтерфейс.
4. Надані функції.

Супровід розробниками (наприклад, безкоштовна технічна підтримка, навчання персоналу) при виборі програмного забезпечення (ПЗ) оцінюються як помітно більш важливі в порівнянні з характеристиками призначеного для користувача інтерфейсу. Ще більш важливим критерієм є можливості (функції), які надаються ПЗ . Але основним при прийнятті рішення все ж є **вартість**.

Припустимо**, А - це дорога система** з широким набором функцій користувача, зручним призначеним для користувача інтерфейсом, супроводжувана розробниками, а **система Б** - проста і недорога розробка.

Купівля якого ПЗ буде більш кращою відповіддю до зазначених критеріїв?

3.4. Застосування мережевого графіку в системному аналізі

Мережевий графік — це динамічна модель виробничого процесу, що відображає технологічну залежність і послідовність виконання комплексу робіт, що погоджує їх звершення в часі з урахуванням витрат ресурсів і вартості робіт з виділенням при цьому вузьких (критичних) місць.

У практичному плані застосування мережевого підходу в логістиці дає можливість використовувати графічні методи планування в поєднанні з елементами імовірнісних моделей розподілу тривалостей окремих етапів робіт.

Система мережевого планування і управління (СПУ) - сукупність науково обґрунтованих положень організації і управління виробництвом, що базується на моделюванні процесу за допомогою сітьового графіка на базі застосування теорії графів, теорії ймовірностей і комп'ютерних технологій.

Система СПУ дозволяє формувати календарний план реалізації складного комплексу робіт, визначати і мобілізувати резерви часу, попереджати можливі зриви в ході робіт, здійснювати оперативну коригування планів.

В даний час можливе застосування СПУ як у формі одноразового використання сітьових методів і моделей, так і у формі постійно діючої системи СПУ як складової частини більш складних систем управління. У цьому випадку методи СПУ поєднуються із застосуванням ряду економіко-математичних методів.

3.4.1. Способи обчислення параметрів мережевих графіків комплексу робіт

Структури можуть відображати порядок дії (виконувані завдання, заходи, процеси) в організації - для технічної системи (телефонна, електрична мережа і т. п.), при виробництві продукції - мережевий графік, при проектуванні - мережева модель, при плануванні - мережевий план і т. д.).

Мережева модель - це мережа, що моделює комплекс робіт.

У вигляді мережевих моделей можуть бути представлені методики системного аналізу. Мережеві графіки дозволяють відобразити розмаїття взаємозв'язків і послідовність виконання робіт відповідно до прийнятих методами їх виконання, містять необхідну інформацію і є інструментом для знаходження найкращого варіанту. Мережеві моделі будуються в основному на початковому етапі планування. Після їх оцінки складається (зшивається) мережевий графік.

Методи обчислень на мережевий моделі - це мережевий графік, матричний і табличний метод) Як правило мережева структура являє собою декомпозицію системи в часі.

Мережа в цьому випадку - це графічне відображення комплексу робіт.

Основними елементами мережі тут є події і роботи.

Подія - це момент завершення процесу, що відображає окремий етап виконання проекту. Комплекс робіт починається з вихідного і закінчується завершальною подією.

Робота - це протяжний у часі процес, необхідний для здійснення події і, як правило, вимагає витрат ресурсів.

Події на мережевому графіку зазвичай зображуються кружками, а роботи - дугами, що з'єднують події. Всі дуги роботи повинні бути спрямовані зліва направо. Над дугами проставляються тривалості робіт.

Подія може здійснитися тільки тоді, коли закінчаться всі роботи, йому передують.

У мережевому графіку не повинно бути "тупикових" подій, (за винятком завершального), не повинно бути подій, яким не передує хоча б одна робота (крім вихідного), не повинно бути замкнутих контурів і петель, а також паралельних робіт.

Спосіб обчислення часових характеристик подій - за допомогою формул

Нехай задана наступна послідовність робіт з їх тимчасовими характеристиками (табл.3.2).

Таблиця 3.2.

Робота	**1-2**	**1-3**	**1-4**	**2-5**	**3-4**	**3-6**	**4-5**	**4-6**	**4-7**
Діяльність	**10**	**4**	**6**	**9**	**7**	**8**	**3**	**10**	**4**
Робота	**5-8**	**6-7**	**6-9**	**7-8**	**7-10**	**7-9**	**8-10**	**9-10**	
Діяльність	**5**	**9**	**7**	**12**	**8**	**6**	**9**	**11**	

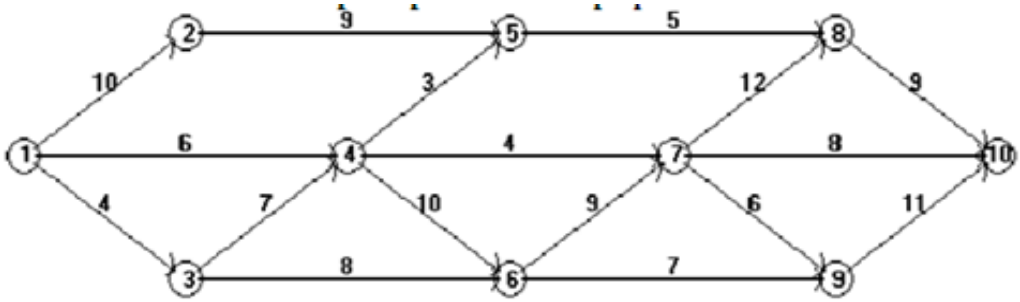


Рис.3.14. Мережевий графік прикладу

Шлях - будь-яка послідовність робіт, в якій кінцева подія кожної роботи збігається з початковим подією наступного за нею роботи.

Повний шлях - будь-який шлях, початок якого збігається з вихідним подією мережі, а кінець - із завершальним.

Критичний шлях представляє собою найбільш тривалий повний шлях в мережевому графіку - шлях від початкової до кінцевої роботи, який має найбільшу тривалість. Критичними також називаються роботи і події розташовані на цьому шляху. Роботи цього шляху визначають загальний цикл завершення всього комплексу робіт, що плануються за допомогою мережевого графіка. І для скорочення загальної тривалості робіт необхідно в першу чергу скорочувати час виконання робіт, що лежать на критичному шляху. Будь-яке уповільнення у виконанні робіт критичного шляху неминуче призведе до зриву виконання всього комплексу робіт, тому критичного шляху приділяється особлива увага.

Основні поняття, пов'язані з критичним шляхом.

Ранній термін настання події (ET). Він визначається для кожної події при русі по мережі зліва направо від початкового до кінцевого події. Для початкового події ET = 0.

Для інших визначається за формулою, де ETj- ранній термін настання події i, що передує події j; tij - тривалість роботи (ij). $ET_j = \max_i \left\{ ET_i + t_{ij} \right\}$.

Пізній термін настання події (LTi) - це найбільш пізній термін, в який може наступити подія без затримки виконання всього комплексу робіт. Визначається він при русі по мережі праворуч наліво від кінцевого події до початкового за формулою: $LT_i = \min_j \left\{ LT_j - t_{ij} \right\}$.

Для критичного шляху ранні і пізні терміни настання подій збігаються. Для кінцевого події ця величина дорівнює довжині критичного шляху. Розрахунок показників мережевого графіка можна проводити безпосередньо по вищенаведеним формулам. Спочатку треба знайти ранні терміни настання подій (при русі по мережі зліва направо, від початку до кінця).і т. д. до 10.

$$ET_1 = 0.$$

$$ET_2 = ET_1 + t_{12} = 0 + 10 = 10.$$

$$ET_3 = ET_1 + t_{13} = 0 + 4 = 4.$$

$$ET_4 = \max\left(ET_1 + t_{14}; ET_3 + t_{34}\right) = \left(0 + 7; 4 + 7\right) = 11.$$

$$ET_5 = \max\left(ET_2 + t_{25}; ET_4 + t_{45}\right) = \left(10 + 9; 11 + 3\right) = 19.$$

$$ET_6 = \max\left(ET_3 + t_{36}; ET_4 + t_{46}\right) = \left(4 + 8; 11 + 10\right) = 21$$

Потім розрахунки виконати в зворотному напрямку і знайти пізні терміни настання подій.

Покласти ET10 = LT10.

$$LT_6 = \min\left\{LT_7 - t_{67}; LT_9 - t_{69}\right\} = \left\{30 - 9; 40 - 7\right\} = 21$$

$$LT_7 = \min\left\{LT_8 - t_{78}; LT_{10} - t_{7,10}; LT_9 - 7,9\right\} = \left\{42 - 12; 51 - 8; 40 - 6\right\} = 30.$$

$$LT_8 = LT_{10} - t_{8,9} = 51 - 9 = 42,$$

$$LT_9 = LT_{10} - t_{9,10} = 51 - 11 = 40.$$ и т.д.

Існує **інший спосіб обчислення тимчасових характеристик подій -в вигляді таблиці.**

Події відзначаються в квадратах "головною" діагоналі. Роботи відзначаються двічі в верхніх і нижніх "побічних" квадратах відносно головною діагоналі таблиці.

У верхніх "побічних" квадратах таблиці номер рядка відповідає попередньому події, номер стовпця - наступного.

В нижніх "побічних" квадратах навпаки.

Порядок заповнення табл.3.3.

1. Спочатку заповнюються чисельники верхніх і нижніх побічних квадратів. У них записуються тривалості відповідних робіт.

2. Заповнюються знаменники верхніх "побічних" квадратів як суми чисельника головного квадрата і чисельника верхнього "побічного" в тому ж рядку.

3. Чисельник першого головного квадрата приймається рівним нулю, чисельники інших головних квадратів рівні максимуму знаменників верхніх "побічних" квадратів в тому ж стовпці.

4. Знаменник останнього головного квадрата приймається рівним чисельнику цього квадрата. Знаменники нижніх "побічних" квадратів рівні різниці знаменника головного і чисельника "нижнього" побічного в тому ж рядку.

5. Знаменники головних квадратів рівні мінімуму знаменників "нижніх» побічних в тому самому стовпці.

Розрахунок показників мережевого графіка (тимчасових характеристик подій)

Таблиця 3.3

	1	2	3	4	5	6	7	8	9	10
1	0 / 0	10 / 10	4 / 4	6 / 6						
2	10 / 18	10 / 28			9 / 19					
3	4 / 0		4 / 4	7 / 11		8 / 12				
4	6 / 5		7 / 4	11 / 11	3 / 14	10 / 21	4 / 15			
5		9 / 28		3 / 34	19 / 37			5 / 24		
6			8 / 13	10 / 11		21 / 21	9 / 30		7 / 28	
7				4 / 26		9 / 21	30 / 30	12 / 42	6 / 36	8 / 38
8					5 / 37		12 / 30	42 / 42		9 / 51
9						7 / 33	6 / 34		36 / 40	11 / 47
10							8 / 43	9 / 42	11 / 40	51 / 51

З табл.3.3 знаходяться тимчасові показники:

1. Ранні терміни настання подій (чисельники головних квадратів).

2. Пізні терміни настання подій (знаменники головних квадратів).

3. Резерви часу подій (різниця між знаменником і чисельником головного квадрата). У нашому випадку критичними подіями (що не мають резервів) є 1, 3, 4, 6, 7, 8, 10. Вони складають критичний шлях.

Тривалість критичного шляху дорівнює 51 (чисельник або знаменник останнього головного квадрата).

4. Ранній термін закінчення робіт (знаменники верхніх "побічних" квадратів).

5. Пізній термін настання робіт (знаменники відповідних нижніх "побічних" квадратів).

6. Загальні резерви часу робіт (різниця між знаменником головного квадрата і знаменником верхнього "побічного" в тому ж стовпці).

7. Вільні резерви часу робіт (різниця між чисельником головного квадрата і знаменником верхнього "побічного" квадрата в тому ж стовпці).

На графіку мережі проставляються над кожною подією зліва - ранній, а праворуч - пізній термін настання події (рис.3.15).

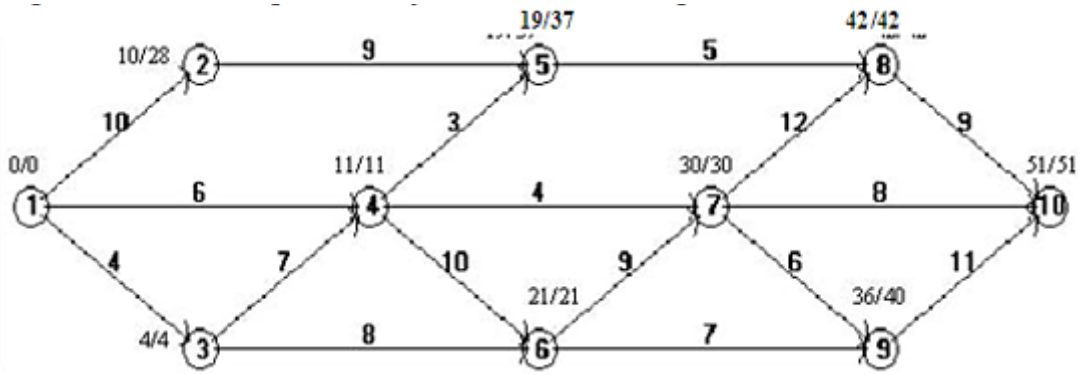


Рис.3.15. Мережевий графік прикладу (з результатами розрахунку)

Таким чином, критичний шлях проходить уздовж робіт 1-3-4-6-7-8-10, і його тривалість дорівнює 51.

Резерв часу події визначається як різниця між їх LT і ET. Ясно, що резерви часу подій вздовж критичного шляху дорівнюють нулю.

Для прикладу резерв часу, наприклад, події 2 дорівнює 28-10 = 18, а події 9 дорівнює 40-36 = 4. На ці проміжки часу може бути затримано виконання відповідних робіт без ризику затримати проект в цілому.

Розрахунок показників мережевого графіка
(тимчасових характеристик робіт)

До **тимчасових характеристик робіт** відносяться:

1. Загальний резерв часу роботи (TS) - визначається зі співвідношення:

$$TSij = LTj - ETi - tij$$

і показує, на скільки можна збільшити тривалість роботи за умови, що термін виконання всього комплексу робіт не зміниться.

2. Вільний резерв часу роботи (FS) визначається зі співвідношення

$$FSij = ETj - ETi - tij$$

і показує частину повного резерву часу, на яке можна збільшити тривалість роботи, не змінивши при цьому раннього терміну її кінцевого події.

Якщо вільний резерв часу робіт може бути використаний по всіх роботах мережі одночасно (тоді всі роботи стають критичними), то для повних резервів цього сказати не можна; його можна використовувати або для однієї роботи шляху повністю, або для різних робіт частинами.

Для критичних робіт TS і FS дорівнюють нулю. TS і FS можуть бути використані при виборі календарних термінів виконання некричних робіт і для часткової оптимізації мережевих графіків.

Остаточно для прикладу маємо результат у табл.3.4 і 3.5.

Таблиця 3.4

Критичний шлях	Тривалість
1-3	4
3-4	7
5-6	10
6-7	9
7-8	12
9-10	9
Спільна	51

Таблиця 3.5

Не критичні праці	Тривалість	Загальний резерв TS	Вільний резерв FS
1-2	10	18	0
1-4	6	5	5
2-5	9	18	0
4-5	3	23	5
3-6	8	9	9
4-7	4	15	15
5-8	5	18	18
6-9	7	12	8
7-9	6	4	0
7-10	8	13	13
9-10	11	4	4

Постановка задачі для самостійного рішення

При виконанні завдання з метою закріплення матеріалу, використовуючи вихідні дані табл.1, підставте замість **n** в табл.3.6 номер свого варіанта (визначає викладач) і отримане число округлити до цілого.

Таблиця 3.6

Вихідні дані

Робота	(1,2)	(1,3)	(1,4)	(2,5)	(2,4)	(3,4)	(3,6)	(4,5)	(4,6)
Тривалість	5+n/3	6+n/3	7+n/3	4+n	8+n/3	3+n	4+n/2	10+n/3	2+n
(4,7)	(5,7)	(5,8)	(6,7)	(6,9)	(7,8)	(7,9)	(7,10)	(8,10)	(9,10)
8+n\3	9+n/2	10+n/3	12+n/2	9+n	7+n/3	5+n	9+n	11+n/2	8+n/3

Потрібно визначити:

1. Ранні терміни настання подій.
2. Пізні терміни настання подій.
3. Резерви часу подій.
4. Критичний шлях.

3.4.2. Рішення задач побудови мережевих моделей в системному аналізі

Для визначення параметрів мережевої моделі за допомогою онлайн-програм можливо ще при використанні програм в розділі **"Мережеві моделі"**, представлених у вигляді онлайн-калькуляторів на сайті https://math.semestr.ru/setm/index.php.

Задача №1

Опис проекту у вигляді переліку виконуваних операцій із зазначенням їх взаємозв'язку

За допомогою онлайн-калькулятора **Параметри мережевої моделі** розраховуються такі показники як ранній і пізній терміни звершення події, резерви часу, критичний шлях (найбільший шлях в мережі) та інші. Вихідні дані зазвичай задаються таблицею.

Приклад рішення онлайн:

Побудува мережевого графіка і визначення критичного шляху

Початкові дані для рішення (приклад)

Операція	Безпосередньо попередня операція	Тривалість
A	-	3
B	-	8
C	A	5
D	B	1
E	C,D	6
F	A	2

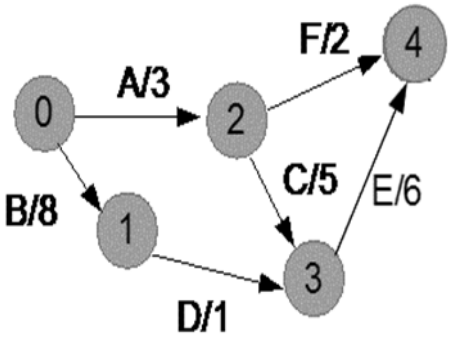


Рис. 3.16. Початкові дані для побудови мережевого графіку

Розрахунок параметрів мережевої моделі

Онлайн-калькулятор призначений для знаходження параметрів мережевої моделі:

• ранній термін звершення події, пізній термін звершення події, ранній термін початку роботи, ранній термін закінчення роботи, пізній термін початку роботи, пізній термін закінчення роботи;

• резерв часу на звершення події, повний резерв часу, вільний резерв часу;

• тривалість критичного і найкоротшого шляху в мережі;

а також дозволяє оцінити ймовірність виконання всього комплексу робіт за задану кількість днів.

Вихідні дані зазвичай задаються за допомогою табл.3.7.

Постановка задачі. Для обраного варіанту треба розрахувати параметри мережного графіка заходи щодо вдосконалення системи управління:

1. Ранні терміни настання подій.
2. Пізні терміни настання подій.
3. Резерви часу подій.
4. Критичний шлях.

Таблиця 3.7.

Тимчасові характеристики мережевої моделі

Робота (i,j)	Кількість наступних робіт	Тривалість	Ранні терміни: початок $t_{ij}^{Р.Н.}$	Ранні терміни: кінець $t_{ij}^{Р.О.}$	Пізні терміни: початок $t_{ij}^{П.Н.}$	Пізні терміни: кінець $t_{ij}^{П.О.}$	Резерви часу: повний $t_{ij}^{П}$	Резерви часу: вільний $t_{ij}^{С.В.}$	Резерви часу: подій R_j
(0,1)	0	8	0	8	0	8	0	0	0
(0,2)	0	3	0	3	1	4	1	0	1
(1,3)	1	1	8	9	8	9	0	0	0
(2,3)	1	5	3	8	4	9	1	1	0
(2,4)	1	2	3	5	13	15	10	10	0
(3,4)	2	6	9	15	9	15	0	0	0

Результати рішення задачі

Критичний шлях: (0,1) (1,3) (3,4). Тривалість критичного шляху: 15.

Незалежний резерв часу роботи RijH - частина повного резерву часу, якщо всі попередні роботи закінчуються в пізні терміни, а всі наступні роботи починаються в ранні терміни.

Використання незалежного резерву часу не впливає на величину резервів часу інших робіт. Незалежні резерви прагнуть використовувати, якщо закінчення попередньої роботи відбулося в пізній допустимий термін, а наступні роботи хочуть виконати в ранні терміни.

Якщо RijH≥0, то така можливість є.

Якщо RijH <0 (величина негативна), то така можливість відсутня, так як попередня робота ще не закінчується, а подальша вже повинна початися (показує час, якого не вистачить у даній роботи для виконання її до самого раннього строку здійснення її (роботи) кінцевого події за умови, що ця робота буде розпочата в найпізніший термін її початкового події).

Фактично незалежний резерв мають лише ті роботи, які не лежать на максимальних шляхах, що проходять через їх початкові і кінцеві події.

Побудова масштабного мережевого графіка

Виконання задачі побудови масштабного мережевого графіка можливе також за допомогою онлайн-сервісу. **"Параметри мережевої моделі". ВІДЕО інструкція рішення задачі в онлайн представлена на сайті https://math.semestr.ru/setm/index.php .**

Як приклади варіантів (для навчання) можна вибрати один з 56 завдань на сайті https://math.semestr.ru/setm/examples_param.php

Постановка задачі.

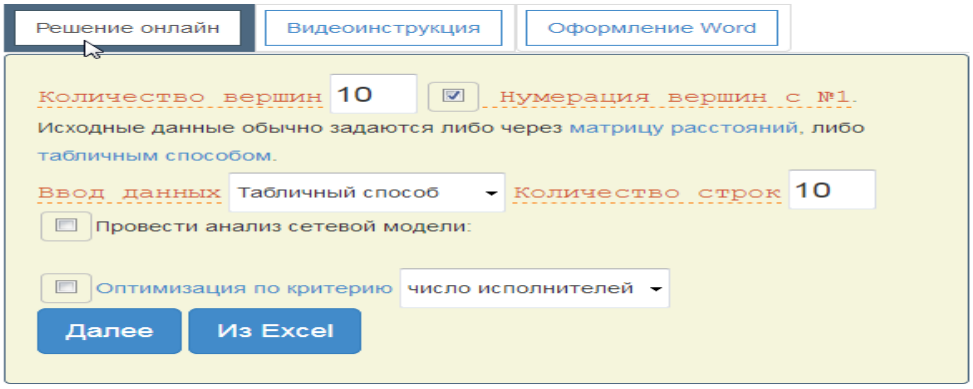
1.Вичісліть табличним методом всі основні тимчасові характеристики робіт і подій, знайти критичний шлях і його тривалість.

2. Побудувати масштабний мережевий графік, аналогічно до розглянутої в прикладі.

3. Оцінити ймовірність виконання всього комплексу робіт за 30 днів.

4. Оцінити максимально можливий термін виконання всього комплексу робіт з імовірністю 95%.

Перейти до онлайн вирішення задачі.



Приклад рішення задачі

Таблиця 3.8

Вихідні дані мережевої моделі

Код роботи (i,j)	Тривалість	
	$t_{min}(i,j)$	$t_{max}(i,j)$
1,2	5	10
1,4	2	7
1,5	1	6
2,3	2	4,5
2,8	9	19
3,4	1	3,5
3,6	9	19
4,7	4	6,5
5,7	2	7
6,8	7	12
7,8	5	7,5

Рішення знаходиться за допомогою сервісу **Мережева модель**. У прикладі задається тривалість виконання роботи двома оцінками - мінімальна і максимальна.

Мінімальна оцінка характеризує тривалість виконання роботи при найбільш сприятливих обставинах, а максимальна tmax (i, j) - при найбільш несприятливих умовах.

Тривалість роботи в цьому випадку розглядається, як випадкова величина, яка в результаті реалізації може прийняти будь-яке значення в заданому інтервалі. Такі оцінки називаються імовірнісними (випадковими), та їх очікуване значення тож (i, j) оцінюється за формулою

$$тож\ (i, j) = (3\ tmin\ (i, j) + 2\ tmax\ (i, j)) / 5$$

Для характеристики ступеня розкиду можливих значень навколо очікуваного рівня використовується показник дисперсії:

$$S2\ (i, j) = 0{,}04\ (tmax\ (i, j) - tmin\ (i, j))\ 2$$

Розрахування очікуваних значень і показників дисперсії:

$t_{ож}(1,2)=(3*5+2*10)/5=7$ $S^2(1,2)=0{,}04*(10-5)^2=1$
$t_{ож}(1,4)=(3*2+2*7)/5=4$ $S^2(1,4)=0{,}04*(7-2)^2=1$
$t_{ож}(1,5)=(3*1+2*6)/5=3$ $S^2(1,5)=0{,}04*(6-1)^2=1$
$t_{ож}(2,3)=(3*2+2*4{,}5)/5=3$ $S^2(2,3)=0{,}04*(4{,}5-1)^2=0{,}25$
$t_{ож}(2,8)=(3*9+2*19)/5=13$ $S^2(2,8)=0{,}04*(19-9)^2=4$
$t_{ож}(3,4)=(3*1+2*3{,}5)/5=2$ $S^2(3,4)=0{,}04*(3{,}5-1)^2=6{,}25$
$t_{ож}(3,6)=(3*9+2*19)/5=13$ $S^2(3,6)=0{,}04*(19-9)^2=4$
$t_{ож}(4,7)=(3*4+2*6{,}5)/5=5$ $S^2(4,7)=0{,}04*(6{,}5-4)^2=0{,}25$
$t_{ож}(5,7)=(3*2+2*7)/5=4$ $S^2(5,7)=0{,}04*(7-2)^2=1$
$t_{ож}(6,8)=(3*7+2*12)/5=9$ $S^2(6,8)=0{,}04*(12-7)^2=1$
$t_{ож}(7,8)=(3*5+2*7{,}5)/5=6$ $S^2(7,8)=0{,}04*(7{,}5-5)^2=0{,}25$

Отримані розрахункові дані заносяться в табл. 3.9.

Таблиця 3.9.

Мережева модель

Код роботи (i,j)	Тривалість		Очікувана тривалість	Дисперсія $S^2(i,j)$
	$t_{min}(i,j)$	$t_{max}(i,j)$		
1,2	5	10	7	1
1,4	2	7	4	1
1,5	1	6	3	1
2,3	2	4,5	3	0.25
2,8	9	19	13	4
3,4	1	3,5	2	6.25
3,6	9	19	13	4
4,7	4	6,5	5	0.25
5,7	2	7	4	1
6,8	7	12	9	1
7,8	5	7,5	6	0.25

Використовуючи отримані дані, можна знайти **табличним методом** основні характеристики мережевої моделі: ***критичний шлях*** і його ***тривалість***, результати - в табл 3.10.

Таблиця 3.10.

Табличний метод розрахунку мережевого графіка

КПР	Код роботи (i,j)	Тривалість роботи (i,j)	Ранні терміни:		Пізні терміни:		Резерви часу	
			$t_{рн}(i,j)$	$t_{ро}(i,j)$	$t_{пн}(i,j)$	$t_{по}(i,j)$	$R_п$	$R_с$
1	2	3	4	5	6	7	8	9
0	1.2	7	0	7	0	7	0	0
0	1.4	4	0	4	17	21	17	8
0	1.5	3	0	3	19	22	19	0
1	2.3	3	7	10	7	10	0	0
1	2.8	13	7	20	19	32	12	12
1	3.4	2	10	12	19	21	9	0
1	3.6	13	10	23	10	23	0	0
2	4.7	5	12	17	21	26	9	0
1	5.7	4	3	7	22	26	19	10
1	6.8	9	2.	32	23	32	0	0
2	7.8	6	17	23	26	32	9	9

Таким чином: Роботи критичного шляху (1,2), (2,3), (3,6), (6,8).

Тривалість критичного шляху Ткр = 32.

Для оцінки ймовірності виконання всього комплексу робіт за 30 днів використовується формула: P (tкр <T) = 0,5 + 0,5 F (Z)

де: Z = (T-Tкр) / Sкр

Z- нормативне відхилення випадкової величини,

Sкр - середньоквадратичне відхилення, яке обчислюється як корінь квадратний з дисперсії тривалості критичного шляху.

F (Z) - функція нормального закону розподілу від величини Z вибирається з табл.3.11.

Таблиця 3.11

Стандартний нормальний розподіл

Z	F(Z)	Z	F(Z)	Z	F(Z)
0	0.0000	1.0	0.6827	2.0	0.9643
0.1	0.0797	1.1	0.7287	2.1	0.9722
0.2	0.1585	1.2	0.7699	2.2	0.9786
0.3	0.2358	1.3	0.8064	2.3	0.9836
0.4	0.3108	1.4	0.8385	2.4	0.9876
0.5	0.3829	1.5	0.8664	2.5	0.9907
0.6	0.4515	1.6	0.8904	2.6	0.9931
0.7	0.5161	1.7	0.9104	2.7	0.9949
0.8	**0.5763**	1.8	0.9281	2.8	0.9963
0.9	0.6319	1.9	0.9545	2.9	0.9973

Розрахунки

Критичний шлях проходить по роботах (1,2) (2,3) (3,6) (3,8).

Дисперсія критичного шляху - S2 (i, j) = 0,04 (tmax (i, j) -tmin (i, j)) 2:

S2¬ (Lкр) = S2 (1,2) + S2 (2,3) + S2 (3,6) + S2 (6,8) = 1 + 0,25 + 4 + 1 = 6,25

S (Lкр) = 2,5

Імовірність того, що весь комплекс робіт буде виконано не більш як за 30 днів

p (tкр <30) = 0,5 + 0,5 F ((30-32) / 2,5) = 0,5-0,5 F (0,8) = 0,5-0,5 * 0 , 5763 = 0,5-0,28815 = 0,213 Або становить 21,3%.

Для визначення максимально можливого терміну виконання всього комплексу робіт з надійністю 95% використовується формула:

T = Tкр + Z * Sкр

Для вирішення поставленого завдання знайдемо значення аргументу Z, яке відповідає заданій ймовірності 95% (значення графи F (Z) - 0,9545 * 100% в табл. Відповідає Z = 1,9).

T = 32 + 1,9 * 2,5 = 36,8

Висновок. Максимальний термін виконання всього комплексу робіт при заданому рівні ймовірності 95% становить всього 36,8 дня.

Питання для самоконтролю

1. Яке призначення мережевої моделі?
2. Що означає: методи обчислень на мережевий моделі?
3. Поясніть: що таке подія і робота в мережевому графіку?
4. Яка різниця між шляхом і критичним шляхом?
5. Як можна разрахувати параметри мережевої моделі?

ТЕМА 4. ОЦІНКА СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

4.1. Оцінка управління економічною та інформаційною безпекою підприємства

Ринкові умови господарювання вимагають якісного оцінювання ефективності функціонування різних економічних суб'єктів. Проте особлива увага приділяється підприємству, яке на сьогоднішній день є основною ланкою народного господарства, що створює конкретні економічні блага, й, відповідно, є першоосновою націо-нального багатства нашої держави. Запорукою ефективного функціонування будь-якого підприємства є прийняття правильних управлінських рішень, що можна забезпечити лише за умов комплексного аналітичного оцінювання всіх сфер діяльності підприємства, факторів його мікро- та макросередовища – економічної діагностики.

Безпека підприємства – це містке, комплексне поняття. У загальному вигляді її можна визначити як відсутність різного роду небезпек і загроз, або наявність можливостей щодо їх попередження, захисту своїх інтересів та недопущення втрат нижче критичної межі.

У процесі антикризового управління за допомогою діагностики визначають: симптоми кризових явищ; стадію й ступінь розвитку кризи; варіанти виходу з кризи і т. д.

Перша стадія кризи – падіння граничної ефективності капіталу, показників ділової активності підприємства, зниження рентабельності й обсягів прибутку, внаслідок чого погіршується фінансовий стан підприємства, скорочуються фінансові можливості розвитку.

Друга стадія кризи – поява збитковості виробництва. Способи розпізнавання кризового стану визначають особливі вимоги до вихідної інформації.

Третя стадія – практична відсутність власних коштів у підприємства (значна частина оборотних коштів направляється на погашення збитків і обслуговування кредиторської заборгованості). Діагностика на цій стадії

акцентує особливу увагу на цінності ознак, що характеризують кризу й рівень ризику при прийнятті управлінських рішень для екстреного варіанта знаходження оборотних коштів.

Четверта стадія – стан гострої неплатоспроможності. Немає можливості профінансувати навіть скорочене відтворення і платежі за попередніми зобов'язаннями. Виникає реальна загроза зупинки або припинення виробництва, а потім і банкрутства. У цій ситуації діагностика з використанням коефіцієнтів платоспроможності й забезпеченості власними оборотними коштами дозволяє встановити фінансову неспроможність і можливість нейтралізувати її через процедуру банкрутства.

Всю сукупність факторів виникнення кризової ситуації в діяльності підприємства можна поділити на дві групи: зовнішні, на які воно не в змозі впливати або його вплив обмежений, та внутрішні, що виникають в результаті діяльності самого підприємства.

За можливістю діагностування та прогнозування фактори виникнення кризової ситуації в діяльності підприємства можна розглядати як такі, що діагностуються; прогнозовані та такі, що не піддаються прогнозуванню.

Боротьба підприємства за виживання в кризових умовах вимагає взаємозв'язку організаційних, правових, фінансових і управлінських аспектів.

Забезпечення економічної безпеки припускає виділення, аналіз та оцінювання існуючих загроз для кожної з функціональних складових і розробку на їх основі системи заходів, що попереджають і протидіють виникненню кризових явищ на підприємстві.

4.1.1. Підходи до оцінки управління економічною та інформаційною безпекою

Аналіз і оцінювання економічної безпеки підприємства виконують у такий послідовності:

- виявлення внутрішніх і зовнішніх факторів, що визначають економічну безпеку підприємства (щодо кожної з функціональних складових), аналіз і оцінювання ступеня їх впливу;
- розрахунок узагальнених показників економічної безпеки для кожної з функціональних складових;
- розрахунок інтегрального показника економічної безпеки підприємства, розробка комплексу заходів, спрямованих на підвищення економічної безпеки, і оцінювання їх ефективності.

Після розрахунку впливу функціональних складових на зміну сукупного критерію економічної безпеки підприємства здійснюють **функціональний аналіз заходів з організації необхідного рівня економічної безпеки підприємства** за окремими складовими в такій послідовності.

1. Визначення структури негативних впливів за функціональними складовими економічної безпеки. Розподіл об'єктивних і суб'єктивних негативних впливів.

2. Фіксація вжитих превентивних заходів для запобігання негативним впливам за всіма функціональними складовими економічної безпеки

3. Оцінювання ефективності вжитих заходів з погляду нейтралізації конкретних негативних впливів за кожною складовою економічної безпеки.

4. Визначення причин недостатньої ефективності заходів, ужитих для подолання вже наявних і можливих негативних впливів на економічну безпеку.

5. Виявлення не усунених і очікуваних негативних впливів на рівень економічної безпеки, а також тих, що можуть з'явитися в майбутньому.

6. Опрацювання рекомендацій щодо усунення існуючих негативних впливів на економічну безпеку й запобігання можливій появі нових.

7. Оцінювання вартості кожного з пропонованих заходів щодо усунення негативних впливів на рівень економічної безпеки й визначення відповідальних за реалізацію таких заходів.

Як показники рівня інформаційної безпеки можуть бути використані **коефіцієнти**:

- ***коефіцієнт повноти інформації (Кпі)*** – розраховується як відношення обсягу інформації, що є в розпорядженні особи, яка приймає рішення (ОПР), і обсягу інформації, необхідної для ухвалення обґрунтованого рішення;

- ***коефіцієнт точності інформації (Кті)*** – розраховується як відношення обсягу релевантної інформації до загального обсягу наявної в розпорядженні ОПР інформації;

- ***коефіцієнт суперечливості інформації (Ксі)*** – розраховується як відношення кількості незалежних свідчень на користь ухвалення рішення до загальної кількості незалежних свідчень у сумарному обсязі релевантної інформації.

Обсяг інформації може бути розрахований у сторінках формату А4, кількості символів тексту, Кбайтах, Мбайтах тощо.

Рівень інформаційної безпеки може бути визначений на основі добутку трьох згаданих коефіцієнтів:

Кі = Кпі*Кті*Ксі.

При цьому, якщо:

***Кі* ≥ 0,7 – рівень безпеки високий;**

0,3 ≤ Кі<0,7 – рівень безпеки середній;

***Кі*<0,3 – рівень безпеки низький.**

Для оцінки управління економічною та інформаційною безпекою на практиці використовують методику аналізу стану економічної безпеки бізнесу підприємства (рис. 4.1).

Рис.4.1. Методика аналізу стану економічної безпеки бізнесу підприємства

4.1.2. Методика оцінки управління економічною та інформаційною безпекою на прикладі

За даними табл.4.1:

- ***розрахувати*** **інтегральну оцінку економічної безпеки підприємства;**
- ***побудувати*** **схему областей економічної безпеки.**

Таблиця 4.1

Вихідні дані для оцінки економічної безпеки підприємства

Назва складової безпеки	Максимальний рівень	Фактичний рівень
Інтелектуальна	3	1
Кадрова	3	2
Технічна	3	3
Правова	3	1
Екологічна	5	4
Інформаційна	3	1
Силова	3	2
Фінансова	5	4
Ринкова	7	4
Інтерфейсна	5	3

Рішення

З метою розрахунку інтегральної оцінки економічної безпеки розрахуємо відносні оцінки безпеки підприємства за кожною складовою безпеки.

Відносна оцінка безпеки за відповідною складовою розраховується відношенням фактичного рівня безпеки (**ni**) до максимального рівня безпеки (**Ni**) відповідної складової.

Так, наприклад, для інтелектуальної складової економічної безпеки підприємства відносна оцінка безпеки дорівнює:

$$P_i = \frac{n_i}{N_i} = \frac{1}{3} = 0,33.$$

Аналогічні розрахунки проводимо для решти складових безпеки, а результати розрахунків зводимо до табл.4.2.

Таблиця 4.2

Оцінка економічної безпеки підприємства

Назва складової безпеки	Максимальний рівень	Фактичний рівень	Відносна оцінка
Інтелектуальна	3	1	0,33
Кадрова	3	2	0,67
Технічна	3	3	1,00
Правова	3	1	0,33
Екологічна	5	4	0,80
Інформаційна	3	1	0,33
Силова	3	2	0,67
Фінансова	5	4	0,80
Ринкова	7	4	0,57
Інтерфейсна	5	3	0,60

Чим ближче значення оцінки до одиниці, тим вищий рівень економічної безпеки.

Оцінка нижче 0,5 свідчить про ослаблення економічної безпеки підприємства.

Аналіз окремих складових дозволить встановити звідки надходять погрози.

Для наочності результати оцінювання економічної безпеки подамо у вигляді діаграми (рис.4.2), де радіус-вектори характеризують рівні складової економічної безпеки.

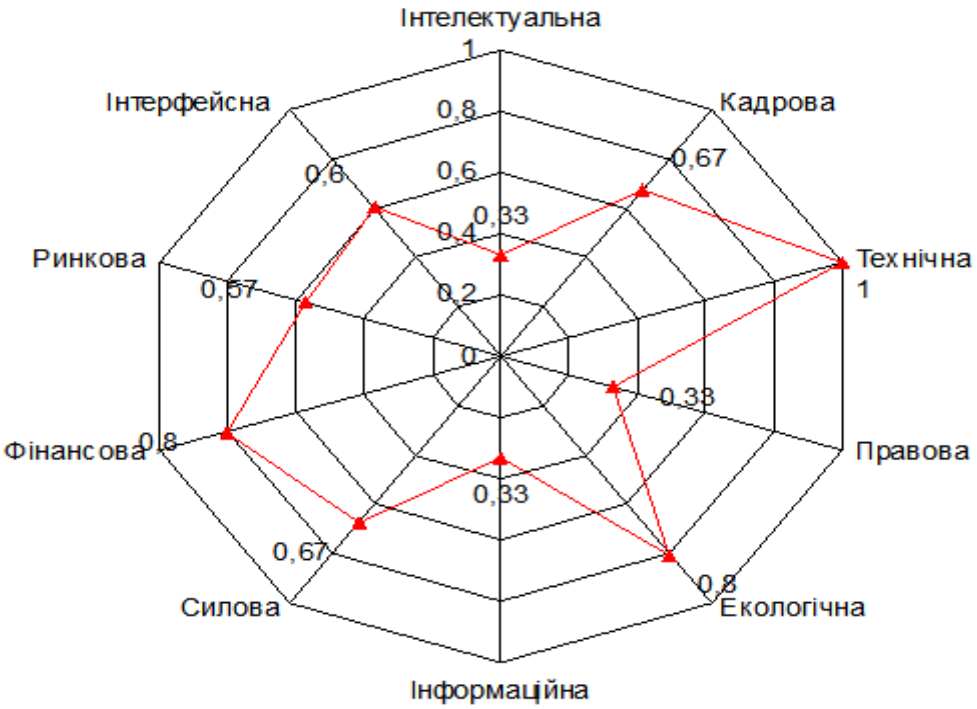


Рис.4.2. Схема областей економічної безпеки підприємства

Задачі для рішення задачі на занятті

Завдання 1

За даними, наведеними у табл.4.3:

- побудувати схему економічної безпеки;
- підготувати аналітичну записку раді директорів підприємства щодо ризиків підприємства.

Таблиця 4.3

Вихідні дані для оцінки економічної безпеки підприємства

Назва складової безпеки	Максимальний рівень	Фактичний рівень
Інтелектуальна	3	2
Кадрова	3	3
Технічна	3	2
Правова	3	3
Екологічна	5	1
Інформаційна	3	2
Силова	3	1
Фінансова	5	2
Ринкова	7	4
Інтерфейсна	5	2

Додаткові практичні завдання з діагностики безпеки підприємства

Завдання 2

Обчислити **коефіцієнт безпеки операційної діяльності підприємства** на основі наведених нижче показників:

1) постійні витрати підприємства протягом року – 230000 грн.
2) змінні витрати на весь обсяг продукції протягом року – 500000 грн.
3) ціна одиниці продукції – 250 грн./од.
4) виручка від реалізації продукції протягом року – 820500 грн.

Завдання 3

Використовуючи показник Вівера, провести **діагностику загрози банкрутства підприємства** протягом трьох років. Вихідні дані наведені в табл.4.4. Порогові значення коефіцієнта Вівера – 0,2.

Таблиця 4.4

Показники діяльності підприємства

Показники	2004 р.	2005 р.	2006 р.
1. Чистий прибуток, тис. грн.	4400	2180	3350
2. Амортизація, тис. грн.	890	1130	1190
3. Короткострокові боргові зобов'язання, тис. грн.	3350	3420	3315
4. Довгострокові боргові зобов'язання, тис. грн.	220	320	220

Завдання 4

Обчислити **коефіцієнт ефективності підприємництва**, використовуючи ці дані:

1) активи підприємства – 28800 тис. грн.

2) первісна вартість основних засобів виробництва – 23500 тис. грн.

3) коефіцієнт зносу основних засобів виробництва – 60%.

Оцінити ефективність підприємства, виходячи з того, що порогове значення коефіцієнта – 0,5.

Завдання 5

Фірма запланувала на звітний період підвищення рентабельності активів до 22%. Фактично рентабельність досягла 25%. **Розрахувати коефіцієнт дієвості фірми й перевищення ним порогового значення (1,0)**.

Завдання 6

Визначити рівень економічної безпеки підприємства, якщо для аналізу аналітику надали 100% інформації, рівень точності та суперечливості інформації відповідно дорівнює – 0,8 та 0,12. Зробити відповідні висновки.

Завдання 7

Рівень безпеки підприємства становить 0,27. **Зробити висновок про стан економічної безпеки** даного підприємства, а також **запропонувати ряд заходів із підвищення рівня його економічної безпеки.** Відомо, що підприємство належить до сфери великого бізнесу. Галузь діяльності – випуск продовольчих товарів.

Питання для самоконтролю

1.Які основні методологічні підходи існують до діагностики економічної безпеки підприємства?

2. Які основні методологічні підходи використовують до визначення станів функціонування підприємства?

3.Охарактеризуйте основні показники рівня економічної безпеки підприємства.

4. Які основні передумови виникнення інтеграційної теорії підприємства?

5. Чи існує різниця між «кризовим станом» функціонування організації та «станом кризи»?

6. Чи можна сформулювати універсальний показник розмежування безпечного і кризового стану функціонування підприємства?

7. Чи можлива довгострокова економічна безпека підприємства?

4.2. Моніторинг інформаційної безпеки організації

З розвитком IT-інфраструктури та впровадженням безлічі різних засобів захисту, збільшується кількість джерел інформації про події інформаційної безпеки (ІБ). При цьому події реєструються в кожному засобі окремо, і зрозуміти загальну картину того, що відбувається, стає дуже складно.

В ході своєї діяльності більшість підприємств постійно піддаються загрозам різного ступеня серйозності. Серед цих загроз - хакери, шкідливі

програми, незадоволені або безвідповідальні співробітники, застарілі і вразливі з інших причин пристрої та операційні системи, мобільні обчислення і обчислення в загальнодоступній хмарі і постачальники послуг з боку.

Через широку поширеність і неминучості ризиків при забезпеченні безпеки систем величезну роль грає оперативне реагування. А автоматизований і безперервний моніторинг безпеки є головною умовою швидкого виявлення та усунення загроз.

Для того, щоб автоматизувати процес збору та аналізу інформації про події ІБ можуть використовуватися спеціалізовані системи моніторингу. Система моніторингу безпеки зобов'язана реагувати на усі зміни, що викликані подіями, як на невідомі заздалегідь інформаційні впливи Уже є досвід створення рішень на базі продукту HP ArcSight, призначених для збору, обробки, кореляції і реагування на події ІБ з єдиного центру управління.

4.2.1. Моніторинг безпеки в інформаційній системі

Моніторинг інформаційної безпеки входить як етап процесу створення захищеної інформаційної системи (ІС) організації. Моніторинг ІБ в основному організації проводять своїми силами і часто не мають персоналу відповідної компетенції.

Такі функції безпеки, як реєстрація подій безпеки, ведення журналів; виявлення (запобігання) вторгнень; контроль (аналіз) захищеності інформації - тісно пов'язані між собою і використовуються в єдиному комплексі, метою якого є регулярний моніторинг стану безпеки ІС (часто в режимі реального часу), спрямованого на:

- виявлення і прогнозування подій та інцидентів ІБ;
- оцінку рівня поточної захищеності ІС;
- прийняття рішень з управління ІБ.

Метою моніторингу безпеки в ІС є спостереження за середовищем з метою виявлення інцидентів безпеки на базі правил аудиту.

Завданнями моніторингу є:

- збір даних з підсистем реєстрації;

- перевірка фізичної доступності обладнання ІС;

- перевірка стану прикладних і системних служб і сервісів, запущених в ІС;

- детальна перевірка не критичних, але важливих параметрів функціонування мережі: продуктивності, завантаження, обсягу і змісту мережевого трафіку;

- перевірка параметрів, специфічних для сервісів і служб даного конкретного оточення;

- контроль дерева і параметрів процесів;

- аналіз даних і обробка подій і аномалій;

- передача зібраних даних в модулі виявлення інцидентів і аудиту безпеки.

Моніторинг та обробка подій в ІС представлений у вигляді рис.4.3.

Таким чином, призначення систем моніторингу - збирати дані і виявляти аномалії в роботі ІС, а потім оперативно на них реагувати.

Виявлення підлягає підозріла і аномальна активність компонентів системи - від користувачів (внутрішніх і зовнішніх) до програмних і апаратних засобів.

Існуючі системи моніторингу використовують для виявлення атак і підозрілої активності в ІС мережевий і системний підходи.

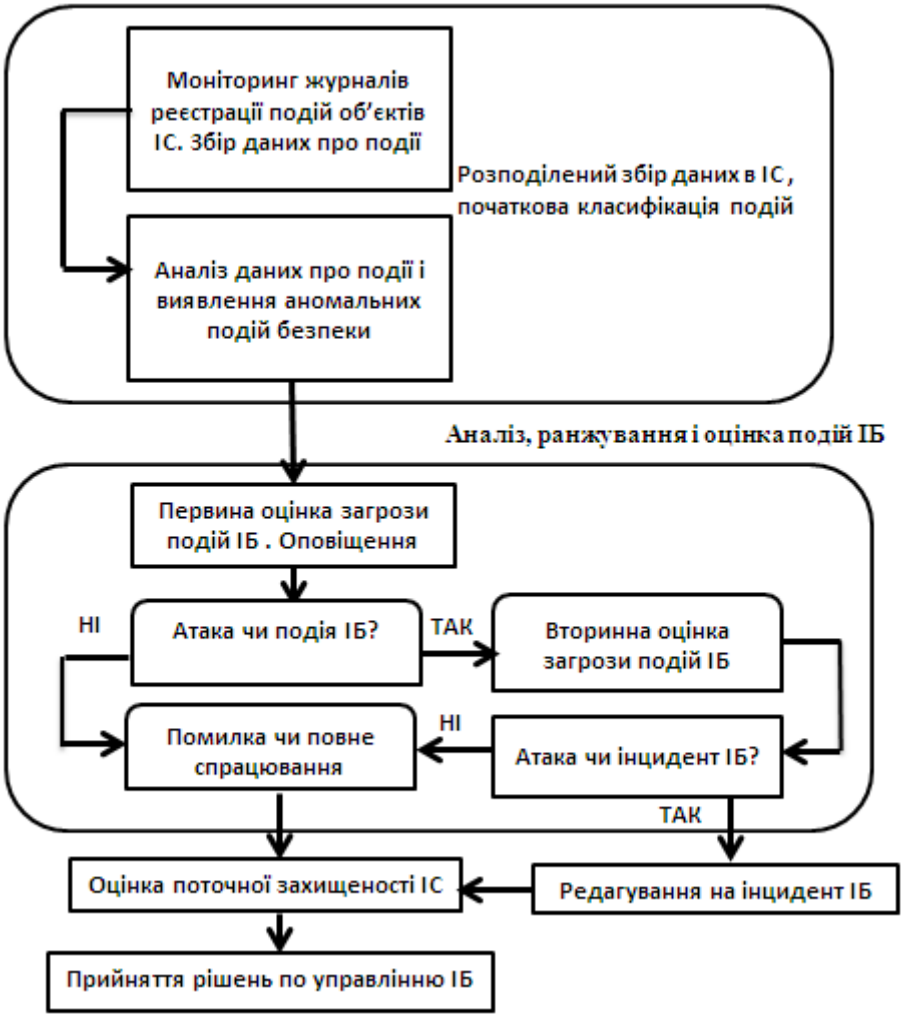


Рис. 4.3. Моніторинг та обробка подій в ІС

При проведенні моніторингу на мережевому рівні використовують як джерело даних для аналізу необроблені мережеві пакети. Для цього використовується мережевий адаптер, що функціонує в режимі «прослуховування», і трафік в реальному масштабі часу в міру його проходження через сегмент мережі.

Моніторинг системного рівня контролює систему, події та журнали реєстрації подій безпеки. Коли будь-якої з цих файлів змінюється, то відбувається порівняння нових записів з сигнатурами атак, щоб перевірити, чи є відповідність. Якщо така відповідність знайдено, то система посилає адміністратору сигнал тривоги або пускає в хід інші задані механізми реагування.

Кожен рівень проведення моніторингу в ІС має свої особливості і охоплює певну область дії. Результати порівняння можливостей проведення моніторингу на різних рівнях представлено в табл.4.4.

Таким чином, недоліки, які є при використанні систем моніторингу тільки системного рівня, нейтралізуються достоїнствами систем моніторингу мережевого рівня і навпаки.

Тому комбінування цих двох технологій значно покращує ефективність контролю і подальше опір ІС до атак і зловживань.

За результатами моніторингу безпеки можна виявити потенційних порушників, і закрити вразливі місця в ІС, що дозволить посилити політику безпеки і внести велику гнучкість в процес експлуатації мережевих ресурсів.

Таблиця 4.4.

Порівняння рівнів проведення моніторингу в ІС

	Рівень моніторингу	Вид	Переваги	Недоліки
1	Системний рівень	Система. Події. Журнал безпеки	- підтверджує успіх або відмова атаки; - контролює діяльність конкретного вузла; - виявляє атаки, які не беруть системи мережевого рівня; - добре підходить для мереж з шифруванням і комутацією; - не вимагають додаткових апаратних засобів; - низька вартістьэксплуатації.	- залежить від ОС; - не може виявити аномалії, що виникають на мережевому рівні
2	Мережевий рівень	Аналіз мережевих пакетів	- низька вартість експлуатації; - виявляє атаки або аномалії в поведінці, які виникають на мережевому рівні; - виявляє і реагує в реальному масштабі часу; - виявляє невдалі атаки або підозрілі наміри; - не залежить від ОС.	- не може виявляти атаки системного рівня

4.2.2 Побудова системи моніторингу подій інформаційної безпеки

Моніторинг безпеки являє собою комплекс заходів і заходів (технічних, організаційних і правових), спрямованих на реалізацію спостереження, аналізу та прогнозування станів безпеки складних систем.

ІБ вимагає врахування всіх подій, в ході яких інформація створюється, модифікується, до неї забезпечується доступ або вона поширюється. Виконання даних заходів є вимогою міжнародного стандарту ISO / IEC 27001.

Система моніторингу подій інформаційної безпеки (СМПІБ) призначена для автоматизації процесу збору та аналізу інформації про події безпеки, що надходять з різних джерел. В якості таких джерел можуть виступати засоби захисту інформації, загальносистемне і прикладне програмне забезпечення (ПЗ), телекомунікаційне забезпечення та ін.

СМПІБ включає в себе наступні компоненти:

-програмно-технічна частина - реалізується на основі продуктів з моніторингу подій безпеки класу SIEM (SecurityInformationandEventManagement);

- документаційна частина - включає в себе набір документів, що описують основні процеси, пов'язані з виявленням і реагуванням на інциденти безпеки;

-кадрова складова - має на увазі виділення співробітників, відповідальних за роботу з СМПІБ.

Типова структура СМПІБ зображена на рис.4.4.

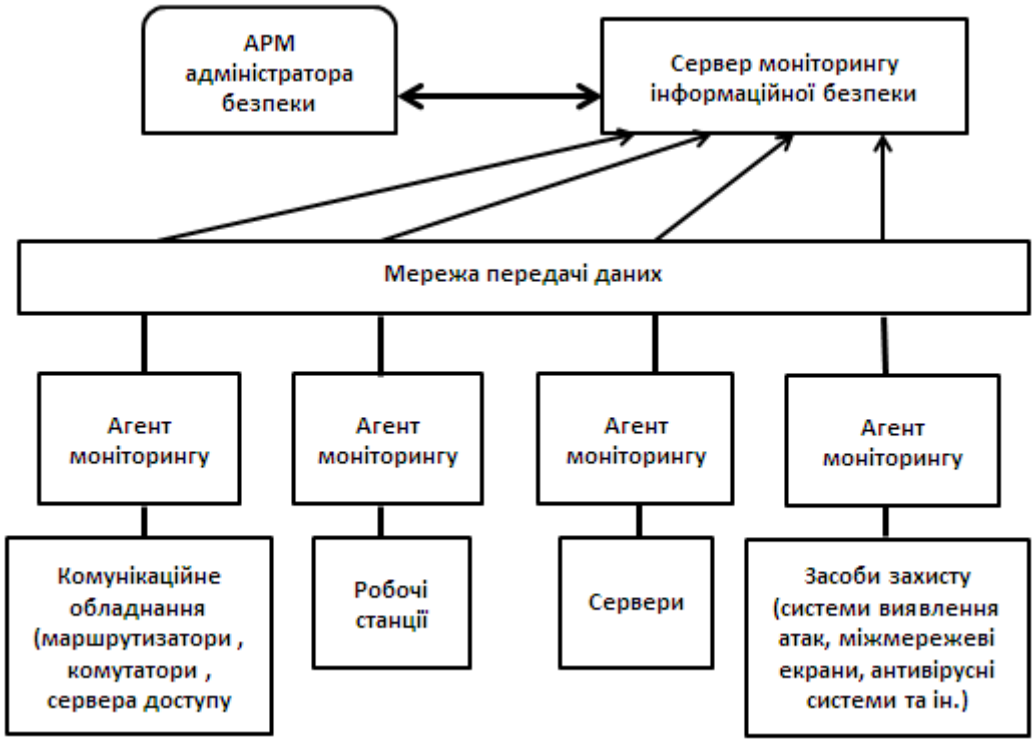


Рис.4.4. Структура системи моніторингу подій інформаційної безпеки

Програмно-технічна частина СМПІБ включає:

-агенти моніторингу, призначені для збору інформації, що надходить від різних джерел подій, що включають в себе засоби захисту, загальносистемне і прикладне ПЗ, телекомунікаційне забезпечення та ін .;

- сервер подій, що забезпечує централізовану обробку інформації про події безпеки, яка надходить від агентів. Обробка здійснюється відповідно до правил, які задаються адміністратором безпеки;

-сховище даних, що містить результати роботи системи, а також дані, отримані від агентів;

-консоль управління системою, що дозволяє в реальному масштабі часу переглядати результати роботи системи, а також керувати її параметрами.

Документаційна частина СМПІБ передбачає розробку пакета нормативних документів з управління інцидентами безпеки. Як правило, для цього формується політика управління інцидентами ІБ, яка визначає класифікацію інцидентів, загальний порядок реагування, відповідальність за реалізацію даного документа

та ін. На основі цієї політики для кожного з видів інцидентів безпеки розробляється окремий регламент, що описує детальний порядок реагування на їх різні види.

Кадрова складова СМПІБ передбачає виділення різних ролей відповідальності. Як правило, виділяють наступні ролі в складі СМПІБ:

-системний адміністратор, який відповідає за підтримку загальносистемного апаратного забезпечення СМПІБ;

-адміністратор безпеки, що забезпечує управління настройкою параметрів функціонування СМПІБ;

- оператор, що виконує завдання перегляду результатів роботи СМПІБ і реалізації базових функцій реагування на типові інциденти;

-аналітик, що забезпечує аналіз і реагування на складні види інцидентів.

Основні етапи створення СМПІБ. Процес впровадження будь-якої системи моніторингу подій ІБ включає етапи:

- обстеження автоматизованої системи. В рамках обстеження проводиться ідентифікація основних джерел подій безпеки, визначення технології збору, зберігання і обробки даних. За результатами обстеження формуються вимоги до архітектури і функціональних можливостей системи моніторингу ІБ.

- розробку технічного проекту, в якому описується конфігурація обладнання та програмного забезпечення, порядок впровадження, схема інформаційних потоків, вимоги до зовнішнього оточення системи моніторингу і т. д.;

- навчання співробітників, які будуть відповідати за експлуатацію системи моніторингу інформаційної безпеки;

- створення пілотного району для тестового впровадження системи моніторингу ІБ. Якщо об'єктом моніторингу є територіально-розподілена система, що охоплює кілька філій, то в якості тестового сегмента, як правило, вибирається найбільш великий підрозділ, на якому можна апробувати рішення, описані в технічному проекті.

- промислове впровадження системи моніторингу. Впровадження проводиться з урахуванням результатів, отриманих в процесі тестового впровадження системи моніторингу;

- технічний супровід системи моніторингу ІБ.

Як правило, на етапі створення СМПІБ підрозділ інформаційної безпеки намагається підключити систему моніторингу до найбільшої кількості джерел і отримати від них максимальний обсяг інформації.

Однак необхідно брати до уваги той факт, що якщо включити всі можливі режими аудиту, то це може привести до значного збільшення навантаження на сервери, з яких виходить інформація, і, як наслідок, порушення їх працездатності.

Саме тому одним із завдань на етапі обстеження є пошук компромісу між бажанням підрозділи ІБ отримувати і обробляти максимальний обсяг інформації і реальною можливістю підрозділу ІТ надати дану інформацію.

Ще одним важливим завданням, які мають вирішуватися в процесі впровадження, є визначення тих інцидентів, які будуть виявлятися в процесі роботи СМПІБ. Для цього виконуються наступні дії:

- визначення типів основних інцидентів ІБ;

- визначення переліку обставин, які ведуть до інциденту ІБ;

- визначення джерела інциденту ІБ;

- визначення та пріоритезація ризиків, пов'язаних з інцидентами ІБ.

Для підвищення ефективності прийняття рішень з реагування на події, пов'язані з порушенням безпеки, рекомендується використовувати спеціалізовані системи моніторингу, які можуть автоматизувати процес збору та аналізу інформації, що надходить від різних засобів захисту. У західній термінології такі системи моніторингу позначаються абревіатурою SIEM (Security Information and Event Management).

Технологія функціонування SIEM-систем передбачає поділ процесу обробки подій безпеки **на шість основних етапів**

-фільтрація, агрегація, нормалізація, збір, кореляція і візуалізація.

- в процесі фільтрації система видаляє події, які не мають прямого відношення до забезпечення інформаційної безпеки.

- агрегація дозволяє видалити повторювані події, що описують один і той же інцидент. Фільтрація і агрегація дозволяють значно скоротити обсяг інформації, який обробляється системою моніторингу (при правильному плануванні обсяг інформації скорочується в 5-10 разів).

- на етапі нормалізації події приводяться до єдиного формату повідомлень. Далі нормалізовані події різних систем і різних агентів передаються в єдину централізовану систему зберігання подій.

- зібрані повідомлення потім обробляються, використовуючи механізми кореляції, засновані на статистичних методах, а також правила побудови експертної системи.

- SIEM-система видає отримані результати на централізовану консоль, що працює в режимі реального часу.

В Україні успішно реалізовано низку проектів з використанням SIEM-систем, в т. ч. для «Райффайзен Банку Аваль» і «ПРАВЕКС-БАНКу». Рішення засновані на продуктах таких виробників, як ArcSight (HP), Symantec, IBM.

В даний час найбільшого поширення набуло рішення ArcSight компанії Hewlett Packard.

ArcSight дозволяє здійснювати моніторинг ІБ всіх необхідних ресурсів в режимі реального часу, отримуючи інформацію як на рівні засобів захисту, так і на рівні мережевих ресурсів, додатків і баз даних, що дозволяє побудувати комплексну систему моніторингу та управління подіями інформаційної безпеки.

ArcSight дозволяє адміністраторам безпеки сфокусуватися на реальних загрозах безпеки, забезпечуючи їх засобами, що дозволяють оперативно реагувати на загрози безпеці мережі.

Для візуалізації результатів роботи системи використовується консоль адміністратора, яка в реальному режимі часу дозволяє проводити поділ подій за категоріями, кореляцію подій, як по ресурсах, так і по зловмисникам, а також здійснювати детальний аналіз.

За допомогою карти порушень безпеки можна отримати уявлення про відхилення в параметрах безпеки. Крім того, консоль надає можливості для підготовки табличних і графічних звітів про безпеку.

Архітектура ArcSight ESM реалізується на основі трирівневої моделі, що включає в себе сервер бази даних, сервер обробки повідомлень і консоль управління системою (рис. 4.5).

На основі систем моніторингу можуть створюватися повноцінні центри управління інформаційною безпекою (SOC, Security Operation Centers). Вони припускають цілодобову роботу операторів, відповідальних за аналіз можливих інцидентів в області ІБ.

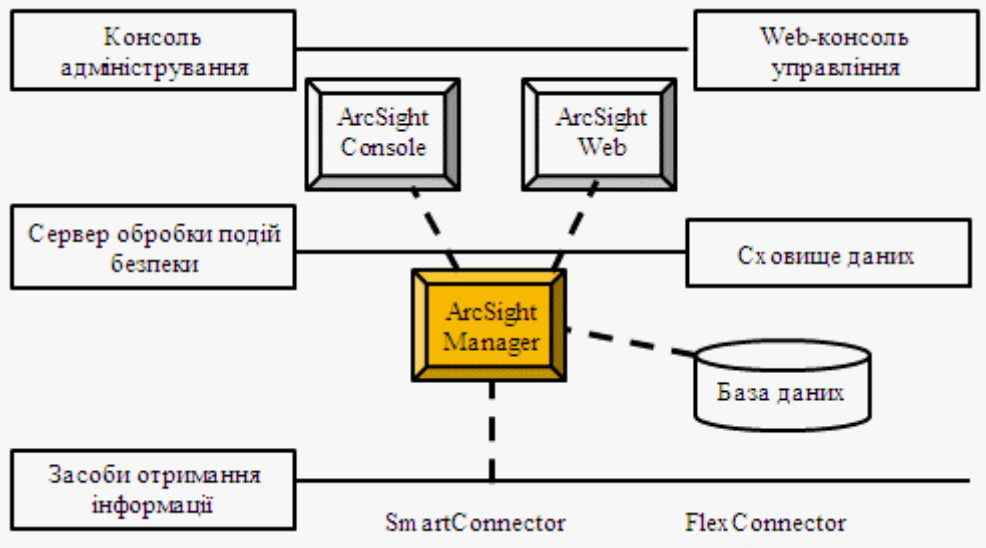


Рис.4.5. Архітектура системи ArcSight ESM.

Таким чином, моніторинг подій є одним з найважливіших процесів забезпечення безпеки інформаційних систем. Для підвищення ефективності прийняття рішень з реагування на події, пов'язані з порушенням безпеки, рекомендується завжди використовувати спеціалізовані системи моніторингу, які можуть автоматизувати процес збору та аналізу інформації, що надходить від різних засобів захисту.

Питання для самоконтролю

1. Що являє собою моніторинг інформаційної безпеки?

2. Яке призначення системи моніторингу подій інформаційної безпеки (СМПІБ)?

3. Дайте характеристику основних елементів структури системи моніторингу подій інформаційної безпеки.

4. Перерахуйте основні етапи створення СМПІБ.

5. Що треба зробити для організації ефективного моніторингу?

6. Розкрийте типові ролі фахівців процесу моніторингу

7. Яка інформаціяреєструється в журналі реєстрації інцидентів інформаційної безпеки?

8. Які типи інцидентів рекомендовані NIST для реєстрації?

4.3. Аудит інформаційної безпеки організації

За останні кілька років, спостерігається збільшення числа атак на автоматизовані системи, що призводять до значних фінансових і матеріальних втрат. Для об'єктивної оцінки поточного рівня безпеки автоматизованих систем застосовується аудит безпеки.

Аудит інформаційної безпеки (ІБ) є одним з найбільш актуальних і напрямків стратегічного і оперативного менеджменту в області безпеки КС і викликає постійний інтерес фахівців. Його основне завдання - об'єктивно оцінити поточний стан ІБ організації, а також її адекватність поставленим цілям і задачам бізнесу.

Аудит інформаційної безпеки - один з найбільш ефективних сьогодні інструментів для отримання незалежної і об'єктивної оцінки поточного рівня захищеності підприємства від загроз інформаційної безпеки. Крім того, результати аудиту дають основу для формування стратегії розвитку системи забезпечення інформаційної безпеки організації.

Процес створення захищеної ІС складається з наступних етапів:

1. Аудит інформаційної системи
2. Виявлення та оцінка загроз інформаційній безпеці
3. Проектування підсистеми захисту інформації (СЗІ)
4. Закупівля, встановлення та налаштування засобів захисту інформації
5. Експлуатація ПЗІ і моніторинг інформаційної безпеки.

Як правило, з першим-четвертим етапами організації справляються своїми силами або із залученням сторонніх виконавців.

Аудит ІБ - це перевірка здатності успішно протистояти загрозам ІБ.

Аудит інформаційної безпеки - процес отримання об'єктивних якісних і кількісних оцінок поточного стану ІБ компанії відповідно до визначених критеріїв та показниками безпеки.

Аудит інформаційних систем - це перевірка використовуваних компанією інформаційних систем, систем безпеки, систем зв'язку з зовнішнім середовищем, корпоративної мережі на предмет їх відповідності бізнес-процесів, що протікають в компанії, а також відповідності міжнародним стандартам, з подальшою оцінкою ризиків збоїв в їх функціонуванні.

Аудит ІБ- системний процес отримання об'єктивних якісних і кількісних оцінок поточного стану ІБ організації відповідно до визначених критеріїв та показниками на всіх основних рівнях забезпечення безпеки: нормативно-методологічному, організаційно-управлінському, процедурному і програмно-технічному.

Аудит інформаційної безпеки є незалежна перевірка або експертна оцінка забезпечення безпеки інформаційної системи (ІС) будь-якого підприємства, установи або організації на основі спеціально розроблених критеріїв і показників.

Основні напрямки аудиту інформаційної безпеки. Що стосується сфери застосування такого аудиту, як правило, їх розрізняють кілька:

- **повна перевірка об'єктів**, задіяних в процесах інформатизації (комп'ютерні автоматизовані системи, засоби комунікації, прийому, передачі та

обробки інформаційних даних, технічних засобів, приміщень для проведення конфіденційних зустрічей, систем спостереження і т .д.);

- **перевірка надійності захисту конфіденційної інформації** з обмеженим доступом (визначення можливих каналів витоку і потенційних дірок в системі безпеки, що дозволяють отримати до неї доступ ззовні з використанням стандартних і нестандартних методів);

- **перевірка всіх електронних технічних засобів і локальних комп'ютерних систем** на предмет впливу на них електромагнітного випромінювання і наведень, що дозволяють відключити їх або привести в непридатність; проектна частина, що включає в себе роботи по створенню концепції безпеки та застосування її в практичному виконанні (захист комп'ютерних систем, приміщень, засобів зв'язку і т. д.).

Супровідні послуги. Іноді в ході активного аудиту замовнику пропонується ряд додаткових послуг, безпосередньо пов'язаних з оцінкою стану системи інформаційної безпеки, зокрема - проведення спеціалізованих досліджень.

Найчастіше організація в своїй інформаційній системі використовує спеціалізоване програмне забезпечення (ПЗ) власної розробки, призначене для вирішення нестандартних завдань (наприклад, корпоративний інформаційний портал, різні бухгалтерські системи або системи документообігу). Подібне ПЗ унікальне, тому будь-яких готових засобів і технологій для аналізу їх захищеності і відмовостійкості не існує. В даному випадку проводяться спеціалізовані дослідження, спрямовані на оцінку рівня захищеності конкретного ПЗ.

Ще один вид послуг, пропонованих в ході активного аудиту, - ***дослідження продуктивності і стабільності системи, або стрес-тестування***. Воно спрямоване на визначення критичних точок навантаження, при якій система внаслідок атаки на відмову в обслуговуванні або підвищеної завантаженості перестає адекватно реагувати на легітимні запити користувачів.

Стрес-тест дозволить виявити «вузькі» місця в процесі формування та передачі інформації.

4.3.1. Аудит інформаційної безпеки інформаційних систем

Аудит інформаційної безпеки інформаційних систем (ІС) спрямований на оцінку стану безпеки і розробки рекомендацій щодо застосування комплексу організаційних заходів та програмно-технічних засобів, спрямованих на забезпечення захисту інформаційних ресурсів ІС від загроз інформаційної безпеки.

Цілі аудиту. Цілями робіт з аудиту стану інформаційної безпеки інформаційної системи є:

• отримання об'єктивної і незалежної оцінки поточного стану захищеності інформаційних ресурсів;

• підвищення рівня надійності та інформаційної безпеки інформаційної системи організації;

Основними конкретними цілями проведення аудиту безпеки є:

• аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки щодо ресурсів ІС;

• оцінка поточного рівня захищеності ІС;

• локалізація вузьких місць в системі захисту ІС;

• оцінка відповідності ІС існуючим стандартам в області ІБ;

• вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС.

Основні елементи аудиту інформаційної безпеки представлені на рис.4.5.

Стандарт ISO / IEC 27007 до: 2017 містить рекомендації з управління програмою аудиту системи менеджменту ІБ (СМІБ), проведення внутрішніх і зовнішніх аудитів СМІБ, а також компетентності і оцінки аудиторів СМІБ. Крім того, він дає рекомендації для аудиту всіх вимог, викладених в ISO / IEC 27001:

2013 і використовується в поєднанні з інструкцією, викладеною в ISO 19011: 2018.

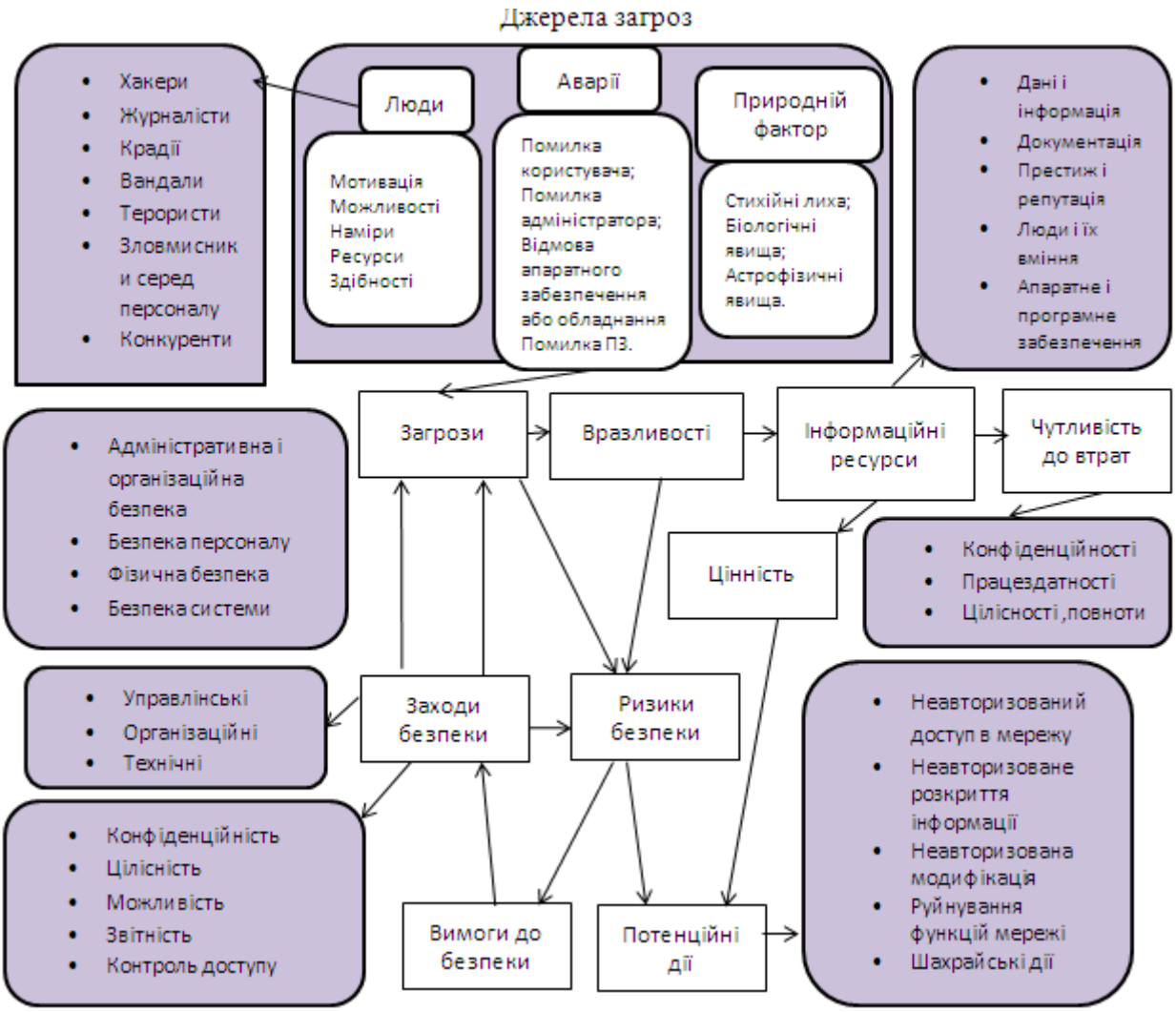


Рис.4.5. Основні елементи аудиту інформаційної безпеки

Стандарт ISO 19011: 2018 містить рекомендації для проведення аудитів організацій різних областей всіх розмірів і типів для аудиторських груп, а також окремих аудиторів. У документі основна увага приділяється внутрішнім аудитів (перша сторона) та аудитів постачальників і інших зовнішніх зацікавлених сторін (інша сторона). Цей документ також може бути корисний для зовнішніх аудитів, проведених з метою, відмінних від сертифікації.

Документ також може бути корисний організаціям, які беруть участь в навчанні аудиторів або сертифікації персоналу.

Стандарт містить рекомендації по системам управління аудитом, включаючи принципи аудиту, управління програмою аудиту та проведення аудитів системи менеджменту, в тому числі комбінованих аудитів, а також керівництво по оцінці компетентності осіб, які беруть участь в процесі аудиту.

Загальна методика проведення аудиту (перевірок) представлена на рис.4.6, схема алгоритму загальної методики аудиту ІБ – на рис.4.7.

Рис.4.6. Загальна методика проведення аудиту (перевірок) ІТС

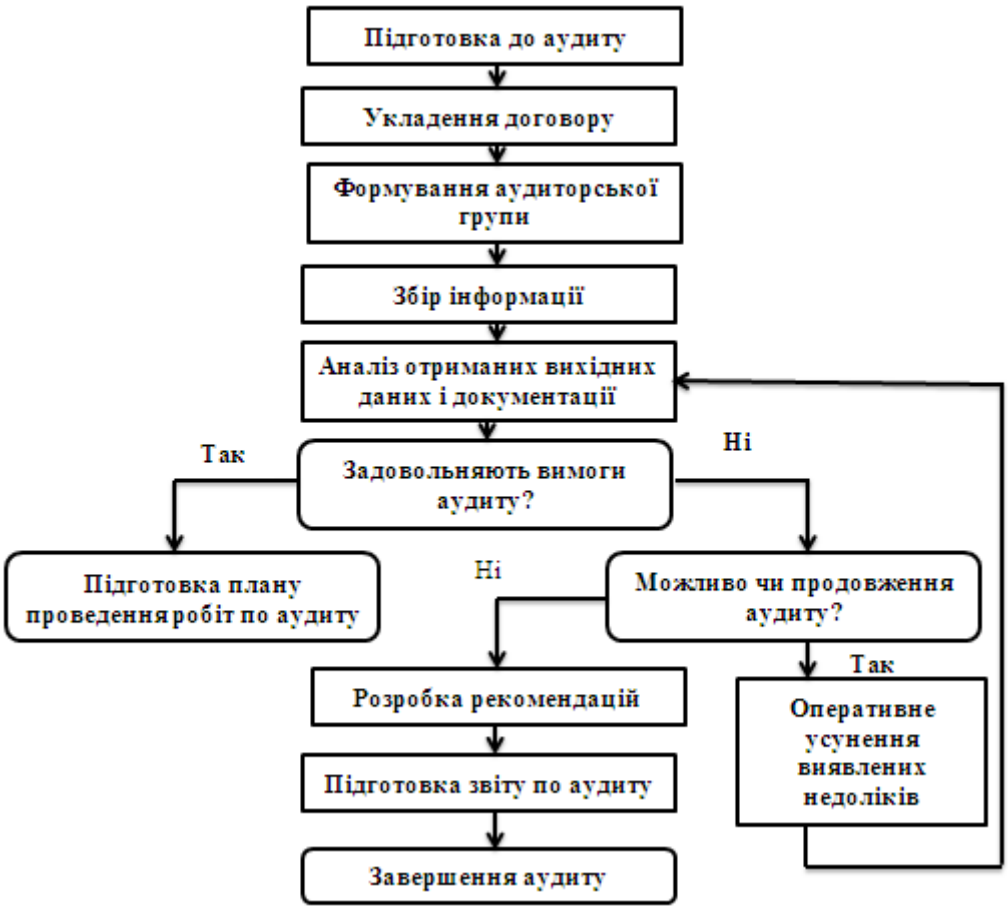


Рис.4.7. Схема алгоритму загальної методики аудиту ІБ

Перелік вихідних даних, необхідних для аудиту безпеки, представлений у табл. 4.5.

Таблиця 4.5.

Перелік вихідних даних, необхідних для аудиту безпеки

Тип інформації	Склад вихідних даних
Організаційно-розпорядча документація з питань інформаційної безпеки	• політика інформаційної безпеки ІС; керівні документи (накази, розпорядження, інструкції) з питань зберігання, порядку доступу і передачі інформації; регламенти роботи користувачів з інформаційними ресурсами ІС

Продовження табл.4.5.

Інформація про апаратне забезпечення хостів	• перелік серверів, робочих станцій і комунікаційного устаткування. встановленого в ІС: • апаратні конфігурації серверів і робочих станцій; • відомості про периферійне обладнанні
Інформація про загальносистемне ПЗ	• відомості про ОС. встановлених на робочих станціях і серверах; • відомості про СУБД встановлених в ПЗ
Інформація про прикладному ПЗ	• перелік прикладного ПЗ загального і спеціального призначення, встановленого в ІС; • опис функціональних завдань, які вирішуються за допомогою прикладного ПЗ
Інформація про засоби захисту, встановлених в ІС	• виробник засоби захисту; • конфігураційні налаштування засобів захисту; • схема установки засобів захисту
Інформація про топології ІС	• карта локальної обчислювальної мережі, включаючи схему розподілу серверів і робочих станцій за сегментами мережі: • типи каналів зв'язку, що використовуються в ІС; • використовувані в ІС мережеві протоколи; • схема інформаційних потоків ІС

4.3.2. Аудит інформаційної безпеки комп'ютерних систем

Результати кваліфіковано виконаного аудиту ІБ організації дозволяють побудувати оптимальну по ефективності і витратам систему забезпечення інформаційної безпеки (СЗІБ), що представляє собою комплекс технічних засобів, а також процедурних, організаційних і правових заходів, об'єднаних на основі моделі управління ІБ.

В результаті проведення аудиту можуть бути отримані як якісні, так і кількісні оцінки. При якісному оцінюванні, наприклад, може бути наведений перелік вразливостей в програмно-апаратному забезпеченні з їх класифікацією за трирівневою шкалою небезпеки: висока, середня і низька. Кількісні оцінки найчастіше застосовуються при оцінці ризику для активів організації, що створюється загрозами безпеці. Як кількісних оцінок можуть виступати, наприклад, ціна ризику, ймовірність ризику, розмір ризику і т. д.

Об'єктивність аудиту забезпечується, зокрема, тим, що оцінка з-стояння ІБ проводиться фахівцями на основі певної методики, що дозволяє об'єктивно проаналізувати всі складові СЗІБ.

Аудит ІБ може являти собою послугу, яку пропонують спеціалізовані фірми, проте в організації повинен проводитися внутрішній аудит ІБ, що виконується, наприклад, адміністраторами безпеки.

Аудит інформаційної безпеки комп'ютерних систем традиційно поділяють на три типи, які відрізняються переліком аналізованих компонентів СЗІБ і одержуваними результатами:

- активний аудит;

- експертний аудит;

- аудит на відповідність стандартам ІБ.

Активний аудит являє собою обстеження стану захищеності певних підсистем інформаційної безпеки (**ПІБ**), що відносяться до програмно-технічним рівнем.

Наприклад, варіант активного аудиту, який називається тестом на проникнення (Penetration test), передбачає обстеження підсистеми захисту мережевих взаємодій. Активний аудит включає:

- аналіз поточної архітектури і налаштувань елементів ПІБ;

- інтерв'ювання відповідальних і зацікавлених осіб;

- проведення інструментальних перевірок, що охоплюють певні ПІБ.

Аналіз архітектури і налаштувань елементів ПІБ проводиться фахівцями, що володіють знаннями щодо конкретних підсистем, представленим в

обстежуваної системі (наприклад, можуть вимагатися фахівці з активного мережевого обладнання фірми Cisco або по ОС сімейства Microsoft), а також системними аналітиками, які виявляють можливі вади в організації підсистем . Результатом цього аналізу є набір опитувальних листів і інструментальних тестів.

Опитувальні листи використовуються в процесі інтерв'ювання осіб, відповідальних за адміністрування АІС:

- для отримання суб'єктивних характеристик АІС,
- для уточнення отриманих вихідних даних і
- для ідентифікації деяких заходів, реалізованих в рамках СЗІБ.

Наприклад, опитувальні листи можуть включати питання, пов'язані з політикою зміни і призначення паролів, життєвим циклом АІС і ступенем критичності окремих її підсистем для АІС і бізнес-процесів організації в цілому.

Паралельно з інтерв'юванням проводяться **інструментальні перевірки** (тести), які можуть включати наступні заходи:

- візуальний огляд приміщень, обстеження системи контролю доступу в приміщення;
- отримання конфігурацій і версій пристроїв і ПЗ;
- перевірка відповідності реальних змін наданим вихідним даним;
- отримання карти мережі спеціалізованим ПЗ;
- використання сканерів захищеності (як універсальних, так і спеціалізованих);
- моделювання атак, що використовують уразливості системи;
- перевірка наявності реакції на дії, які виявляються механізмами виявлення та реагування на атаки.

Аудитор може виходити з таких моделей, що описують ступінь його знання досліджуваної АІС (**модель знання**):

- модель «чорного ящика» - аудитор не володіє ніякими апріорними знаннями про досліджувану АІС. Наприклад, при проведенні зовнішнього активного аудиту (тобто в ситуації, коли моделюються дії зловмисника, який би

поза досліджуваної мережі), аудитор може, знаючи тільки ім'я або IP-адреса WEB-сервера, намагатися знайти уразливості в його захист;

- модель «білого ящика» - аудитор має повним знанням про структуру досліджуваної мережі. Наприклад, аудитор може мати картами і діаграмами сегментів досліджуваної мережі, списками ОС і додатків. Застосування даної моделі не в повній мірі імітує реальні дії зловмисника, але дозволяє, проте, уявити «найгірший» сценарій, коли атакуючий має повним знанням про мережі;

- модель «сірого ящика» або «кришталевого ящика» - аудитор імітує дії внутрішнього користувача АІС, що володіє обліковим записом доступу в мережу з певним рівнем повноважень. Дана модель дозволяє оцінити ризики, пов'язані з внутрішніми загрозами, наприклад від неблагонадійних співробітників компанії. Аудитори повинні погоджувати кожен тест, модель знання, яка застосовується в тесті, і можливі негативні наслідки тесту з особами, зацікавленими в безперервній роботі АІС (керівниками, адміністраторами системи і ін.).

За результатами інструментальної перевірки проводиться перегляд результатів попереднього аналізу і, можливо, організується додаткове обстеження (рис.4.8).

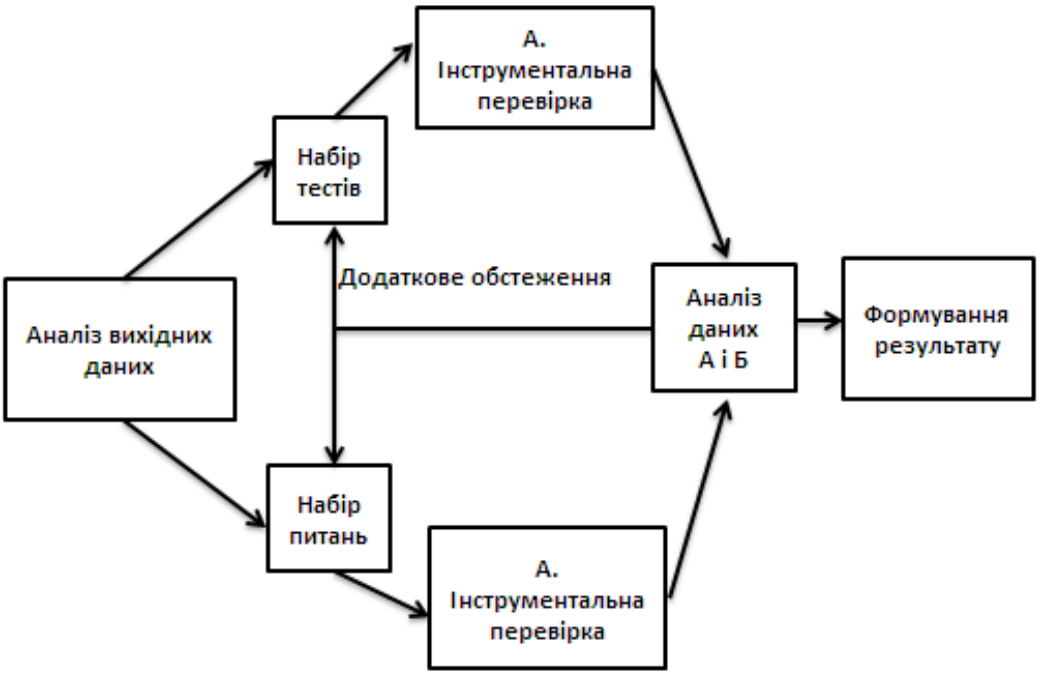


Рис.4.8. Схема проведення активного аудиту ІБ

За результатами **активного аудиту** створюється **аналітичний звіт**, що складається з опису поточного стану технічної частини СЗІБ, списку знайдених вразливостей АІС зі ступенем їх критичності і результатів спрощеної оцінки ризиків, що включає модель порушника і модель загроз.

Додатково може бути розроблений план робіт по модернізації технічної частини СЗІБ, що складається з переліку рекомендацій по обробці ризиків.

Експертний аудит. Експертна аудит призначений для оцінювання поточного стану ІБ на нормативно-методологічному, організаційно-управлінському та процедурному рівнях. Експертна аудит проводиться переважно зовнішніми аудиторами, його виконують силами фахівців із системного управління.

Співробітники організації-аудитора спільно з представниками замовника проводять такі **види робіт**:

- збір вихідних даних про АІС, її функції і особливості, використовувані технології автоматизованої обробки і передачі інформації (з урахуванням найближчих перспектив розвитку);

- збір інформації про наявні організаційно-розпорядчих документах щодо забезпечення ІБ і їх аналіз;

- визначення захищаються активів, ролей і процесів СЗІБ.

Найважливішим інструментом експертної оцінки є збір даних про АІС шляхом інтерв'ювання керівництва замовника і технічних фахівців.

Основні цілі інтерв'ювання керівного складу організації:

- визначення політики та стратегії керівництва в питаннях забезпечення ІБ;

- виявлення цілей, які ставляться перед СЗІБ;

- з'ясування вимог, які пред'являються до СЗІБ;

- отримання оцінок критичності підсистем обробки інформації, оцінок фінансових втрат при виникненні інцидентів.

Основні цілі інтерв'ювання технічних фахівців:

- збір інформації про функціонування АІС;

- отримання схеми інформаційних потоків в АІС;

- отримання інформації про технічну частину СЗІБ;

- оцінка ефективності роботи СЗІБ.

В рамках експертного аудиту проводиться аналіз організаційно-розпорядчих документів, таких як політика безпеки, план захисту і-ти, різного роду положення та інструкції.

Організаційно-розпорядчі документи оцінюються на предмет достатності і несуперечності декларованим цілям і заходам ІБ, а також на предмет відповідності стратегічній політиці керівництва в питаннях ІБ.

Результати експертного аудиту можуть містити рекомендації щодо вдосконалення нормативно-методологічних, організаційно-управлінських та процедурних компонентів СЗІБ.

Офіційний звіт в результаті проведення аудиту включає:

• Ступінь відповідності перевіряється інформаційної системи обраним стандартам

• Ступінь відповідності власним внутрішнім вимогам компанії в області інформаційної безпеки

• Кількість і категорії отриманих невідповідностей і зауважень

• Рекомендації з побудови або модифікації системи забезпечення інформаційної безпеки, що дозволяють привести її у відповідність з даним стандартом

• Детальне посилання на основні документи замовника, включаючи політику безпеки, опису процедур забезпечення інформаційної безпеки, додаткові обов'язкові і необов'язкові стандарти і норми, які застосовуються до даної компанії.

Аудит на відповідність стандартам найчастіше має на увазі проведення активного і експертного аудиту.

Спеціально уповноважені організації-аудитори за результатами аудиту приймають рішення і видають документальне підтвердження про відповідність СЗІБ того чи іншого еталонного стандарту (проводять сертифікацію).

Сертифікація є показником якості СЗІБ і піднімає престиж і рівень довіри до організації.

За результатами можуть бути підготовлені звіти, що містять наступну інформацію:

- ступінь відповідності перевіряється ІС обраним стандартам;

- кількість і категорії отриманих невідповідностей і зауважень;

- рекомендації з побудови або модифікації СЗІБ, що дозволяють привести її у відповідність до вимог даного стандарту.

Основою для проведення будь-яких робіт в області ІБ (в тому числі і аудиту) є стандарти:

ISO 15408 Загальні критерії оцінки безпеки інформаційних технологій - представлені критерії для оцінки механізмів безпеки програмно-технічного рівня, визначено функціональні вимоги безпеки, вимоги до адекватності реалізації функцій безпеки і надійності реалізації цих функцій. ОК дозволяють оцінити рівень захищеності АС організацій.

ISO / IEC 27002 (до 2007р.-ISO / IEC 17799) Інформаційні технології - Технології безпеки - Практичні правила управління ІБ.

4.3.3. Методика проведення інструментальних перевірок

Інструментальні перевірки (ІП) виконуються ***в процесі активного аудиту ІБ***. ІП складаються з набору заздалегідь узгоджених тестів, спрямованих на отримання характеристик про рівень захищеності обраних ППБ.

Методика передбачає тестування можливості несанкціонованого доступу (НСД) до інформації, що обробляється або зберігається в автоматизованій інформаційній системі (АІС), як зсередини організації, так і з зовнішніх мереж. Методика включає **три етапи: аналіз структури АІС, внутрішній аудит, зовнішній аудит.**

На етапі аналізу структури АІС з позицій ІБ проводиться аналіз і інвентаризація інформаційних ресурсів: формується перелік захищених

відомостей; описуються інформаційні потоки, структура і склад АІС; проводиться категорування ресурсів, що підлягають захисту.

На другому етапі - внутрішній аудит АІС включає аналіз налаштувань АІС з точки зору ІБ і аналіз захищеності від небезпечних внутрішніх впливів. Досліджується можливість несанкціонованих дій легальних користувачів комп'ютерної мережі, які можуть привести до модифікації, копіювання або руйнування конфіденційних даних. Аналіз здійснюється шляхом детального вивчення налаштувань безпеки засобів захисту з використанням як загальновживаним (в тому числі входять до арсеналу хакерів), так і спеціально розроблених автоматизованих засобів дослідження уразливості АІС.

Аналізуються такі компоненти АІС:

- засоби захисту персональних комп'ютерів (ПК) - можливість відключення програмно-апаратних систем захисту при фізичному доступі до вимкнених станцій; використання і надійність вбудованих засобів парольного захисту BIOS;

- стан антивірусного захисту - наявність в АІС шкідливих програм, можливість їх впровадження через машинні носії, мережа Інтернет;

- ОС - наявність необхідних налаштувань безпеки;

- парольний захист в ОС - можливість отримання файлів з зашифрованими паролями і їх подальшого дешифрування; можливість підключення з порожніми паролями, підбору паролів, в тому числі по мережі;

- система розмежування доступу користувачів АІС до ресурсів - формування матриці доступу; аналіз дублювання і надмірності в наданні прав доступу; визначення найбільш обізнаних користувачів і рівнів захищеності конкретних ресурсів; оптимальність формування робочих груп;

- мережева інфраструктура - можливість підключення до мережного обладнання для отримання інформації, що захищається шляхом перехоплення і аналізу мережевого трафіку; настройки мережевих протоколів і служб;

- аудит подій безпеки - настройка і реалізація політики аудиту;

- прикладне ПЗ - надійність елементів захисту використовуваних АРМ; можливі канали витоку інформації; аналіз версій програмного забезпечення, на наявність вразливих місць;

- СЗІ: надійність і функціональність використовуваних СЗІ;

- настройка СЗІ.

На третьому етапі- зовнішнього аудиту АІС оцінюється стан захищеності інформаційних ресурсів організації від НСД, здійснюваного із зовнішніх мереж, в тому числі з Інтернет.

Послідовно аналізуються наступні можливості проникнення ззовні:

- отримання даних про внутрішню структуру АІС - наявність на web - серверах інформації конфіденційного характеру; виявлення налаштувань DNS і поштового серверів, що дозволяють отримати інформацію про внутрішню структуру АІС;

- виявлення комп'ютерів, підключених до мережі і досяжних з Інтернет - сканування по протоколам ICMP, TCP, UDP; визначення ступеня доступності інформації про використаний в АІС ПЗ і його версіях; виявлення активних мережевих служб; визначення типу і версії ОС, мережевих додатків і служб;

- отримання інформації про облікові записи, зареєстрованих в АІС із застосуванням утиліт, специфічних для конкретної ОС.

- підключення до доступним мережевих ресурсів - визначення наявності доступних мережевих ресурсів і можливості підключення до них;

- використання відомих вразливостей в програмному забезпеченні мережевих екранів (МЕ), виявлення невірної конфігурації МЕ;

- виявлення версій ОС і мережевих додатків, схильних до атакам типу «відмова в обслуговуванні»;

- тестування можливості атак на мережеві додатки - аналіз захищеності web - серверів, тестування стійкості систем віддаленого управління.

За результатами тестування оформляється **експертний висновок,** що описує реальний стан захищеності АІС від внутрішніх і зовнішніх загроз, що містить перелік знайдених вад в налаштуваннях систем безпеки.

На підставі отриманого висновку розробляються **рекомендації щодо підвищення ступеня захищеності AIC**, з адміністрування систем, щодо застосування СЗІ.

Реалізація методики вимагає постійного оновлення знань про виявлені вади в системах захисту. Не всі етапи методики можуть бути автоматизовані. У багатьох випадках потрібна участь експерта, що володіє відповідною кваліфікацією.

Супровідні послуги. Іноді в ході активного аудиту замовнику пропонується ряд додаткових послуг, безпосередньо пов'язаних з оцінкою стану системи інформаційної безпеки, зокрема - ***проведення спеціалізованих досліджень***.

Найчастіше організація в своїй інформаційній системі використовує спеціалізоване програмне забезпечення власної розробки, призначене для вирішення нестандартних завдань (наприклад, корпоративний інформаційний портал, різні бухгалтерські системи або системи документообігу). Подібні ПЗ унікальні, тому будь-яких готових засобів і технологій для аналізу їх захищеності і відмовостійкості не існує. В даному випадку проводяться спеціалізовані дослідження, спрямовані на оцінку рівня захищеності конкретного ПЗ.

Ще один вид послуг, пропонованих в ході активного аудиту, - ***дослідження продуктивності і стабільності системи, або стрес-тестування*.** Воно спрямоване на визначення критичних точок навантаження, при якій система внаслідок атаки на відмову в обслуговуванні або підвищеної завантаженості перестає адекватно реагувати на легітимні запити користувачів.

Стрес-тест дозволить виявити «вузькі» місця в процесі формування та передачі інформації і визначити ті умови, при яких нормальна робота системи неможлива. Тестування включає в себе моделювання атак на відмову в обслуговуванні, призначених для користувача запитів до системи і загальний аналіз продуктивності.

Питання для самоконтролю

1. Що таке аудит інформаційної безпеки?
2. Яке місце займає аудит в процесах створення захищеної ІС ?
3. Чим відрізняється аудит інформаційних систем від аудиту ІБ?
4. Перелічіть основні напрямки аудиту інформаційної безпеки.
5. В чому полягають цілі робіт з аудиту стану інформаційної безпеки ІС?
6. Приведіть загальну методику проведення аудиту (перевірок) ІТС?
7. Які необхідні вихідні дані для проведення аудиту безпеки?
8. В чому полягають особливості аудиту ІБ комп'ютерних систем?
9. Перелічіть заходи інструментальної перевірки (тести), які можуть включатись в аудит.
10. Що таке модель знання і як її використовує аудитор при аудиті?
11. Що включає аналітичний звіт за результатами активного аудиту?
12. Яке призначення експертного аудиту?
13. Які основні цілі інтерв'ювання керівного складу і технічних фахівців організації?
14. Який зміст офіційного звіту в результаті проведення експертного аудиту?
15. Який зв'язок аудиту на відповідність стандартам з проведенням активного або експертного аудиту?
16. Що таке інструментальні перевірки і як вони проводяться?
17. Які компоненти АІС включають інструментальні перевірки?
18. Що включає зовнішній аудит АІС?

4.4. Використання IBM QRadar SIEM в системі управління подіями інформаційної безпеки

Забезпечення безпеки і безперебійної роботи всієї IT-інфраструктури підприємства є однією з найважливіших і, в той же час, найскладніших завдань сучасного бізнесу. Одне з ключових засобів, що використовується для її вирішення - це SIEM-системи (скорочення від англ. Security information and event management) - системи управління подіями інформаційної безпеки.

Основні завдання, які вирішуються сучасним SIEM-додатком: збір, аналіз і надання користувачеві в зручному вигляді інформації, отриманої з різних мережевих компонентів і пристроїв безпеки. Подібні інструменти дозволяють оперативно і з найменшими затратами реагувати як на вже існуючі, так і на потенційні загрози безпеки IT-інфраструктури компанії.

Згідно зі звітом аналітичного агентства Gartner, що спеціалізується в області IT-рішень, безсумнівними лідерами серед розробників SIEM-систем є компанії Splunk (з продуктом Splunk Enterprise Security), IBM (QRadar Security Intelligence Platform), LogRhythm (NextGen SIEM) і McAfee (McAfee Enterprise Security Manager).

Згідно зі звітом Gartner за 2017 рік, лідером на ринку SIEM протягом останніх 10 років. є IBM Qradar.

IBM QRadar SIEM є однією з найбільш ефективних аналітичних систем безпеки для захисту від різних загроз. Важливим є той факт, що рішення QRadar SIEM підтримує роботу з більш ніж 200 продуктів від провідних виробників і проводить збір, аналіз і кореляцію даних через широкий спектр систем, включаючи мережеві рішення, засоби безпеки, сервери, хости, операційні системи і додатки. Крім того, додатковою перевагою рішення є невисока вартість системи початкового рівня.

При виникненні загроз ІБ або для профілактики і розслідування інцидентів ручної аналіз даних з лог-файлів займає чимало часу і не завжди можливий у зв'язку з завантаженістю персоналу підприємства. В інфраструктурі ИС

підприємства як правило також відсутні автоматизовані спеціалізовані засоби для аналізу даних і кореляції подій безпеки з різних лог-файлів.

Тому виникла необхідність у створенні системи моніторингу подій безпеки для збору, кореляції і аналізу даних про події та загрози безпеці, що надходять від різних інформаційних систем.

При побудові такої системи можна використовувати програмно-апаратний комплекс IBM Security QRadar SIEM (QRadar).

Слід зазначити, що ефективним ознакою застосування IBM QRadar SIEM є поєднання аналітичної діяльності фахівців із забезпечення кібербезпеки (ІБ) і з адміністрування ІС підприємств .

4.4.1. Можливості комплексу IBM QRadar SIEM в вирішенні задач СУІБ

Компанія IBM для захисту від загроз мережевої безпеки пропонує рішення IBM QRadar Security Intelligence Platform, яка надає єдину архітектуру для інтегрування інформації про безпеку та управління подіями (SIEM) і журналами, визначення аномальних ситуацій, аналізу інцидентів, реагування на них, управління настройками і усунення вразливостей .

Єдина архітектура QRadar дозволяє вирішувати завдання:

- аналізувати журнали, мережеві потоки, пакети, уразливості, а також дані про користувачів і ресурсах;
- використовувати можливості Sense Analytics для проведення аналіз кореляції для виявлення найбільш серйозних загроз, атак і вразливостей в реальному часі;
- розставляти пріоритети і виділяти найбільш важливі інциденти з величезного потоку даних;
- автоматично реагувати на інциденти і виконувати нормативні вимоги за рахунок можливостей збору даних, визначення їх кореляції і складання звітності.
- прогнозувати аналіз наявних ризиків, викликаних некоректним настроюванням пристроїв і відомими уразливими.

SIEM - це система управління подіями інформаційної безпеки, яка може заздалегідь виявити атаки, слабкі і вразливі місця в інфраструктурі компанії.

Компанія IBM включила в платформу QRadar Security Intelligence Platform кілька модулів:

- QRadar SIEM, Log Manager (управління журналами),
- Risk Manager (управління ризиками), Vulnerability Manager (управління уразливими),
- колектори QFlow і VFlow і Incident Forensics.

Основні модулі IBM QRadar представлені на рис.4.9.

Рис.4.9. Основні модулі IBM Qradar

Одним з ключових компонентів рішення є інструмент IBM QRadar SIEM - система збору та аналізу подій. Він консолідує інформацію з журналів подій, що надходить від пристроїв, кінцевих точок і додатків в мережі. QRadar SIEM нормалізує і аналізує кореляцію для виявлення загроз безпеки, а також використовує передовий механізм Sense Analytics для виявлення нормального

поведінки, виявлення аномалій, розкриття передових загроз і видалення хибно позитивних результатів. Цей програмний модуль дає можливість зібрати всі пов'язані події в один інцидент.

QRadar SIEM може включати в себе кошти аналізу загроз IBM X-Force Threat Intelligence зі списком потенційно шкідливих IP-адрес, адрес комп'ютерів з шкідливим ПЗ, джерел спаму та інших загроз, що дозволяє впровадити попереджуючий підхід до забезпечення безпеки. Крім того, для визначення пріоритетів продукт вміє зіставляти загрози для систем з подіями і даними з мережі. Докладні звіти щодо доступу до даних і дій користувачів забезпечує більш ефективне управління погрозами і відповідність стандартам.

QRadar SIEM можна також використовувати в локальних і хмарних середовищах.

IBM планує використовувати платформу штучного інтелекту Watson в сфері безпеки, інтегрувавши її з програмним забезпеченням QRadar і базою даних X-Force. Це дозволить підвищити рівень аналітики для визначення характеру загроз, а також компенсувати брак IT-персоналу в сфері інформаційної безпеки.

Функціональні можливості IBM QRadar SIEM

Забезпечення прозорості в реальному часі надходження від комутаторів і маршрутизаторів - даних мережевих потоків, включаючи дані рівня 7 (рівень додатків). Це дозволяє:

- виявити неправильне використання додатків, внутрішнє шахрайство і невеликі загрози, які можна було б випустити з уваги серед мільйонів подій, що відбуваються щодня;
- забезпечити збір журналів і подій з різних джерел, включаючи пристрої безпеки, операційні системи, програми, бази даних та системи управління доступом та ідентифікацією;
- отримувати інформацію від контролю доступу та ідентифікацією і таких служб інфраструктури, як протокол динамічної настройки вузла (DHCP), а також від сканерів уразливості в мережі і додатках.

- виконує миттєву нормалізацію подій і зіставлення з іншими даними для виявлення загроз і створення нормативних звітів;

- визначати пріоритети подій, виділяючи невелика кількість реальних порушень, які несуть найбільш серйозну загрозу для бізнесу.

- виявляти аномалії викликають зміни, пов'язані з додатками, комп'ютерами, користувачами і сегментами мережі (при використанні програмного забезпечення IBM X-Force Threat Intelligence визначаються також дії, пов'язані з підозрілими IP-адресами.

- більш ефективно управляти погрозами, відстежуючи серйозні інциденти та надаючи посилання на всі необхідні дані для проведення аналізу (дозволяє виявити дії в неробочий час або незвичайне використання додатків і хмарних сервісів, а також мережеву активність, яка не відповідає збереженим шаблонам використання.);

- використовувати пристрої IBM QRadar QFlow і IBM QRadar VFlow Collector для глибокого розуміння і кращого відображення додатків, баз даних і продуктів для спільної роботи і соціальних мереж (дозволяють проводити детальний аналіз мережевих потоків на рівні 7);

- отримувати оперативну інформацію про безпеку в хмарних середовищах (збір подій і потоків даних від програм виконується як в хмарі, так і на локальних ресурсах) - в разі установки в хмарі SoftLayer QRadar SIEM;

- створювати звіти про доступ до даних і активності користувачів з можливістю відстеження інформації по імені і IP- адресою, що гарантує дотримання політик безпеки, а також відповідність нормативним вимогам.

Панель управління IBM QRadar SIEM представлена на рис.4.10. На панель можна вивести всі необхідні звіти і графіки.

Рис.4.10. Панель управління IBM QRadar SIEM

Основні переваги для впровадження IBM QRadar на підприємстві:

- Проста конфігурація і розгортання на локальних ресурсах і в хмарної середовищі.
- Відображення подій в реальному часі або за результатами минулих періодів.
- Комплексне виявлення інцидентів і управління уразливими.
- Сильні аналітичні можливості завдяки яким QRadar використовує контекст для підозрілих інцидентів, що призводить до масивного скорочення даних і більш високій швидкості виявлення інцидентів.
- Можливість надавати аналіз поведінки і відхилень даних мережевого потоку і журналів.
- Дані потоку (мережевий трафік) і дані подій об'єднані в єдину панель, що дозволяє користувачам точно визначати пріоритети даних про інциденти, зменшуючи кількість помилкових спрацьовувань.

• IBM Security App Exchange дозволяє клієнтам, діловим партнерам та іншим розробникам створювати додатки, що розширюють можливості QRadar.

• Інтегрується з усіма відповідними продуктами IBM і багатьма сторонніми постачальниками.

Одним з найбільш важливих є QRadar Risk Manager, який зіставляє інформацію про уразливість з даними про топологію мережі і з'єднаннях. Рішення виявляє уразливості в мережі компанії і працюють в ній додатках, оцінивши ризики і мінімізувавши їх. Risk Manager відстежує конфігурацію комутаторів, маршрутизаторів, мережевих екранів і систем запобігання вторгнень (IPS), розпізнаючи умови, що представляють загрозу безпеці. Крім того, він дозволяє моделювати мережеві атаки та інші сценарії вторгнень, вносячи в конфігурацію мережі зміни, які дають можливість оцінити масштаб загрози.

Ще один цікавий інструмент - **модуль QRadar Log Manager**. Він збирає і обробляє дані про події в режимі реального часу, що надходять від маршрутизаторів, комутаторів, брандмауерів, мереж VPN, систем виявлення і запобігання вторгнень (IDS / IPS), антивірусних програм та інших джерел. Log Manager дає можливість спростити ведення необхідної звітності та контроль за дотриманням нормативно-правових вимог.

4.4.2. Побудова системи моніторингу подій безпеки на основі IBM QRadar SIEM

Цілями створення системи моніторингу подій безпеки (СМПБ) для компанії є:

• відповідність вимогам документів щодо забезпечення ІБ в частині, пов'язаній з моніторингом подій безпеки, виявленням і реагуванням на інциденти, а також контролем інформаційної безпеки;

• організація процесу збору, обробки та зберігання даних про події ІБ;

• організація процесу швидкого доступу, пошуку, категорування даних про події ІБ;

• організація процесу оперативного і ефективного реагування на інциденти ІБ;

• мінімізація ризиків ІБ і прийняття превентивних заходів до нанесення шкоди шляхом оптимізації процесу управління інцидентами ІБ;

Завдання, які повинна вирішувати СМПБ:

- збір і централізоване зберігання даних про події ІБ;
- контроль активності користувачів, пристроїв, додатків;
- кореляція і аналіз подій ІБ від різних джерел;
- формування інцидентів інформаційної безпеки;
- допомога в проведенні розслідувань інцидентів;
- попередження про потенційні загрози безпеки;
- оцінка вразливостей ІС;
- зниження ризиків виникнення інцидентів безпеки.

Процес роботи СМПБ і порядок взаємодії компонентів системи складається з наступних кроків:

• аналізу подій (на основі IBM QRadar SIEM) збирає (отримує) події з пристроїв IT-інфраструктури (маршрутизатори, MCE, сервера, додатки і т.д.).

• збору мережевого трафіку (на основі IBM QRadar QFlow) отримує дані про мережеві потоках з ЛВС (через «віддзеркалювати» порт комутатора) і перенаправляє їх на підсистему аналізу подій.

• аналізу подій виробляє нормалізацію вихідних подій (приведення до єдиного формату). Події фільтруються і агрегуються (опціонально) у відповідність із заданою конфігурацією.

• аналізу подій робить аналіз і кореляцію подій, використовуючи дані про загрози, мережеві потоки, вразливості, активи IT-інфраструктури та зберігає

отримані події в сховищі подій.Отримані події безпеки викликають спрацьовування правил кореляції і створюють інциденти безпеки.

Інциденти безпеки зберігаються в базі інцидентів.

Користувачі системи переглядають інциденти і звіти про події, що відбулися і забезпечують їх дозвіл до розслідування.

Як **апаратні платформи для компонентів СМПБ** використовуються наступні пристрої:

• IBM QRadar QFlow Collector 1201

• IBM QRadar Core Appliance 3105

Плафторми IBM QRadar QFlow Collector 1201 дозволяє збирати мережевий трафік на рівні додатків (7 рівень моделі OSI) і передавати дані про трафік на IBM QRadar Core Appliance 3105.

Платформа IBM QRadar Core Appliance 3105 представляє комбінований програмно-апаратний комплекс, який забезпечує функції збору, аналізу, кореляції і зберігання даних. Цей пристрій підтримує роздільну нарощування продуктивності до 5000 подій в секунду (EPS) при сталому потоці подій шляхом програмного поновлення ліцензії, без необхідності заміни, розширення або придбання нової апаратної частини, підтримує підключення не менше 1000 мережевих пристроїв, забезпечує збір і обробку не менше 25 000 мережевих потоків в хвилину

Пристрій IBM QRadar Core Appliance 3105 включає:

- Колектор збору інформації (Event Collector);
- Оброблювач подій (Event Processor) для аналізу подій і мережевих потоків;

Внутрішнє сховище для подій і мережевих потоків.

Підсистема аналізу подій (на основі IBM QRadar SIEM) забезпечує кореляцію подій, довгострокове зберігання подій безпеки і мережевих потоків, їх архівацію і формування звітів.

Продуктивність комплексу забезпечує підключення до 750 джерел подій і обробку не менше 500 подій в секунду (Events per Second, EPS) при сталому

потоці подій (Sustained Rate). Події, як нормалізовані, так і ненормалізованние (raw), а також мережеві потоки, зберігаються в єдиній високопродуктивної спеціалізованій базі даних для зберігання і подальшої обробки.

Підсистема забезпечує збір, обробку та відображення подій в реальному часі, а також забезпечує повнотекстовий пошук по подіях.

Підсистема аналізу подій включає спеціалізований агент WinCollect, що встановлюється на засновані на Windows пристрої у вигляді ПО. Агент WinCollect дозволяє збирати логи з ОС Windows і додатків і перенаправляти їх на IBM QRadar SIEM.

Для збору подій з інфраструктури компанії використовуються наступні протоколи:

• Syslog;

• NetFlow;

• Програмний агент WinCollect;

• Microsoft Exchange protocol;

• IBM AIX

Підсистема аналізу подій автоматично виробляє виявлення джерела подій після отримання кількох лог-повідомлень за певний проміжок часу. Всі **отримані дані** представляються **за трьома категоріями**:

Події (events);

Потоки мережевих даних (flows);

Інформація про уразливість (Vulnerability assessment).

Підсистема аналізу подій забезпечує прийом і обробку подій з компонентів всієї IT-інфраструктури.

Підсистема збору мережевого трафіку (на основі IBM QRadar QFlow Collector)

Підсистема збору мережевого трафіку функціонує на програмно-апаратному комплексі IBM QRadar SIEM All-In-One Hardware Appliance 2100 Light і проводить збір мережевого трафіку на SPAN («дзеркальних») портах і виконує профілювання трафіку до рівня 7 (рівня додатків), тим самим допомагає

краще зрозуміти і побачити програми, бази даних, продукти для спільної роботи і соціальні мережі за допомогою глибокого аналізу мережевих пакетів (на рівні 7).

На підставі аналізу типу додатків підсистема виробляє виявлення поведінки додатків в мережі і виявляє поведінкові аномалії мережевого трафіку на рівні додатків.

Основним призначенням СМПБ є формування інцидентів інформаційної безпеки, що виникають в корпоративній інформаційній інфраструктурі.

Для формування інцидентів інформаційної безпеки необхідно функціонування правил кореляції подій інформаційної безпеки, що надходять від різних джерел або мережевих потоків.

Технічне рішення передбачає такі категорії загроз інформаційній безпеці (табл.4.6).

Таблиця 4.6.

Категорії загроз інформаційній безпеці

Категорія	Опис
Аномалія	Правилами повинні визначатись потенційно небезпечні події , коли поведінка хосту або мережевого трафіку являються підозрілими (наприклад, фрагментація пакетів або відомі техніки обходу систем виявлення вторгнень).
Аутентифікація	Правилами повинні визначатись події , що відносяться до аутентифікації користувачів , груп або зміненню привілегій акаунтів (наприклад , вхід і вихід користувачів з системи).
Експлоїт	Правилами повинні визначатись події , зв’язані з спробами експлуатації експонентів , переповнення буферами або атаки , використовуючи вразливості web додатків.
Величина регулювання	Правилами повині визначатись параметри значення і достовірності подій і мережевих потоків для формування інцидентів.

Продовження табл.4.6.

Категорія	Опис
Підозріла активність	Правилами повинні визначатись події, пов’язані з виявленням сканування мережі або іншими техніками , застованими для пошуку і визначення мережевих ресурсів.
Система	Правилами повинні визначатись події, пов’язані з системними змінами , встановленням ПО або інформаційними службовими повідомленнями .
Шкідливе ПО	Правилами повинні визначатись події, пов’язані з вірусними атаками або іншими формами активності шкідливого програмного забезпечення (трояни, шпіони, малваре).
Ботнети	Правилами повині визначатись події, пов’язані з виявленням активностей мереі ботнетів (наприклад , якщо локальний хост намагається встановити з’єднання з відомою мережою ботнетів).
Порушення політики	Правилами повині визначатись події, пов’язані з порушенням корпоративних політик безпеки або загальноприйнятих рекомендацій з безпеки.
Відповідність стандартам	Правилами повині визначатись події, визначені як небажані або потенційно небезпечні з точки зору.
База даних	Правилами повині визначатись події, які відносяться до роботи з базами даних , наприклад, змінення прав доступу до бази даних з недовіреної мереі або не в робочий час.

У разі виникнення інциденту СМПБ формує відповідний запис у Переліку інцидентів і відправляє повідомлення адміністратору через поштовий сервер

Для оптимального функціонування механізмів кореляції і виділення найбільш критичних подій безпеки визначаються наступні **параметри в системі**:

1. Вказуються значення ***важливості ресурсів***.

2. Вказуються ***параметри мережевої ієрархії*** (ім'я мережі, маска мережі, критичність мережі, основні вузли мережі).

3. Для ресурсів задаються ***параметри операційних систем і використовуваних додатків*** (номерів портів).

Щоб дозволити або заборонити доступ і розмежування виконуваних дій в СМПБ використовується **рольове управління**.

Кожна створювана роль може визначати повноваження доступу до всієї системи СМПБ (через інтерфейс управління). При створенні ролі є можливість визначити доступ або до всіх дій, або розмежувати адміністративні повноваження з управління системою та повноваження з моніторингу (перегляду). При цьому кожному користувачеві може призначатися кілька ролей.

Технічні рішення передбачають створення в СМПБ **чотирьох типів ролей:**

1. Роль, яка забезпечує адміністративні повноваження до управління системою.

2. Роль, яка забезпечує управління правилами, конфігураціями і системними настройками.

3. Роль, яка забезпечує управління інцидентами.

4. Роль, яка дозволяє тільки переглядати дані СМПБ.

Для роботи компонентів СМПБ і взаємодії їх між собою повинна бути налаштована:

1. Маршрутизація трафіку між підсистемою аналізу подій і підсистемою збору мережевого трафіку

2. Маршрутизація трафіку між підсистемою аналізу подій і джерелами подій в мережі підприємства.

Для входу в IBM QRadar SIEM використовується веб-додаток. QRadar використовує дані для входу за замовчуванням для URL, ім'я користувача і пароль.

Інтерфейс IBM QRadar SIEM забезпечує вкладки, які дозволяють здійснювати переміщення і фокусування уваги на певних фрагментах зібраних, проаналізованих і відображених даних.

Функціональність ділиться на вкладки призначеного для користувача інтерфейсу. При вході в систему відображається (за замовчуванням) вкладка

«Панель моніторингу» (Dashboard). Доступні п'ять панелей інструментів (за замовчуванням.) Кожна панель інструментів має елементи, які містять зведену та детальну інформацію про порушення, які відбуваються в мережі. Також можна створити призначену для користувача панель моніторингу, щоб можна було зосередитися на своїх функціях з безпеки або мережевим операціям. При вході в систему вкладка «Панель моніторингу» (Dashboard) є поданням за замовчуванням. Вона забезпечує середу робочого простору, яка підтримує кілька інформаційних панелей, на яких можна відображати уявлення про мережевої безпеки, активності або зібраних даних і відстежувати поведінку події безпеки.

На вкладці «Панель моніторингу» представлені **п'ять панелей моніторингу за замовчуванням**, які орієнтовані ***на безпеку***, ***активність мережі***, ***активність додатків***, ***моніторинг системи*** і ***її відповідність***. На кожній панелі відображається набір елементів панелі, які служать відправною точкою для переходу до більш докладним їх даними.

1. Вкладка «Порушення» (Offenses) дозволяє переглядати порушення, які відбуваються в мережі, використовуючи різні варіанти навігації або пошукові запити. На вкладці можна досліджувати (розслідувати) порушення, щоб визначити основну причину проблеми або її вирішити.

2. Вкладка «Активність журналу» (Log activity) дозволить відстежувати журнали подій, що відправляються на QRadar в режимі реального часу, виконувати пошуки і переглядати активність журналу, використовуючи

настроюються діаграми часових рядів. Вкладка «Активність журналу» дозволить провести поглиблене дослідження даних про події.

3. Вкладка «Активність мережі» або «Мережева активність», (Network activity) використовується для дослідження потоків, які відправляються в режимі реального часу, виконання пошуку та перегляду мережевої активності, використовуючи настроюються графіки часових рядів.

Перегляд інформації про потік дозволяє визначити, як передається трафік, що передається (якщо включений режим захоплення контенту) і хто спілкується. Дані потоку також включають в себе протоколи, значення ASN, значення IFIndex і пріоритети.

4. Вкладка «Активи» (Assets). QRadar автоматично виявляє активи, сервери і хости, що працюють в мережі. Автоматичне виявлення засноване на даних пасивного потоку і даних про уразливість, дозволяючи QRadar створювати профіль активів. Активи надають інформацію про кожного відомому ресурсі в мережі, включаючи інформацію про особу, якщо така є, і які служби працюють для кожного активу. Дані профілю використовуються для кореляції, щоб зменшити помилкові спрацьовування.

5. Вкладка «Звіти» (Reports). На вкладці «Звіти» можна створювати, поширювати і управляти звітами для будь-яких даних в QRadar.

Функція «Звіти» дозволяє створювати персоналізовані звіти для оперативного і виконавчого використання. Щоб створити звіт, необхідно

об'єднати інформацію (наприклад, безпеку або мережу) в один звіт. Також можна використовувати попередньо шаблони звітів, які включені в QRadar.

Вкладка «Звіти» також дозволяє створювати свої звіти за допомогою настроюваних логотипів. Ця настройка корисна для поширення звітів - в різних аудиторіях.

6. Вкладка IBM QRadar Risk Manager

IBM QRadar Risk Manager - це окремо встановлений пристрій для моніторингу конфігурацій пристроїв, моделювання змін в мережевому середовищі і визначення пріоритетності ризиків та вразливостей в мережі.

IBM QRadar Risk Manager використовує дані конфігурації з мережі і пристрої безпеки, такими як брандмауери, маршрутизатори, комутатори або IPS, джерела вразливостей і джерела безпеки постачальників. Ці дані використовуються для визначення ризиків безпеки, політики і відповідності в інфраструктурі мережевої безпеки і ймовірності тих ризиків, які використовуються.

Питання для самоконтролю

1. Перелічите основні завдання, розв'язувані сучасним Siem-Додатком.

2. Які компанії у світі є лідерами серед розроблювачів Siem-Систем?

3. Приведіть завдання, розв'язувані IBM Qradar Security Intelligence Platform.

4. Які модулі включаються в платформу IBM Qradar і їх основні можливості?

5. Розкрийте функціональні можливості IBM Qradar SIEM.

6. У чому основні переваги для впровадження IBM Qradar на підприємстві?

7. У чому полягають завдання СМПБ?

8. Розкрийте кроки роботи СМПБ і порядок взаємодії її компонентів.

9. Перелічите категорії загроз інформаційної безпеки, пов'язані з небезпечними подіями.

10. Перелічите назви п'яти доступних панелей інструментів на вкладці «Панель моніторингу» (Dashboard) моделі IBM Qradar SIEM.

Список використаної літератури

1. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко. Київ: ДУТ, 2015. 345 с. URL: http://www.dut.edu.ua/uploads/l_1242_54311567.pdf https://app.box.com/s/g7bqinazmw3i52kp43qizon9v6u9ryxd .
2. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020.-256 с. URL: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf
3. Данілова Е.І. Концепція системного підходу до управління економічною безпекою підприємства. Монографія. Вінниця: Європейська наукова платформа, 2020. 342с. URL: https://ojs.ukrlogos.in.ua/index.php/monograph/article/view/danilova.kontseptsiia-2020/1859.
4. Домарев В.В. Моделирование процессов создания и оценки эффективности систем защиты информации. URL:http://citforum.ru/security/articles/model_proc/.
5. Кузнецов В.В. Системный анализ: учебник и практикум для академического бакалаври ата. В. В. Кузнецов и др.; под общ. ред. В. В. Кузнецова. Москва : Издательство Юрайт, 2018. 270 с. URL: https://biblio-online.ru/viewer/489A965E-87FC-474C-A640-0330297E28EE/sistemnyy-analiz#page/26 .
6. Маркіна І.А. Основи формування системи менеджменту інформаційної безпеки підприємства. URL: http://dspace.pdaa.edu.ua:8080/bitstream/123456789/3092/1/piprp_2016_3%281%29__18.pdf .
7. Оразбаев Б.Б. Теория и методы системного анализа: учебное пособие. Москва: Издательский дом Академии Естествознания, 2017. 248 с. URL: https://www.monographies.ru/docs/2017/12/file_5a44d16054af5.pdf , https://monographies.ru/ru/book/view?id=749 .
8. Роїк О. М. Системний аналіз. Навчальний посібник. О. М. Роїк, А. А. Шиян, Л.О. Нікіфорова. Вінниця : ВНТУ, 2015. 83 с. URL: http://nikiforova.vk.vntu.edu.ua/file/bfb63146b18f718fe1ff1ed4ce9b9a58.pdf .
9. Созинов В.А. Исследование систем управления. URL: http://abc.vvsu.ru/Books/issled_sist_upr/page0038.asp#xex122.

10. Филиппов, С. Д. Теория систем и системный анализ : учеб. пособие / С. Д. Филиппов, П. С. Гончарь. – Екатеринбург : УрГУПС, 2018. – 155 с.

11. Швець С. В. Основи системного аналізу : навчальний посібник / С. В. Швець, У. С. Швець. – Суми : Сумський державний університет, 2017. – 126 с.

12. Ямашкин Ю. В. Системный подход к организации: учебно-методическое пособие. Ю. В. Ямашкин, О.А. Новокрещенова; Мордов. гос. ун-т. Саранск, 2016. 195 с. URL: https://www.mrsu.ru/ru/getfile.php?ID=75685 .

13. Закон единства анализа и синтеза. Анализ и синтез как методы исследования и проектирования организаций. URL: http://allendy.ru/teoria-org/333-zakon-analiza-i-sinteza.html, http://allendy.ru/teoria-org/333-zakon-analiza-i-sinteza.pdf.

14. КОНДОР+2.2 программный комплекс проверки политики информационной безопасности компании. URL: http://sec4all.net/kondor.html.

15. Метод анализа иерархий: пример расчета в excel коэффициентов значимости (весовых коэффициентов) подходов к оценке при определении итоговой стоимости бизнеса (формат Excel) URL: www.vamocenka.ru/metod-analiza-ieratxij-primer-resheniya-zadachi-v-ocenke/ .

16. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України. URL: https://zakon.rada.gov.ua/laws/show/v0365500-11.

17. Побудова Системи управління інформаційною безпекою (СУІБ). URL: https://zahyst-ua.com/pobudova-sistemi-upravlinnya-informacijnoju-bezpekoju-suib/.

18. Система управления событиями информационной безопасности IBM QRadar. URL: https://pirit.biz/reshenija/informacionnaja-bezopasnost/sistema-upravleniya-sobytiyami-informacionnoj-bezopasnosti-ibm-qradar/ .

19. Savchenko V. Coordination Model for the National Cyber Security System of Ukraine / V. Savchenko, S. Kononenko. V. Bobylov, L. Drok // Сучасні інформаційні технології у сфері безпеки та оборони. – К.: НУОУ, 2017, № 1 (28).

20. Савченко В. А. Нейромережева технологія виявлення інсайдерських загроз на основі аналізу журналів активності користувачів / Савченко В. А., Савченко В. В., Довбешко С. В., Мацько О. Й., Зідан А. М. // Сучасний захист інформації №4(36), 2018, – С. 40-49.

21. Савченко В. А. Управління ризиками кібербезпеки на основі теоретико-ігрового підходу / Савченко В. А., Мацько О. Й. // Сучасний захист інформації №2(38), 2019 – С. 6-16.

22. Савченко В. А., Моделювання кібератак засобами теорії графів // В. А. Савченко, О. Й. Мацько, С. В. Легомінова, І. С. Полторак, В. В. Марченко // Сучасний захист інформації №4(40), 2019. – С. 6-11.

23. The Model of Secure Social Networks Activity Based on Graph Theory / Pavlo Shchypanskyi, Vitalii Savchenko, Volodymyr Akhramovych, Tetiana Muzshanova, Svitlana Lehominova, Volodymyr Chegrenets // International Journal of Innovative Technology and Exploring Engineering (IJITEE). Volume-9 Issue-4, February 2020, ISSN: 2278-3075 (Online). P 1803-1810.

24. Компонентна модель захисту передачі даних у системі електронного урядування / Пуха М.С., Савченко В.А., Панадій С.В. // Сучасний захист інформації №1(41), 2020. – С. 11-17.

25. Модель трансформації національної системи кібербезпеки в умовах дії гібридних загроз / Боярчук Р. М., Савченко В. А., Мацько О. Й., Новікова І. В. // Сучасний захист інформації №1(41), 2020. – С. 6–10.

26. Модель інформаційного стримування між державами на основі теорії рефлексивних ігор / Савченко В. А., Дзюба Т. М. //Сучасний захист інформації №2(42), 2020. С. 6-18.

27. Основні напрями застосування технологій штучного інтелекту у кібербезпеці / Савченко В. А., Шаповаленко О. Д // Сучасний захист інформації №4(44), 2020. – С. 6–11.

28. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov, V. Savchenko and others. – Kharkiv: PC Technology Center, 2021. – 188 p.

29. Якименко Ю. М. Реализация метода анализа иерархий при обосновании принимаемых управленческих решений по безопасности в организации / Ю. М. Якименко // Сучасний захист інформації. – № 2. – К.: ДУТ, 2015. – С. 54-64. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/337.

30. Якименко Ю. М. Про підхід до створення системи інформаційної безпеки в організації. Інформаційна безпека України: Зб. наук. доп. та тез НТК. Київ: Київський національний університет імені Тараса Шевченка(23-24 березня 2017року). С. 372-376.

31. Якименко Ю. М. Використання метрик для оцінки ефективності управління інцидентами інформаційної безпеки. Матеріали: інтернет-конференція *«Актуальні проблеми інформаційної та кібернетичної безпеки»*(26 жовтня 2018 року). Тези доповідей. Київ: ДУТ(ННІЗІ), 2018. С.69-71.

32. Якименко Ю.М. Застосування системного підходу при організації захисту інформації. Матеріали: інтернет-конференція *«Актуальні проблеми*

*інформаційної та кібернетичної безпеки»(*26 жовтня 2018 року). Тези доповідей. Київ: ДУТ(ННІЗІ), 2018. С. с.44-45.

33. Якименко Ю.М. Особливості реалізації системного методу стосовно побудови систем управління інформаційною безпекою організації. Матеріали: *«Актуальні проблеми управління інформаційною безпекою держави: нові виклики та стратегії протидії*». X Всеукраїнська науково-практична конференція. Збірник тез наукових доповідей. Електронне видання . Київ: Нац. акад. СБУ, 2019. С. 144-147. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf.

34. Якименко Ю. М. Методологічні аспекти впровадження системного аналізу в побудові системи управління інформаційною безпекою. Матеріали: IУ-ої Всеукраїнської Інтернет-конференції «*Професійний розвиток фахівців у системі освіти дорослих: історія, теорія,технології,програма»* (16 жовтня 2019 р.).м. Київ.,за наук. ред. В.В. Сидоренко; упорядкування Я.Л. Швень, М.І. Скрипник. Київ: Агроосвіта, 2019. С.41-43.

35. Якименко Ю. М. Огляд та оцінка стану кібербезпеки в умовах промислової революції (industry 4.0) в Україні Матеріали: конференція *«Цифрова трансформація кібербезпеки»*(26 квітня 2020 року). К.: ДУТ, 2020. С.5-6. URL: http://www.dut.edu.ua/uploads/p_1739_99516793.pdf

36. Якименко Ю. М. Системний аналіз методологічних підходів до управління підприємством у сфері інформаційних технологій. Матеріали: II Міжнародна науково-практична конференції *«Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку»*(11лютого 2021 року). Київ: ДУТ, 2021. С. 279-282. URL: http://www.dut.edu.ua/uploads/n_9074_59003267.pdf

37. Якименко Ю. М. Управління інцидентами інформаційної безпеки в організації системи забезпечення кіберстійкості підприємства. Матеріали Всеукраїнської НПК Інтернет-конференції *«Стратегії кіберстійкості: управління ризиками та безперервність бізнесу»* (25 лютого 2021 року). Київ: ННІЗІ ДУТ, 2021.С.24-25. URL: http://www.dut.edu.ua/uploads/l_2173_91341086.pdf

38. Якименко Ю. М. Методичні піходи системного аналізу до вирішення проблем управління інформаційною безпекою в системі національної безпеки держави. Матеріали: «*Актуальні проблеми управління інформаційною безпекою держави*». XII Всеукраїнська науково-практична конференція. Збірник тез наукових доповідей. Електронне видання . Київ: Нац. акад. СБУ, 2021. С. 162-164.
URL:http://academy.ssu.gov.ua/upload/file/%D0%BA%D0%BE%D0%BD%D1%84

%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D1%8F%2026.03.2021.pdf

39. Якименко Ю. М. Використання спеціалізованих платформ і рішень з безпеки інформації в системному аналізі інформаційної безпеки організацій Матеріали: Всеукраїнська науково-практична інтернет-конференція, *«Цифрова трансформація кібербезпеки»* (25 березня 2021). Тези доповідей . Київ: ДУТ, 2021. С.5-8. URL : http://www.dut.edu.ua/uploads/n_9126_17047934.pdf

40. Мужанова Т.М., Легомінова С.В., Якименко Ю.М., Мордас І.В. *Тех*нології моніторингу й аналізу діяльності користувачів у запобіганні внутрішнім загрозам інформаційній безпеці організації. Електронне фахове наукове видання *«Кібербезпека: освіта, наука, техніка»*, 1(13), 50-62. URL : https://doi.org/10.28925/2663-4023.2021.13.5062.

41. Якименко Ю.М., Мужанова Т.М., Легомінова С.В. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE. Електронне фахове наукове видання *«Кібербезпека: освіта, наука, техніка»*. Київ, 2021. 4(12), 36-50. URL : https://doi.org/10.28925/2663-4023.2021.12.3650 .

42. Якименко Ю. М. Особливості використання методичних заходів захисту інформації підприємства від сучасних видів загроз, кібератак і ризиків. Матеріали: Всеукраїнська наукова конференція, «*Актуальні проблеми кібербезпеки»* (27 жовтня 2021). Київ, ДУТ, 2021. С.173-176. URL: http://www.dut.edu.ua/uploads/p_2099_79407917.pdf

43. ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. (ISO/IEC 27000:2018, IDT) . (ДСТУ ISO/IEC 27000:2017).

44. ДСТУ ISO/IEC 27001:2015.(Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).

45. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. (Ідентичний до міжнародного ISO/IEC 27002:2013 Cor 1:2014).

46. ДСТУ ISO/IEC 27003:2018. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова . (ISO/IEC 27003:2017, IDT) (ISO/IEC 27003:2010).

47. ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. (ISO/IEC 27005:2018, IDT).

48. ДСТУ ISO/IEC 27007:2018. Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою. (ISO/IEC 27007:2017, IDT).

49. ДСТУ ISO/IEC TS 27008:2019.Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки. (ISO/IEC TS 27008:2019, IDT).

50. ДСТУ ISO/IEC 27009:2018. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги. (ISO/IEC 27009:2016, IDT).

51. ДСТУ ISO/IEC 27031:2015. Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу. (ISO/IEC 27031:2011, IDT).

52. ДСТУ ISO/IEC 27035-1:2018.Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки.Частина 1. Принципи керування інцидентами(ISO/IEC 27035-1:2016, IDT).

53. ДСТУ ISO/IEC 27035-2:2018. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти. (ISO/IEC 27035-1:2016, IDT).

54. ДСТУ ISO 19011:2019. Настанови щодо проведення аудитів систем управління. (ISO 19011:2018, IDT).

55. ДСТУ ISO 31000:2018.Менеджмент ризиків. (ISO 31000:2018, IDT).

Навчальне видання

ЯКИМЕНКО Юрій Михайлович
САВЧЕНКО Віталій Анатолійович
ЛЕГОМІНОВА Світлана Володимирівна

СИСТЕМНИЙ АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: СУЧАСНІ МЕТОДИ УПРАВЛІННЯ

ПІДРУЧНИК

2022

309