МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

РАК Андрій Андрійович

Модель управління інформаційною безпекою на основі систем підтримки прийняття рішень / Model of information security management based on decision support systems

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
А.А. Рак

Науковий керівник
д.т.н., професор М.М.Касянчук

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2024 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2024

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь "магістр"
спеціальність:125 – Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
"____"_____20__ р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
РАК Андрій Андрійович

(прізвище, ім'я по-батькові)

1. Тема кваліфікаційної роботи
Модель управління інформаційною безпекою на основі систем підтримки прийняття рішень / Model of information security management based on decision support systems
керівник роботи: д.т.н., проф. М.М.Касянчук
затверджені наказом по університету від 12 грудня 2023 року № 753
2. Строк подання студентом закінченої кваліфікаційної роботи
12 грудня 2024 р.
3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.
4. Основні питання, які потрібно розробити

– визначити основні напрямки заходів щодо забезпечення захисту інформації та управління інформаційною безпекою;

– розробити схему взаємозв'язку ризиків з використанням систем підтримки прийняття рішень;

– визначити ступінь небезпеки та оцінки можливості реалізації загроз інформаційній безпеці з урахуванням систем підтримки прийняття рішень;

– розробити структуру методу управління інформаційною безпекою на основі систем підтримки прийняття рішень

– розробити моделі даних для управління інформаційною безпекою на основі систем підтримки прийняття рішень;

– розробити комплексну модель управління інформаційною безпекою на основі систем підтримки прийняття рішень та розрахувати її ефективність...

5. Перелік графічного матеріалу у роботі.

Схема повного взаємозв'язку параметрів загроз інформаційній безпеці визначеного активу.

Структура методу управління інформаційною безпекою.

Схема моделі взаємодії даних процесу формування та підтримки актуальності інформаційно-довідкової системи з питань інформаційної безпеки.

Схема моделі взаємодії даних процесу управління ресурсами системи захисту інформації.

Схема моделі взаємодії даних процесу управління інформаційною безпекою під час роботи з персоналом організації.

Схема моделі взаємодії даних процесу управління інформаційною безпекою при інформаційному обміні та співпраці з третіми особами.

Комплексна модель управління інформаційною безпекою на основі СППР.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання: 12 грудня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Основні напрямки управління інформаційною безпекою	12.2023 р. – 03.2024 р.	
2	Оцінка методу управління інформаційною безпекою	03.2024 р. – 06.2024 р.	
3	Моделі управління інформаційною безпекою на основі систем підтримки прийняття рішень	06.2022 р. – 11.2024 р.	

Студент _____ Рак А.А.
(підпис)

Керівник роботи _____ д.т.н., проф. Касянчук М.М.
(підпис)

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Модель управління інформаційною безпекою на основі систем підтримки прийняття рішень” на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека та захист інформації” освітньо-професійної програми «Кібербезпека» написана обсягом 81 сторінка і містить 16 ілюстрацій, 3 таблиці, 1 додаток та 31 джерело за переліком посилань.

Метою випускної кваліфікаційної роботи є розробка моделі управління інформаційною безпекою на основі систем підтримки прийняття рішень

Методи дослідження. Методи управління інформаційною безпекою, методи застосування систем підтримки прийняття рішень.

Результати дослідження. Визначено основні напрямки заходів щодо забезпечення захисту інформації та управління інформаційною безпекою, що дозволило розробити схему взаємозв’язку ризиків з використанням систем підтримки прийняття рішень та встановити типові підходи до застосування систем підтримки прийняття рішень для управління інформаційною безпекою. Визначено апріорну можливість реалізації загроз інформаційній безпеці на основі систем підтримки прийняття рішень, що дозволило встановити ступінь небезпеки та оцінку можливості реалізації загроз інформаційній безпеці з урахуванням систем підтримки прийняття рішень. Розроблено структуру методу управління інформаційною безпекою на основі систем підтримки прийняття рішень. Розроблено часткові та комплексну модель для управління інформаційною безпекою на основі систем підтримки прийняття рішень.

Результати роботи можуть успішно застосовуватися в різних установах для управління інформаційною безпекою.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ, ОЦІНКА ЗАГРОЗ, МОДЕЛЬ ДАНИХ.

ABSTRACT

The graduate work on the topic „Model of information security management based on decision support systems” for Master’s degree on speciality 125 "Cybersecurity and Information Protection" is written on 81 pages and contains 16 illustrations, 3 tables, 1 suplements and 31 references.

The aim of graduate work is to develop an information security management model based on decision support systems.

Research methods. Methods of information security management, methods of applying decision support systems.

Results of the study. The main directions of measures to ensure information protection and information security management have been determined, which allowed to develop a scheme of risk correlation using decision support systems and establish typical approaches to the application of decision support systems for information security management. The a priori possibility of implementing threats to information security based on decision support systems has been determined, which allowed to establish the degree of danger and assess the possibility of implementing threats to information security taking into account decision support systems. The structure of the information security management method based on decision support systems has been developed. A partial and comprehensive model for information security management based on decision support systems has been developed.

The results of the work can be successfully applied in various institutions for information security management.

Keywords: INFORMATION SECURITY, DECISION SUPPORT SYSTEM, THREAT ASSESSMENT, DATA MODEL.

ЗМІСТ

ВСТУП

На даний час загальне розуміння цілей та завдань з управління інформаційною безпекою (ІБ) можуть по-різному трактуватися кожним із фахівців, зважаючи на відсутність уніфікованих стандартних підходів та науково-методичного апарату управління ІБ [1-4]. У зв'язку з цим ефективність прийняття рішень щодо ІБ (та їх обґрунтованість) безпосередньо залежить від сукупності досвіду та компетенції експертів, а також урахування специфіки зв'язків та логічних залежностей інформації всередині процесів забезпечення ІБ, що протікають у системі захисту інформації (СЗІ) організації [5-7]. При цьому часові витрати, необхідні для прийняття відповідних управлінських рішень та їх обґрунтування, завжди обмежені, а значить час та коректність ухвалення рішення безпосередньо впливатимуть на показники ефективності СЗІ. З урахуванням обсягів оброблюваної інформації, які постійно збільшуються, а також ускладнення логічних залежностей процесів забезпечення ІБ, ефективність реалізації СЗІ у кожній організації з часом починає погіршуватися. Вирішення цієї ситуації можливе за рахунок розробки та застосування нового науково-методичного апарату управління ІБ, здатного призвести до скорочення часових витрат на прийняття управлінських рішень та суттєво підвищити ефективність СЗІ.

Крім того, проаналізувавши міжнародну та вітчизняну нормативно-правову документацію в галузі інформаційної безпеки та захисту інформації [8-11], результати праць фахівців та вчених у сфері ІБ, а також з урахуванням типового підходу до побудови СЗІ, можна судити про те, що теоретичний та практичний підхід до управління інформаційною безпекою має низку істотних недоліків, що тягне за собою невідповідність уявленням класичного контуру управління, який пов'язує за інформаційних каналах суб'єкти та об'єкти управління [12-15]. В умовах поточного розвитку інформаційної безпеки будь-яка організація стикається зі строго фіксованими вимогами та обмеженнями при побудові системи захисту інформації [16-19], зафіксованих у вигляді

нормативно-методичної документації в галузі ІБ, включаючи власні вимоги до цієї галузі. Механізми забезпечення ІБ часто не передбачають реалізацію зворотного зв'язку між суб'єктами та об'єктами взаємодії та спрямовані лише виконання кінцевого, суворо певного набору функций [20-22]. При цьому можливість удосконалення використовуваних підходів, а також інструментів для проведення детального аналізу даних про стан СЗІ, що змінюються з часом, і виникаючих загроз ІБ просто відсутні [23-25].

Таким чином, основне завдання цього дослідження може бути сформульоване як розробка моделі управління ІБ типової організації по заданих вимогах та обмеженням нормативно-методичної документації в галузі ІБ, які грунтуються на системах підтримки прийняття рішень, які б забезпечили підвищення ефективності СЗІ за рахунок скорочення часових витрат на прийняття управлінських рішень.

Мета роботи. Метою даної роботи є розробка Моделі управління інформаційною безпекою на основі систем підтримки прийняття рішень.

Для вирішення поставленої мети вирішуються наступні **завдання**:

– визначити основні напрямки заходів щодо забезпечення захисту інформації та управління інформаційною безпекою;

– розробити схему взаємозв’язку ризиків з використанням систем підтримки прийняття рішень;

– визначити ступінь небезпеки та оцінки можливості реалізації загроз інформаційній безпеці з урахуванням систем підтримки прийняття рішень;

– розробити структуру методу управління інформаційною безпекою на основі систем підтримки прийняття рішень

– розробити моделі даних для управління інформаційною безпекою на основі систем підтримки прийняття рішень;

– розробити комплексну модель управління інформаційною безпекою на основі систем підтримки прийняття рішень та розрахувати її ефективність.

Об’єкт дослідження. Процес моделювання управління інформаційною безпекою.

Предмет дослідження. Алгоритми та моделі управління інформаційною безпекою на основі систем підтримки прийняття рішень.

Методи дослідження. Математичні методи моделювання, методи управління інформаційною безпекою, методи застосування систем підтримки прийняття рішень.

Наукова новизна одержаних результатів.

1. Визначено основні напрямки заходів щодо забезпечення захисту інформації та управління інформаційною безпекою, що дозволило розробити схему взаємозв’язку ризиків з використанням систем підтримки прийняття рішень та встановити типові підходи до застосування систем підтримки прийняття рішень для управління інформаційною безпекою.

2. Визначено апріорну можливість реалізації загроз інформаційній безпеці на основі систем підтримки прийняття рішень, що дозволило встановити ступінь небезпеки та оцінку можливості реалізації загроз інформаційній безпеці з урахуванням систем підтримки прийняття рішень.

3. Розроблено структуру методу управління інформаційною безпекою на основі систем підтримки прийняття рішень, що дозволило побудувати часткові та комплексну моделі даних процесу управління інформаційною безпекою.

Практичне значення отриманих результатів.

Розроблено часткові та комплексну модель для управління інформаційною безпекою на основі систем підтримки прийняття рішень.

Публікації та апробація КР.

1. Рак А., Залужна В. Структура методу управління інформаційною безпекою на основі систем підтримки прийняття рішень. Матеріали науково-практичного симпозіуму «Захист інформації» (ЗІ-2024). Тернопіль, 2024. С.82-84 [26].

2. Рак А., Прончук Д. Комплексна модель управління інформаційною безпекою та розрахунок її ефективності. Збірник матеріалів проблемної наукової міжгалузевої конференції «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2024). Тернопіль, 2024. С.156-157 [27].

1 ОСНОВНІ НАПРЯМКИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1.1 Визначення основних напрямів заходів щодо забезпечення захисту інформації

Захист інформації, згідно з чинними нормативно-правовими документами, ділитися за такими основними напрямками – організаційна, інженерно-технічна, програмна та спеціальна [28]. Найпоширенішими заходами в організаціях різного роду діяльності зараз є інженерно-технічні та спеціальні. Найбільш логічним поясненням цього стану речей може бути той факт, що до певного етапу розвитку інформаційних технологій в організації такі заходи дають найбільш відчутні та вагомі результати. Однак при відсутності належних механізмів контролю та моніторингу за реалізованими заходами не можна судити про те, наскільки доцільним є їх застосування та яка їх ефективність.

З врахуванням проведеного аналізу нормативно-правової документації з питань забезпечення ЗІ було виявлено такі основні тенденції при формуванні вимог щодо захисту інформації, а саме:

− організація контрольованої зони;

− встановлення контрольно-пропускного режиму;

− реалізація систем моніторингу інформаційної безпеки в контрольованій зоні;

− встановлення об'єктових та периметрових датчиків та засобів захисту;

− організація захисту локальної обчислювальної мережі;

− організація захищеної міжмережевої взаємодії;

− організація захисту серверів та робочих станцій;

− організація розмежування доступу до інформації;

− організація захисту приміщень, в яких відбувається обробка інформації;

− організація резервування інформації та обладнання, які мають бути захищені;

− організація криптографічного захисту інформації;

− організація роботи з інформацією, що захищається;

− організація проведення контролю за захистом та процесами обробки інформації;

− здійснення протоколювання дій, що відбуваються всередині організації;

− організація моніторингу та документування подій інформаційної безпеки;

− організація контролю за відсутністю недекларованих можливостей;

− організація антивірусного захисту;

− регламентація процесів забезпечення захисту інформації;

− організація роботи з персоналом, який здійснює безпосередню обробку інформації та обслуговуючого персоналу організації.

Типова схема побудови СЗІ наведена на рисунку 1.1.

Даний список можна продовжувати і продовжувати, а у разі деталізації кожного з напрямів, що увійшли до списку, будуть народжуватися нові і нові пункти, проте основні тенденції видно і так. Як випливає з вищепредставленого списку, більшість з вимог можливо реалізувати тільки за допомогою технічних, програмних та спеціальних засобів захисту інформації. Проте за відсутності належного ступеня контролю та регламентації здійснення роботи таких засобів, це є тратою ресурсів.

Для прикладу на рисунках 1.2-1.5 наведено відповідно схеми СЗІ при відсутності єдиної підсистеми управління інформаційної системи, зворотного зв’язку між елементами системи, використання автоматизації організаційних заходів, аналітичної складової процесів розвитку та забезпечення СЗІ. Останні два недоліки реалізуються за допомогою систем підтримки прийняття рішень (СППР).

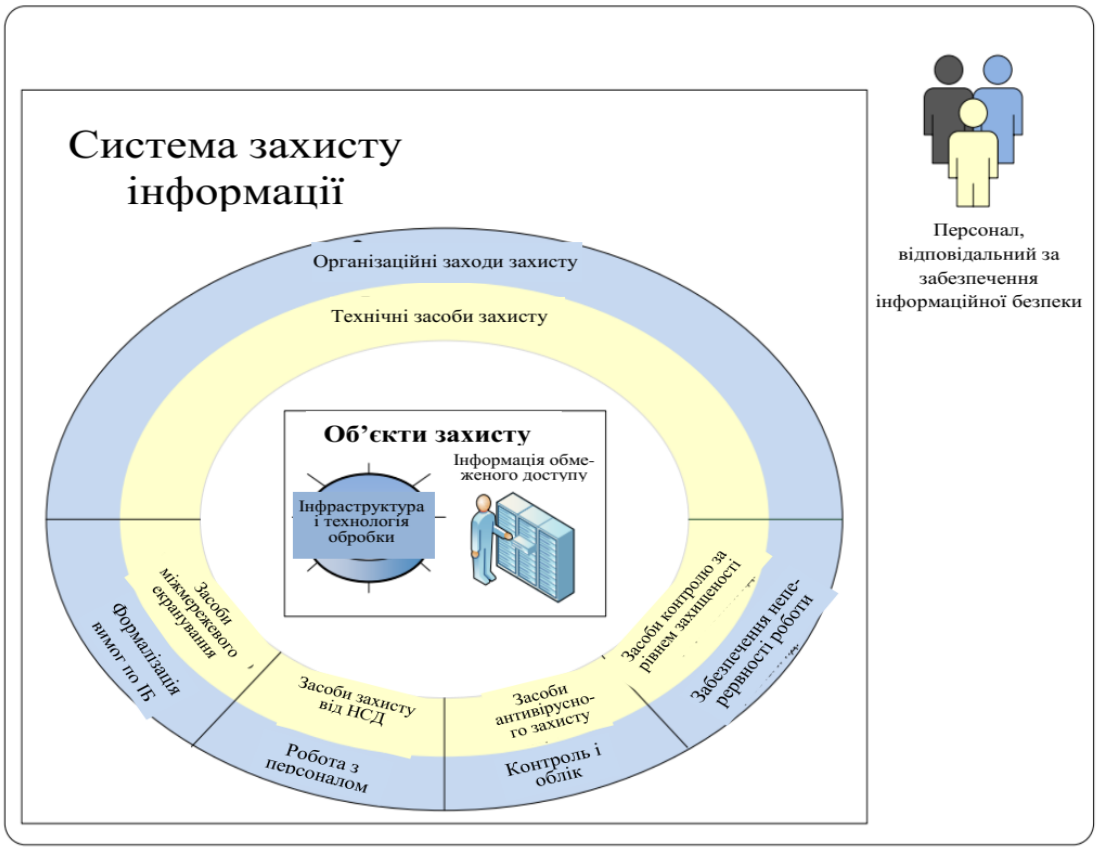

Рисунок 1.1 – Типова схема побудови СЗІ

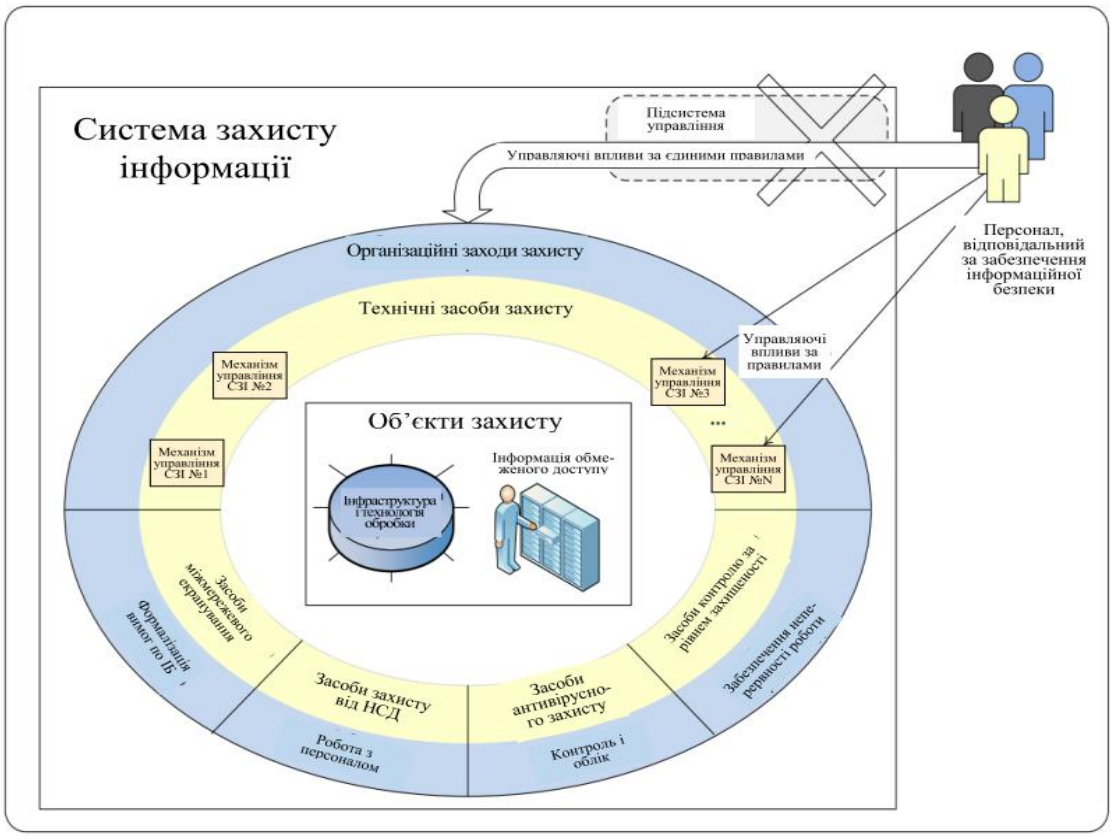

Рисунок 1.2 – Схема СЗІ при відсутності єдиної підсистеми управління інформаційною безпекою

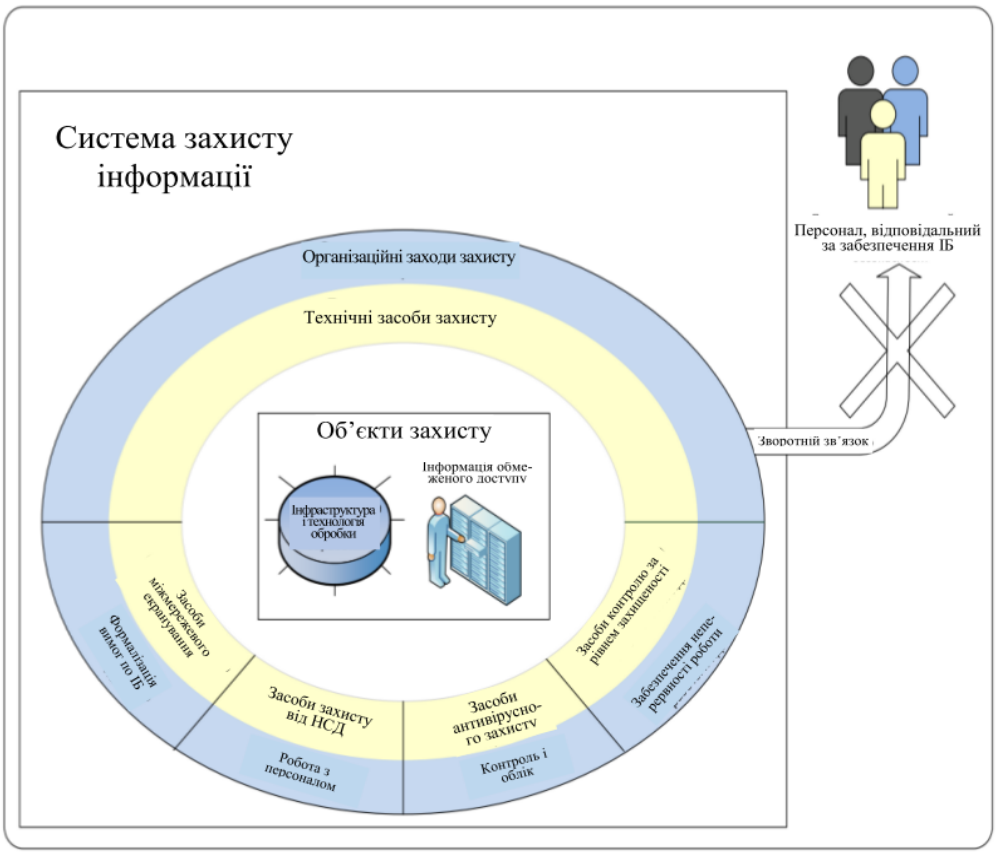

Рисунок 1.3 – Схема СЗІ при відсутності зворотного зв'язку

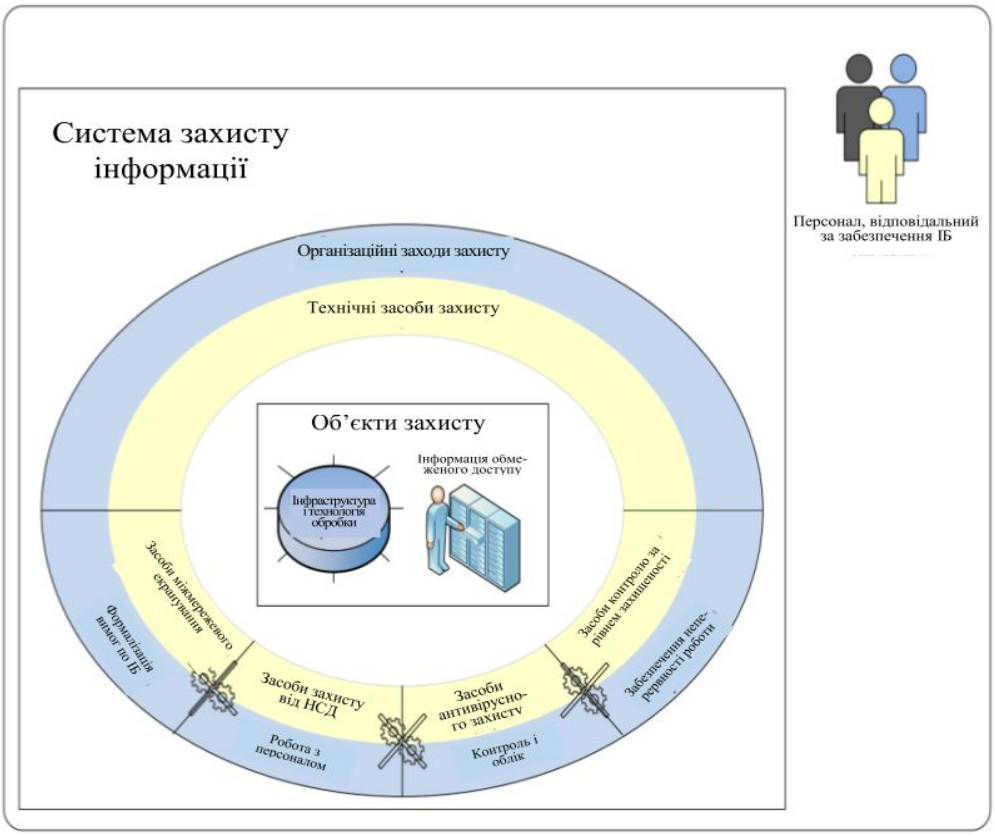

Рисунок 1.4 – Схема СЗІ при відсутності використання автоматизації організаційних заходів

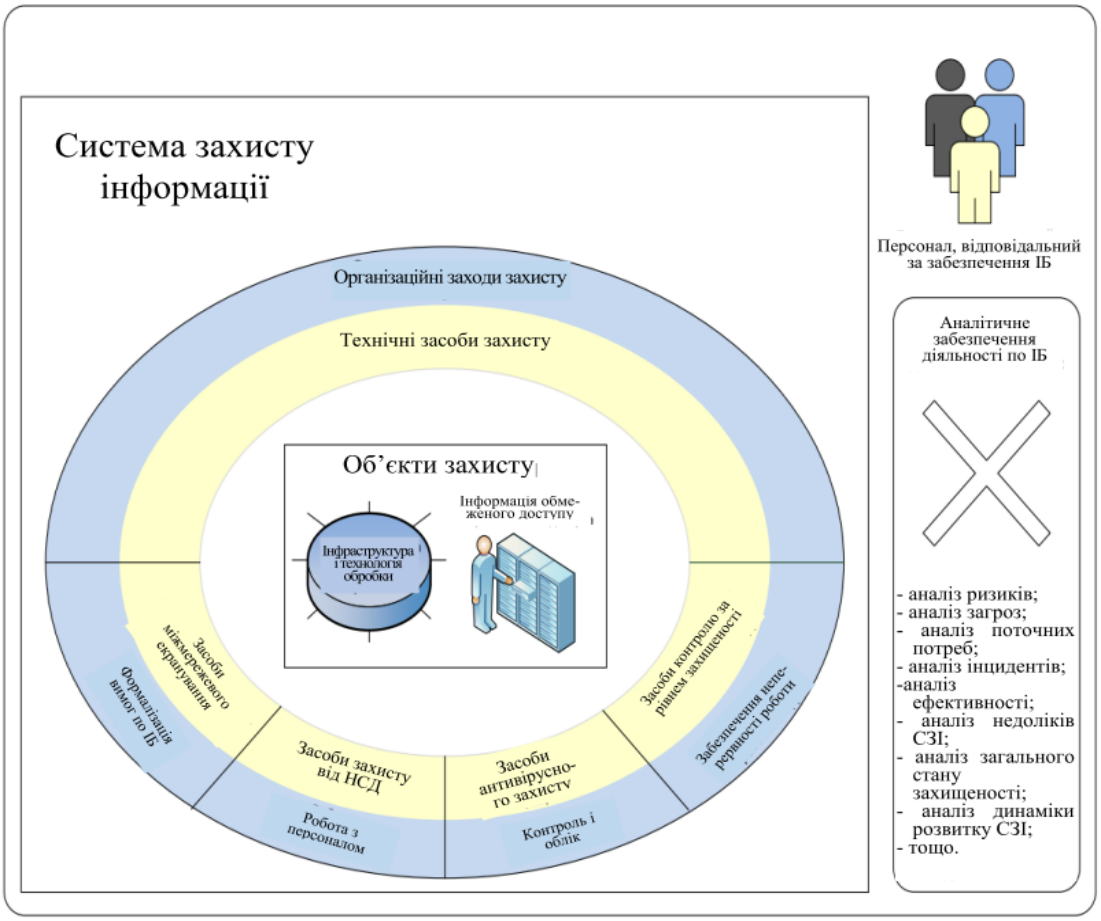

Рисунок 1.5 – Схема СЗІ при відсутності аналітичної складової процесів розвитку та забезпечення СЗІ

Захист інформації є процесом, що потребує комплексного підходу до його здійснення. Таким чином, постає проблема відсутності належного рівня організаційних заходів щодо забезпечення захисту інформації та управління інформаційною безпекою в організаціях різного роду діяльності, що насамперед відображається у відсутності чітких законодавчих та нормативних вимог, що визначають питання управління інформаційною безпекою. За результатами проведеного аналізу нормативно-правової документації з питань забезпечення захисту інформації можна зробити висновок про недосконаліть існуючої нормативно-правової бази та неповну відповідність до вимог або реально затребуваних механізмів захисту інформації (схема взаємозв'язків між документами нарративно-правової бази менеджменту інформаційної безпеки наведена на рисунку 1.6).

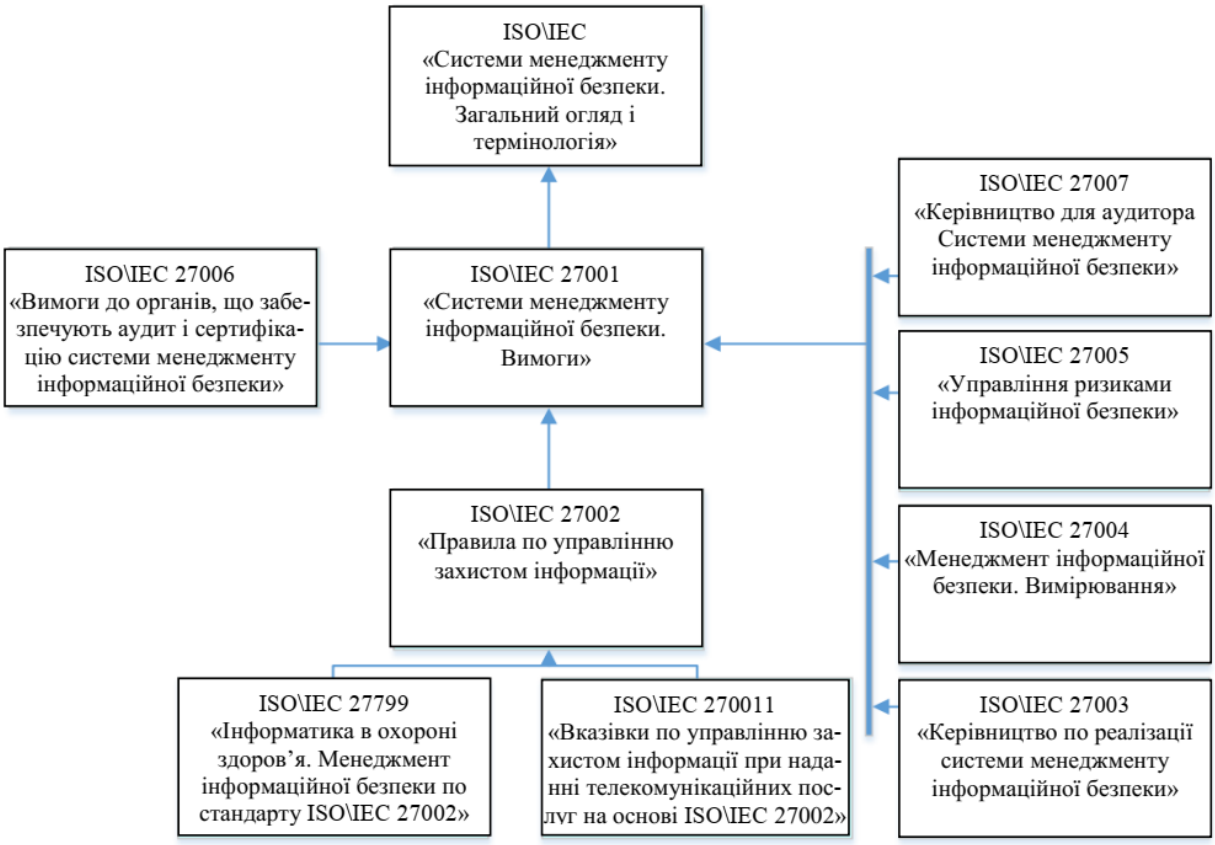

Рисунок 1.6 – Схема взаємозв'язків між документами нормативно-правової бази менеджменту інформаційної безпеки

Грунтуючись на результатах проведеного аналізу вітчизняної та міжнародної нормативно-правової документації [29-30], можна визначити основні напрямки в галузі забезпечення інформаційної безпеки в організаціях різного роду діяльності. До таких напрямів відносяться:

1) забезпечення безперервності роботи інформаційних систем та інформаційно-телекомунікаційних послуг;

2) забезпечення моніторингу, виявлення та реагування на події інформаційної безпеки;

3) забезпечення інформаційної безпеки на різних етапах розвитку інформаційних систем, а також підтримка та продовження життєвих циклів інформаційних систем організації;

4) забезпечення інформаційної безпеки під час здійснення роботи з співробітниками організації, перевищення їх кваліфікації та загальної компетенції щодо питань інформаційної безпеки;

5) забезпечення інформаційної безпеки під час здійснення інформаційного обміну та взаємодії з третіми сторонами;

6) забезпечення раціонального розмежування прав доступу до інформації та інформаційних систем користувачам організації, а також наступного контролю за цим процесом.

Дані напрямки у забезпеченні захисту інформації є основними і до них може бути віднесений будь-який процес у рамках діяльності із захисту інформації, таким чином запроваджуючи єдину систему класифікації діяльності щодо забезпечення інформаційної безпеки. Необхідність пропорційного розвитку кожного з цих напрямків обумовлюється їхньою взаємопов'язаністю. Відсутність належного рівня розвитку одного з напрямів, порівняно з іншими, неминуче призведе до нераціонального та слабоефективного використання ресурсів системи захисту інформації, а також до фінансових втрат з боку організації, не кажучи вже про збільшення ймовірності реалізації загроз інформаційній безпеці та супутньому збільшенню рівня ризику для активів організації.

Враховуючи явний процесний розподіл діяльності цих напрямків, а також асоційовану децентралізацію їх реалізації, забезпечення своєчасного та раціонального управління даними процесами є одним з основних питань сучасної СЗІ. Управління цими напрямами дозволить суттєво спростити реалізацію механізмів СЗІ, простежити за планомірністю розвитку кожного з напрямків та дасть можливість грамотно перерозподілити матеріальні ресурси між напрямами, що допоможе суттєво збільшити ефективність реалізованих механізмів захисту інформації за збереження поточного рівня витрат організації захисту інформації.

На рисунку 1.7 наведено схему управління інформаційною безпекою на основі систем підтримки прийняття рішень в СЗІ

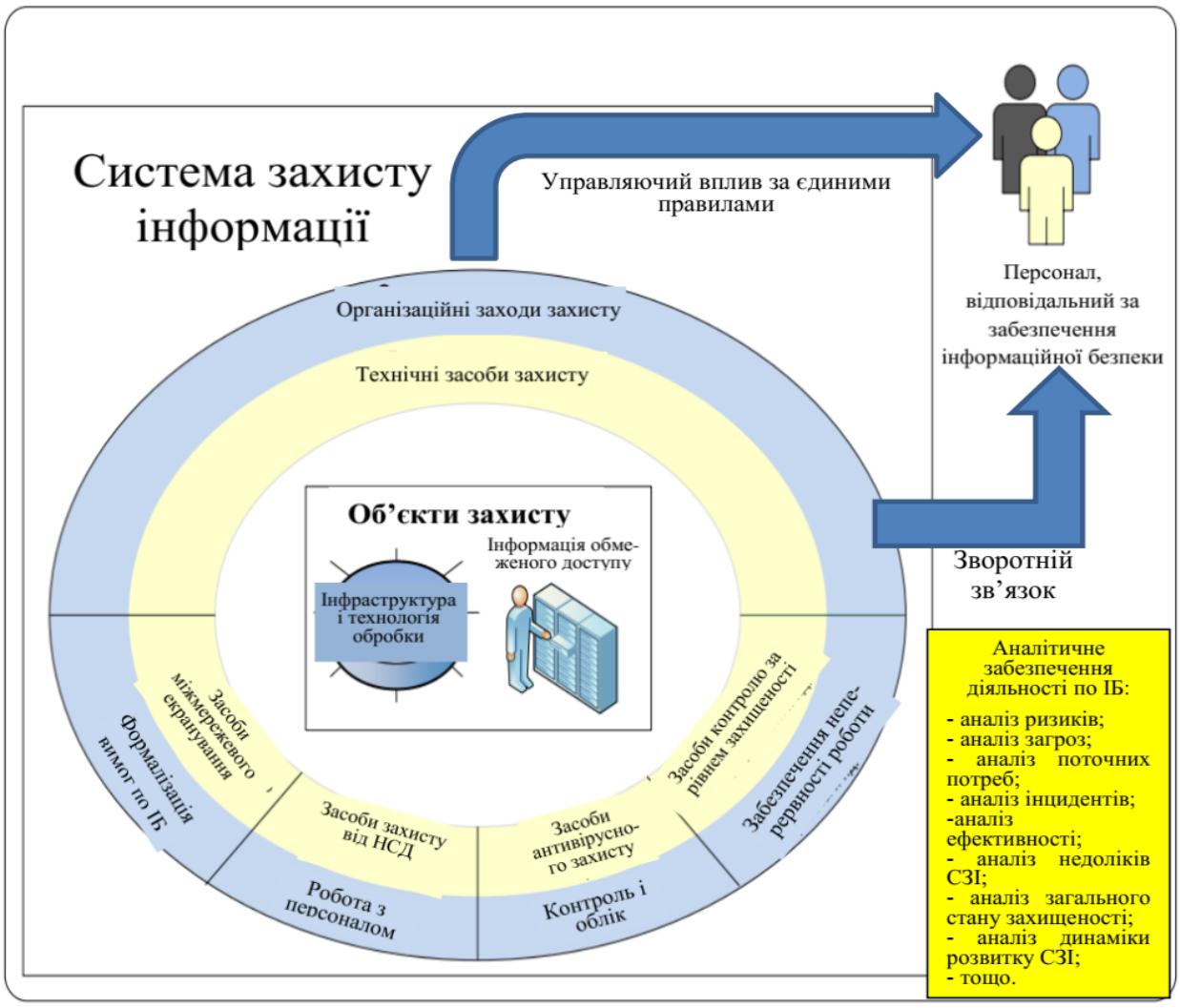

Рисунок 1.7 – Схему управління інформаційною безпекою на основі систем підтримки прийняття рішень в СЗІ

Таким чином, управління процесами забезпечення інформаційної безпеки є важливою, невід'ємною складовою будь-якої СЗІ в кожній організації [31].

1.2 Визначення основних напрямів управління інформаційною безпекою в організаціях різного роду діяльності

Грунтуючись на результатах проведеного аналізу вітчизняної та міжнародної нормативно-правової документації, а також враховуючи основні напрямки у сфері забезпечення інформаційної безпеки, було визначено

основні напрямки в галузі управління інформаційною безпекою в організаціях різного роду діяльності. До підсумкових напрямів управління інформаційною безпекою відносяться:

1) управління активами організації;

2) управління ресурсами СЗІ, реалізованої в організації;

3) управління ризиками та загрозами інформаційній безпеці;

4) управління документацією та інформаційною довідковою системою в організації;

5) управління аудитом інформаційної безпеки;

6) управління аналізом ефективності системи захисту;

7) управління завданнями та діяльністю співробітників, які здійснюють процеси забезпечення інформаційної безпеки в організації;

8) управління процесами забезпечення безперервності роботи інформаційних систем та інформаційно-телекомунікаційних сервісів;

9) управління процесами забезпечення моніторингу, виявлення та реагування на події інформаційної безпеки;

10) управління процесами забезпечення інформаційної безпеки на різних етапах розвитку інформаційних систем, а також підтримання та продовження життєвих циклів інформаційних систем організації;

11) управління процесами забезпечення інформаційної безпеки при здійсненні роботи зі співробітниками організації, підвищення їх кваліфікації та загальної компетенції з питань інформаційної безпеки;

12) управління процесами забезпечення інформаційної безпеки при здійсненні інформаційного обміну та взаємодії з третіми сторонами;

13) управління процесами забезпечення розмежування прав доступу до інформації та інформаційних систем користувачів організації, а також наступного контролю за цим процесом.

Залежно від рівня зрілості організації з питань інформаційних технологій та захисту інформації, а також зважаючи на різницю специфіки роду діяльності кожної організації, у зв'язку з чим до них можна застосовувати

різні нормативно–правові вимоги у сфері захисту інформації, окремі напрямки можуть мати різні пріоритети, проте з урахуванням необхідності побудови комплексної системи для захисту інформації дані напрямки будуть притаманні будь-якій організації. Слід звернути увагу, що реалізація системи управління інформаційною безпекою не повинна переслідувати за собою мету забезпечення інформаційної безпеки та поєднувати або дублювати засоби захисту інформації, а має бути спрямована лише на збільшення ефективності засобів захисту, підтримувати процеси розвитку інформаційно-телекомунікаційної структури організації та надавати актуальну інформаційно-довідкову підтримку з питань забезпечення інформаційної безпеки, з метою своєчасного прийняття коригувальних та попереджуючих впливів та рішень, ґрунтуючись на:

− регламентації процесів захисту інформації;

− обліку та класифікації активів, що захищаються;

− обліку та класифікації ресурсів СЗІ;

− постійному аналізі ризиків інформаційної безпеки та актуалізації моделі загроз інформації;

− моніторинг подій інформаційної безпеки;

− рівні компетенції та професійних можливостей співробітників організації та обслуговуючого персоналу;

− ступеня навантаження\зайнятості та професійної історії фахівців із захисту інформації;

− аналізі накопичених даних з питань інформаційної безпеки.

Таким чином, одними з невід'ємних складових будь-якої системи управління інформаційною безпекою повинні бути регламентація та реалізація механізмів щодо:

− централізованого сигналізування та повідомлення співробітників організації та фахівців із захисту інформації про події всередині системи управління зокрема та СЗІ в цілому;

− аналізу подій всередині системи управління та СЗІ, що дозволить суттєво спростити управління інформаційною безпекою та знизити навантаження на аналітиків з інформаційної безпеки.

1.3 Формування концептуальних принципів управління інформаційною безпекою

Побудова моделі управління інформаційною безпекою має дотримуватися загальноприйнятих концептуальних принципів, закладених при побудові будь-якої СЗІ. Відповідно до чинного законодавства, нормативно-методичних вимог, а також основних тенденцій у сфері забезпечення захисту інформації, метод управління інформаційною безпекою повинен мати такі концептуальні принципи:

− законність;

− системність;

− процесність;

− комплексність;

− безперервність;

− наступність та безперервність удосконалення;

− розумну достатність;

− персональну відповідальність;

− мінімізацію повноважень;

− наукову обґрунтованість та технічну реалізованість;

− обов'язковість контролю.

Під принципом законності передбачається створення моделі управління інформаційною безпекою, її реалізація та експлуатація відповідно до чинного законодавства в галузі інформаційних технологій та інформаційної безпеки, інших нормативних актів, затверджених органами державної влади та управління в межах їх повноважень, а також локальних організаційно-розпорядчих документів, прийнятих всередині організації. У процесі

здійснення даного концептуального принципу користувачі та обслуговуючий персонал організації повинні мати уявлення про відповідальність за правопорушення у сфері інформаційної безпеки, а також бути попередженими, що своїми діями вони можуть не тільки нести матеріальну та адміністративну відповідальність, а й кримінальну.

Під принципом системності передбачається такий підхід до створення моделі управління інформаційною безпекою, який враховуватиме всі взаємопов'язані, взаємодіючі та змінювані в часі елементи, умови та фактори, суттєво значущі для розуміння та вирішення проблем управління всіма напрямками інформаційну безпеку в організації. У процесі здійснення цього концептуального принципу особливу увагу слід звернути на взаємодію структур та фахівців із захисту інформації, а також концентрацію та аналіз наявних у їх розпорядженні даних, з метою найбільш раціонального використання елементів системи, а також моніторингу та обліку факторів та умов, що впливають на інформацію.

Під принципом процесності передбачається відокремлене вивчення та структуроване розбиття всіх заходів щодо забезпечення інформаційної безпеки, реалізованих та/або які реалізуються в організації. У процесі здійснення даного концептуального принципу необхідно приділити особливу увагу деталізації опису кожного із складових процесів інформаційної безпеки з метою формування найефективніших механізмів керування ними.

Під принципом комплексності передбачається використання методів та засобів управління та контролю інформаційної безпеки, що означає узгоджене застосування різнорідних засобів при побудові цілісної системи управління інформаційною безпекою, що реалізує весь необхідний функціонал, по кожному з процесів забезпечення ІБ. У процесі здійснення цього концептуального принципу необхідно звернути увагу на те, що реалізація даного методу управління не повинна переслідувати в собі цілі заміщення або суміщення функцій засобів захисту інформації, а повинна лише керувати ними, що може бути досягнуто за допомогою інтеграції засобів захисту

інформації та механізмів налаштування та управління ними у систему управління інформаційною безпекою.

Під принципом безперервності моделі управління інформаційною безпекою передбачається, що при реалізації цієї моделі необхідно забезпечувати безперервний цілеспрямований процес, що передбачає здійснення контролю стану та управління всіма компонентами СЗІ та вжиття відповідних заходів у разі порушення працездатності на всіх етапах життєвого циклу СЗІ, починаючи з ранніх стадій проектування та модернізації, а також у процесі її експлуатації. При реалізації цього концептуального принципу слід звернути увагу на необхідність збирання та накопичення оброблюваних даних по СЗІ загалом та її окремим компонентам з метою підтримки працездатності та своєчасного внесення змін. Більшості програмних та технічних засобів контролю та управління, включаючи реалізації даної моделі, для ефективного виконання своїх функцій потрібна постійна організаційна (адміністративна) підтримка (своєчасна зміна та забезпечення правильного зберігання та застосування імен, паролів, ключів шифрування, перевизначення повноважень тощо). Перерви у роботі даних засобів мають зводитись до мінімального часу відновлення їх працездатності, що має бути закріплено на адміністративному рівні організації.

Під принципом наступності та безперервності вдосконалення передбачається постійне вдосконалення заходів та засобів контролю та управління на основі наступності організаційних та технічних рішень, кадрового складу, аналізу функціонування системи УІБ та СЗІ з урахуванням змін методів та програмно-технічних засобів, нормативних вимог, у тому числі по захисту накопиченого вітчизняного та зарубіжного досвіду в цій галузі. У процесі реалізації даного концептуального принципу необхідно приділити особливу увагу формуванню універсальних алгоритмів взаємодії даних при побудові системи УІБ.

Під принципом розумної достатності передбачається економічна доцільність та сумісність можливої шкоди та витрат. Він передбачає

відповідність рівня витрат на використовувані заходи та засоби управління та контролю механізмів захисту інформації, що забезпечують інформаційну безпеку, цінності активів, що захищаються та величині можливої шкоди від їх розголошення, втрати, витоку, знищення та спотворення. При реалізації цього концептуального принципу слід враховувати, що вживані заходи та засоби реалізації даного методу не повинні помітно погіршувати основні характеристики СЗІ.

Під принципом персональної відповідальності передбачається покладання персональної відповідальності за управління та контроль засобами захисту інформації, що входять до складу СЗІ, на кожного співробітника в межах його повноважень. Відповідно до цього принципу розподіл прав та обов'язків співробітників будується таким чином, щоб у разі будь-якого порушення коло винуватців було чітко відоме або зведене до мінімуму. У процесі реалізації цього концептуального принципу необхідно враховувати, що процеси розмежування прав доступу до інформації та засобів захисту інформації є однією з основ методу управління інформаційною безпекою.

Під принципом мінімізації повноважень передбачається надання користувачам та обслуговуючому персоналу при реалізації методу мінімальних прав доступу відповідно до виробничої необхідності. При реалізації цього концептуального принципу слід надавати доступ до механізмів керування інформаційною безпекою та інформації, що обробляється всередині, тільки в тому випадку, якщо це необхідно співробітнику для виконання його посадових обов'язків.

Під принципом наукової обґрунтованості та технічної реалізованості передбачається, що інформаційні технології, технічні та програмні засоби, засоби та заходи управління та контролю методу управління інформаційною безпекою повинні бути реалізовані на сучасному рівні розвитку науки і техніки, науково обґрунтовані з точки зору досягнення заданого рівня безпеки інформації та повинні відповідати встановленим нормам та вимогам щодо безпеки інформації, що застосовуються в організації.

Під принципом обов'язковості контролю передбачається обов'язковість та своєчасність виявлення та припинення спроб порушення встановлених регламентів роботи. Контроль за діяльністю користувачів та обслуговуючого персоналу системи УІБ та СЗІ щодо будь-якого об'єкта захисту повинен здійснюватися на основі застосування засобів оперативного контролю та реєстрації та має охоплювати як несанкціоновані, так і санкціоновані дії користувачів та обслуговуючого персоналу. При реалізації даного концептуального принципу слід звернути особливу увагу, що повні механізми процесів аудиту до цього принципу не входять, а зачіпають лише його складові.

1.4 Схема взаємозв’язку ризиків з використанням систем підтримки прийняття рішень

Процес управління ризиками та загрозами інформаційній безпеці є одним із ключових аспектів при забезпеченні інформаційної безпеки в організаціях різного роду діяльності. На даний момент існує величезна кількість методик, що дозволяють визначати, виявляти та оцінювати ризики інформаційної безпеки. В основі кожної методики незмінно лежить поняття «загроз інформаційній безпеці». Найчастіше під загрозами інформаційній безпеці розуміють сукупність умов та факторів, які можуть створювати (або створюють) небезпеку порушення однієї з властивостей безпеки інформації. Таким чином поняття «ризик інформаційної безпеки» та «загроза інформаційній безпеці» є взаємодоповнювальними поняттями та безперервно пов'язані при формуванні вимог до забезпечення інформаційної безпеки. Такий підхід до управління інформаційної безпеки прийнято називати ризиковим. Слід розуміти, що різні методології часто ґрунтуються на специфіці конкретних напрямів діяльності організації, що дає повніше уявлення про типи активів, які захищаються, ступеня критичності властивостей безпеки інформації для конкретного типу активу, і

найголовнішим – вартістю втрати активу або порушення властивостей безпеки інформації. Таким чином, ризик інформаційної безпеки стає інструментом для визначення наслідків реалізації загрози та має яскраво виражений комерційний характер. Такий підхід є застосовним для організацій, що займаються комерційною діяльністю, основна мета яких - отримання прибутку. Однак у сучасних тенденціях розвитку інформаційних технологій інформація, що відноситься до комерційної таємниці, є лише одним з видів конфіденційної інформації. У зв'язку з цими обставинами ризик-орієнтований підхід отримує дуже суттєві протиріччя. Справа в тому, що у разі неможливості визначення вартості активу оцінити втрати даного активу в кількісному еквіваленті просто неможливі. Прикладом такої інформації можуть бути:

− відомості, що становлять державну таємницю;

− персональні дані;

− відомості, пов'язані з професійною діяльністю;

− відомості, що становлять таємницю слідства та судочинства.

Дані види інформації, для кожної організації, а також носії, що їх містять, будуть захищатися інформаційними активами, при цьому захист такої інформації диктуватиметься не лише побажаннями самої організації, а й відповідними законодавчими вимогами. Таким чином, питання управління ризиками інформаційної безпеки необхідно безпосередньо розглядати у прив'язці до управління загрозами інформаційної безпеки. Вважають, що загрози інформаційній безпеці є завжди, проте в залежності від низки умов процес реалізації та ступінь небезпеки цієї загрози можуть істотно змінюватись.

З врахуванням параметрів, необхідних для оцінки ризиків та загроз інформаційній безпеці для активу, що захищається, можна отримати схему повного взаємозв’язку параметрів загроз інформаційній безпеці, яка наведена на рисунку 1.8.

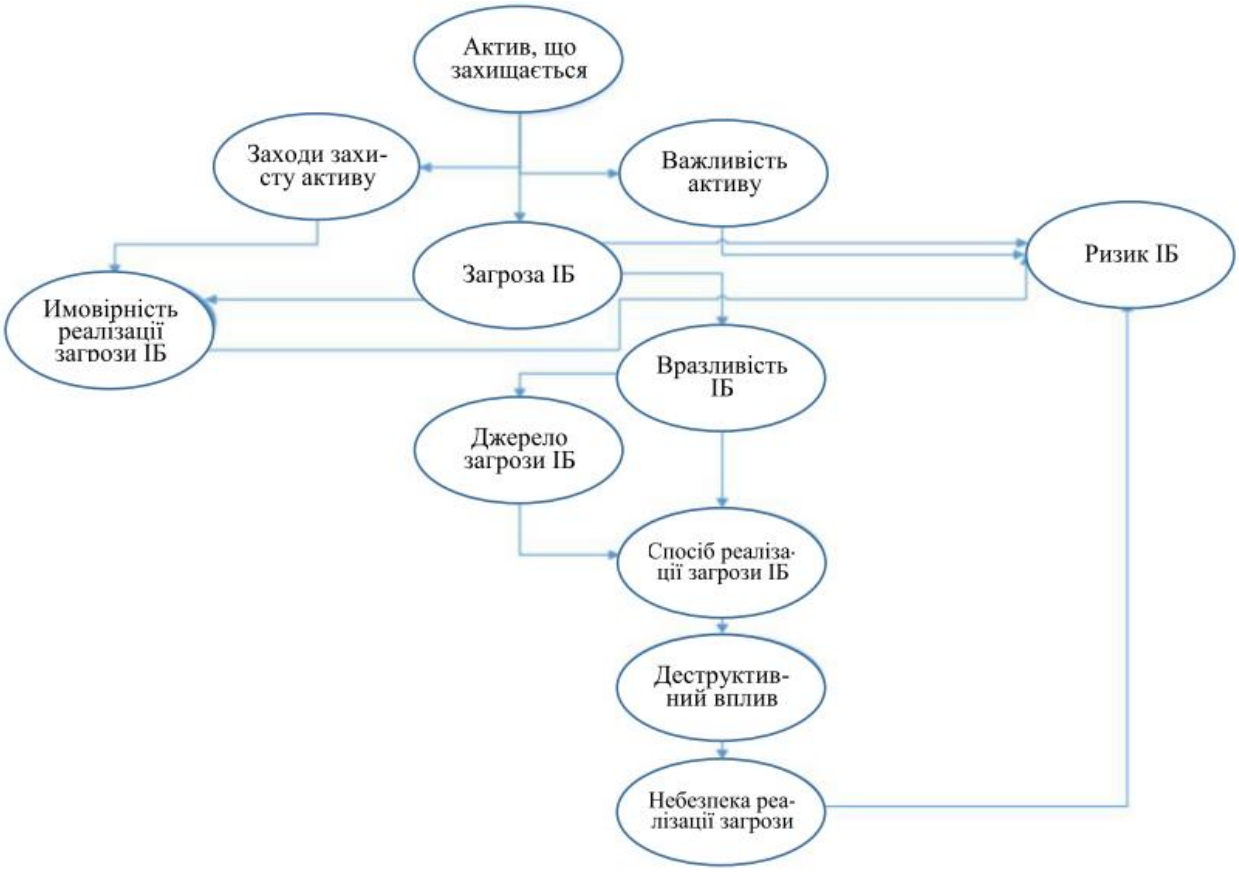

Рисунок 1.8 – Схема повного взаємозв’язку параметрів загроз інформаційній безпеці визначеного активу

Основне призначення процесу управління ризиками та загрозами інформаційній безпеці є визначення, аналіз та контроль заходів, що враховують ймовірності реалізації загроз інформаційній безпеці, а залежно від типу та складу захищеного інформаційного активу давати можливість математично прорахувати можливу (потенційну) величину втрат, пов'язану з реалізацією небезпеки. Визначення таких наслідків та втрат характеризується двома основними складовими: вартість активу та небезпека реалізації загрози. Виходячи з описаних вище фактів, поняття «вартість активу» надалі доцільно замінити на загальне поняття – «важливість активу», яка буде характеризуватись трьома вербальними значеннями: «Висока важливість активу», «Середня важливість активу», «Низька важливість активу». Виходячи з детального аналізу існуючих методик оцінки ризиків та

визначення актуальності загроз інформаційній безпеці, кожну загрозу можна охарактеризувати такими основними параметрами:

1) об'єкт впливу загрози (актив або тип активу);

2) джерело виникнення небезпеки;

3) вразливість, що використовується у процесі реалізації загрози;

4) спосіб реалізації загрози через використання властивої їй вразливості;

5) деструктивний вплив, який виникає у процесі реалізації загрози;

6) можливість реалізації небезпеки;

7) небезпека реалізації небезпеки.

2 ОЦІНКА МЕТОДУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

2.1 Визначення апріорної можливості реалізації загроз інформаційній безпеці на основі систем підтримки прийняття рішень

В основу апріорного визначення ймовірності реалізації загроз інформаційній безпеці буде закладено метод експертної оцінки та принцип усереднення коефіцієнтів для мінімізації недоліків, супутніх з методом експертної оцінки. На відміну від більшості методик, запропонований метод управління інформаційною безпекою розглядає загрозу як об'єкт, що утворюється цілим рядом параметрів. Тобто як абстрактний дискретний об'єкт, що складається з цілого ряду взаємопов'язаних параметрів. Зміна одного з них веде до неминучої зміни всього ланцюжка зв'язків.

Ґрунтуючись на даній логіці було визначено першочерговий взаємозв'язок параметра, який найбільш повно описує вплив конкретного джерела загрози на можливість реалізації самої небезпеки. Цей параметр пов'язаний безпосередньо як із самим джерелом загрози, так і з аналізованою загрозою і безпосередньо впливає на можливість виникнення загроз.

З урахуванням структури динамічних експертних систем апріорне визначення можливості реалізації загроз полягатиме в наступному:

1) конкретизації досліджуваної проблемної галузі (імовірності виникнення
загроз інформаційній безпеці) для виключення комбінаторного вибуху;

2) підборі експертів;

3) інженерії знань експертів;

4) формування робочої бази даних;

5) формалізації ухвалення рішень при отриманні результатів.

З врахуванням застосування методу експертної оцінки та принципу усереднення коефіцієнтів додаються такі пункти:

6) визначення можливості здійснення способу реалізації методом експертної оцінки;

7) усереднення коефіцієнтів, одержаних від експертів.

Для первинного наповнення бази даних відібраним експертам по інформаційній безпеці пропонується для заповнення матриця, представлена в таблиці 2.1.

Таблиця 2.1 – Матриця визначення взаємозв'язку джерела загроз та способу реалізації загроз інформаційній безпеці.

	Спосіб реалізації	Спосіб реалізації 1	Спосіб реалізації 2	Спосіб реалізації 3	…	Спосіб реалізації *M*
Джерело загрози						
Джерело загрози 1						
Джерело загрози 2						
…						
Джерело загрози *N*						

Для застосування апріорної оцінки можливості реалізації загрози необхідно попередньо провести аналіз усіх загроз інформаційній безпеці, що розглядаються в рамках використовуваної методології прорахунку актуальності загроз визначення всіх супутніх їм способів реалізації. У разі відсутності цієї класифікації, то у межах самої методології.

Для визначення параметрів взаємодії джерела загроз та способу реалізації експертам необхідно провести заповнення перетину стовпців та рядків матриці виходячи з наступних міркувань:

− неможлива (Н\М) – значення присвоюється перетину в тому випадку, якщо експерт вважає, що цей спосіб реалізації не може бути застосований даним джерелом небезпеки;

− низька (Н) – значення присвоюється перетину у тому випадку, якщо експерт вважає, що даний спосіб реалізації має низьку застосовність даним джерелом небезпеки;

− середня (С) – значення присвоюється перетину у тому випадку, якщо експерт вважає, що даний спосіб реалізації має середню застосовність даним джерелом небезпеки;

− висока (В) – значення присвоюється перетину у тому випадку, якщо експерт вважає, що даний спосіб реалізації має високу застосовність даним джерелом небезпеки.

Для отримання первинних коефіцієнтів ймовірності реалізації загрози кожному з параметрів надається числовий коефіцієнт:

− Н\М = 0;

− Н = 0,2;

− С = 0,5;

− В = 1.

Таким чином, ми маємо матрицю виду:

$$\begin{bmatrix} 11 & \dots & 1M \\ \dots & \dots & \dots \\ N1 & \dots & NM \end{bmatrix}_{k_i},$$

де i – кількість експертів;

N - кількість джерел загроз;

M – кількість способів реалізації.

При цьому можливість реалізації V_i загрози інформаційній безпеці i описується сукупною множиною способів реалізації цієї загрози $E_i \in M$.

Підсумкова матриця k_r можливості реалізації загроз після заповнення всіма запрошеними експертами матиме вигляд:

$$k_r = \sum_{i=1}^{n} \begin{bmatrix} 11 & \dots & 1M \\ \dots & \dots & \dots \\ N1 & \dots & NM \end{bmatrix}_{k_i}.$$

Показник можливості реалізації загрози (V_i) порушником N розраховується як середнє арифметичне повної суми показників рядка N матриці k_r для всіх E_i.

Залежно від використовуваної методології розрахунку актуальності загроз та ризиків інформаційної безпеки дані коефіцієнти підлягають додатковому трактуванню, однак виходячи із загальної логіки методу розкид можливих значень підсумкових показників слід трактувати так:

– $V_i \in [0\ ,\ 0{,}2)$ – неможливо реалізувати;

– $V_i \in [0{,}2\ ,\ 0{,}5)$ – мала ймовірність реалізації;

– $V_i \in [0{,}5\ ,\ 0{,}8)$ – середня ймовірність реалізації;

– $V_i \in [0{,}8\ ,\ 1]$ – висока ймовірність реалізації.

2.2 Визначення ступеня небезпеки реалізації загроз інформаційній безпеці з урахуванням систем підтримки прийняття рішень

В основу визначення ступеня небезпеки реалізації загроз інформаційній безпеці закладено принципи динамічних експертних систем підтримки прийняття рішення. Найчастіше щодо ступеня небезпеки реалізації загрози інформаційній безпеці беруть до уваги величину та ступінь впливу можливих деструктивних наслідків під час реалізації загрози. В основному дані ступеня небезпеки формалізують у вигляді передбачуваної суми у грошовому еквіваленті, однак такий підхід не застосовний для випадків, коли наслідки реалізації загроз інформаційній безпеці неоціненні у грошовому еквіваленті, або коли така оцінка неприйнятна, виходячи з важливості самих активів організації. У таких випадках побудова моделі загроз має на меті не визначити найбільш пріоритетні напрямки захисту інформації для мінімізації фінансових втрат і прибутку, а для визначення найбільш уразливих місць у системі захисту інформації, а також формуванні необхідного переліку заходів щодо їх усунення.

Виходячи з наведених вище аспектів, в основу оцінки ступеня небезпеки загроз інформаційній безпеці буде закладено метод експертної оцінки та принцип усереднення коефіцієнтів для мінімізацій недоліків, супутніх методу експертної оцінки. Слід враховувати, що з урахуванням запропонованого підходу розгляд загрози як абстрактного дискретного об'єкта, що складається з цілого ряду взаємопов'язаних параметрів, і зміна одного з них веде до неминучої зміни всього ланцюжка зв'язків. Ці параметри впливатимуть на ступінь небезпеки самої загрози, при цьому ступінь небезпеки загрози варіюватиметься залежно від важливості активу, в рамках якого розглядатиметься сама загроза інформаційній безпеці.

Ґрунтуючись на даній логіці, був визначений першочерговий взаємозв'язок параметра, який найбільш повно описує вплив конкретного джерела загрози на ступінь небезпеки самої загрози. Цей параметр пов'язаний безпосередньо як із самим джерелом загрози, так і аналізованою загрозою, і безпосередньо впливає на ступінь небезпеки загрози – деструктивний вплив.

З урахуванням структури динамічних експертних систем підтримки прийняття рішень оцінка ступеня небезпеки для загрози полягатиме в наступному:

1) конкретизації досліджуваної проблемної галузі (ступінь небезпеки загроз інформаційній безпеці), щоб уникнути комбінаторного вибуху;

2) підборі експертів;

3) інженерії знань експертів;

4) формування робочої бази даних;

5) формалізації ухвалення рішень при отриманні результатів.

З урахуванням застосування методу експертної оцінки та принципу усереднення коефіцієнтів додаються такі пункти:

6) визначення ступеня небезпеки деструктивного впливу реалізації загрози методом експертної оцінки;

7) усереднення коефіцієнтів, одержаних від експертів;

8) визначення важливості активів, що захищаються.

Для первинного наповнення бази даних, відібраним експертам з інформаційної безпеки для заповнення надається матриця, представлена в таблиці 2.2.

Таблиця 2.2 – Матриця визначення взаємозв'язку джерела загроз та деструктивного впливу загроз інформаційної безпеки.

	Деструктивний вплив	Деструктивний вплив 1	Деструктивний вплив 2	Деструктивний вплив 3	…	Деструктивний вплив *M*
Джерело загрози						
Джерело загрози 1						
Джерело загрози 2						
…						
Джерело загрози *N*						

Для оцінки ступеня небезпеки необхідно попередньо провести аналіз усіх загроз інформаційній безпеці, що розглядаються в рамках використовуваної методології прорахунку актуальності загроз для визначення всіх супутніх їм деструктивних впливів, ґрунтуючись на способах реалізації загроз у разі відсутності цієї класифікації у межах самої методології.

Для визначення параметрів взаємодії джерела загроз та деструктивного впливу експертам необхідно провести заповнення перетину стовпців та рядків матриці, виходячи з таких міркувань:

− низька (Н) – значення присвоюється перетину у тому випадку, якщо експерт вважає, що цей деструктивний вплив має низький ступінь впливу на активи організації, що захищаються від даного джерела загрози;

− середня (С) – значення присвоюється перетину у тому випадку, якщо експерт вважає, що цей деструктивний вплив має середній ступінь впливу на активи організації, що захищаються від даного джерела загрози;

− висока (В) – значення присвоюється перетину у тому випадку, якщо експерт вважає, що цей деструктивний вплив має високий ступінь впливу на активи організації, що захищаються від даного джерела загрози.

Для отримання первинних показників ступеня небезпеки загрози кожному з параметрів надається числовий коефіцієнт:

− Н = 0;

− С = 0,5;

− В = 1.

Таким чином, отримуємо матрицю:

$$\begin{bmatrix} 11 & \dots & 1M \\ \dots & \dots & \dots \\ N1 & \dots & NM \end{bmatrix}_{k_i},$$

де i – кількість експертів;

N кількість джерел загроз;

M – кількість деструктивних дій.

При цьому ступінь небезпеки D_i загрози інформаційної безпеки i описується сукупною множиною можливих деструктивних впливів даної загрози $Q_i \in M$.

Підсумкова матриця k_r можливості реалізації загроз після заповнення всіма запрошеними експертами матиме вигляд:

$$k_r = \sum_{i=1}^{n} \begin{bmatrix} 11 & \dots & 1M \\ \dots & \dots & \dots \\ N1 & \dots & NM \end{bmatrix}_{k_i}$$

Показник небезпеки загрози (D_i) порушником N розраховується як середнє арифметичне повної суми показників рядка N матриці k_r для всіх Q_i.

Залежно від використовуваної методології розрахунку актуальності загроз та ризиків інформаційної безпеки дані коефіцієнти підлягають додатковому трактуванню, проте виходячи із загальної логіки методу розкид можливих значень підсумкових показників слід трактувати таким чином:

– $D_i \in [0; 0{,}4)$ – низький ступінь небезпеки;

– $D_i \in [0{,}4; 0{,}8)$ – середній ступінь небезпеки;

– $D_i \in [0{,}8; 1]$ – високий ступінь небезпеки.

2.3 Визначення постапріорної оцінки можливості реалізації загроз інформаційній безпеці

При визначенні постапріорної оцінки можливості реалізації загроз інформаційній безпеці закладено структуру динамічних експертних систем підтримки прийняття рішень та метод експертної оцінки. Основою, для прийняття рішень при оцінці можливості реалізації загроз інформаційній безпеці є сукупність інформації у статичній та динамічній базі даних. Динамічна база даних містить перелік необхідної інформації щодо інформаційної системи, включаючи відомості про типи та склад активів, засобів і механізмів захисту інформації, що захищаються, спільно з унікальним переліком атрибутів та метаінформації щодо кожного конкретного активу та засобу захисту інформації.

Статична база даних містить перелік службової інформації та складових правил взаємодії, як усередині своєї структури, так і зовні (динамічної БД). До її складу входять:

1) інформація щодо кожної з існуючих (в рамках моделі) загроз безпеки інформації, включаючи:

- об'єкт впливу;

- методи реалізації вразливості, властивої для даної загрози;

2) умова (сукупність умов) наявності даної загрози для активу, що захищається (об'єкта впливу).

Для побудови первинних правил використовується фіксована прив'язка один до одного наступних параметрів:

− «Тип активу» – «Загроза»;

− «Загроза» – «Умова виникнення загрози»;

− «Загроза» – «Заходи перекриття загрози»;

− «Заходи перекриття загрози» – «Засоби перекриття».

Оскільки умова виникнення загрози безпосередньо залежить від поєднання типу активу та властивих йому загроз, значення параметра «Умова виникнення загрози» змінюватиметься у значеннях (α):

1 – умова виникнення небезпеки існує;

0 – умова виникнення небезпеки немає.

Кількість та склад умов визначається для кожної загрози окремо на етапі роботи щодо наповнення експертної системи даними з урахуванням сукупної думки опитуваних експертів.

Грунтуючись на знаннях про умови виникнення загроз та типи активів, схильних до загрози, на етапі наповнення експертної системи даними відбувається формалізація заходів перекриття загрози, для кожної з яких запроваджуються відповідні засоби перекриття. У разі необхідності перекриття загрози сукупністю заходів для кожним із заходів вводиться відсоткова градація ступеня перекриття загрози (X).

Для кожного засобу перекриття конкретного заходу визначається максимальне значення, що встановлює повноту перекриття міри цим засобом. Грунтуючись на результатах опитування експертів у галузі інформаційної безпеки, встановлюються наступні значення повноти перекриття міри засобом перекриття (R):

0 – засіб перекриття небезпеки відсутня;

3 – засіб перекриття не має підтвердження реалізації необхідних функцій, коректності їх настроювання;

5 – засіб перекриття має підтвердження необхідних функцій, але відсутні відомості про коректність;

7 – засіб перекриття має підтвердження необхідних функцій і є підтвердження коректності налаштування.

Таким чином, розрахунок можливості реалізації (*V*) загрози визначатиметься за наступною формулою:

$$\begin{cases} V = \alpha \cdot \dfrac{\left(\left(R_{1\max} - R_{1par}\right)\cdot \dfrac{X_1}{100}\right) + \left(\left(R_{2\max} - R_{2par}\right)\cdot \dfrac{X_2}{100}\right) + \ldots + \left(\left(R_{n\max} - R_{npar}\right)\cdot \dfrac{X_n}{100}\right)}{R_{\max}}; \\ X_1 + X_2 + \ldots + X_n = 100; \alpha \in [0,1], \end{cases}$$

де R_{npar} – поточне значення повноти перекриття міри засобу *R* для міри *n*;

X_n – коефіцієнт ступеня перекриття загрози *X* для міри *n*;

α – наявність умови виникнення загрози.

Основні переваги використання запропонованого підходу полягають у наступному:

− об'єктивності оцінки можливості реалізації загрози з урахуванням сукупної думки багатьох експертів;

− формалізації використовуваних параметрів оцінки ймовірності реалізації загроз інформаційній безпеці;

− автоматизації виконання процесу;

− обліку вимог та існуючих засобів та заходів захисту інформації, які діють в організації;

− суттєве скорочення періоду проведення оцінки:

− спрощення актуалізації та проведення переоцінки;

− скорочення навантаження на аналітиків у галузі інформаційної безпеки;

− встановлення логічного взаємозв'язку параметрів, що використовуються при оцінці ймовірність реалізації загроз інформаційній безпеці;

− статистична достовірність отриманих результатів;

− відсутності людського фактора;

− можливості подальшого використання та актуалізації зібраної інформації, яка досягається за допомогою використання засобів автоматизації.

2.4 Структура методу управління інформаційною безпекою на основі систем підтримки прийняття рішень

В основу розробленого методу управління інформаційною безпекою закладено динамічні експертні системи підтримки ухвалення рішень. Виходячи з уточненого визначення поняття «Управління інформаційною безпекою», а також ґрунтуючись на процесі подання забезпечення інформаційною безпекою, управління всією інформаційною безпекою в організації має бути засноване на комплексному підході до управління кожним із процесів забезпечення інформаційної безпеки в організації.

Повний перелік розглянутих та описаних вище процесів підлягає відповідному розбиттю на основні функціональні групи, виходячи з їх ролі в рамках процесів забезпечення інформаційної безпеки, а саме:

1) група формування вимог та вихідної інформації до системи захисту інформації та об'єктів захисту;

2) група систематизації інформації щодо системи захисту інформації та об'єктів захисту;

3) група актуалізації інформації щодо системи захисту інформації та об'єктів захисту;

4) група аналітичної обробки, контролю та аналізу ефективності реалізації механізмів захисту, які діють в рамках системи захисту інформації;

5) група прийняття рішень щодо управління інформаційною безпекою та застосування коригувальних та попереджувальних впливів у поєднанні з плануванням та вдосконаленням механізмів захисту, що діють у рамках системи захисту інформації

Кожна з даних функціональних груп може бути подана у вигляді однієї з складових частин у структурі експертної системи, що відповідає за конкретні дії в рамках даного методу управління інформаційною безпекою. Якщо провести аналогію між процесами управління інформаційною безпекою та структурою експертної системи, то відсунувши на другий план питання автоматизації самих процесів, отримується повноправна експертна система, що відповідає за реалізацію конкретного процесу у межах організації.

Група формування вимог та вихідної інформації до системи захисту інформації та об'єктів захисту призначена для систематизації вимог зовнішньої та внутрішньої нормативно-правової документації у сфері забезпечення інформаційної безпеки в організації та повинна забезпечувати формування вихідного набору інформації щодо всіх об'єктів захисту та механізмів системи захисту інформації у прив'язці до нормативних вимог, що виникають. До цієї групи належатиме:

− процес управління документацією та інформаційною довідковою системою в організації;

− процес управління активами організації;

− процес управління ресурсами системи захисту інформації, реалізованої в організації;

− процес управління процесами забезпечення інформаційної безпеки при здійсненні роботи зі співробітниками організації, підвищення їх кваліфікації та загальної компетенції з питань інформаційної безпеки;

− процес управління процесами забезпечення інформаційної безпеки при здійсненні інформаційного обміну та взаємодії з третіми сторонами;

− процес управління процесами забезпечення розмежування прав доступу до інформації та інформаційних систем користувачів організації, а також подальшого контролю за цим процесом.

У межах реалізації функціонального призначення цієї групи процесів з урахуванням структури динамічних експертних систем підтримки прийняття рішень для детального формування вимог та вихідної інформації для суміжних

процесів має бути залучено групу експертів у галузі забезпечення інформаційної безпеки. Дана функціональна група покликана забезпечити формалізацію та визначити класифікатори по формованим вихідним даним для подальшої їх систематизації у межах системи управління інформаційною безпекою в установі. З точки зору динамічних експертних систем дана функціональна група буде «Базою знань».

Група систематизації інформації щодо системи захисту інформації та об'єктів захисту призначена для структуризації всіх зібраних вихідних даних та вимог щодо інформаційної безпеки, сформованих у рамках роботи першої функціональної групи. При роботі цієї функціональної групи відбувається формальний розподіл зібраної вихідної інформації щодо складових частин системи захисту інформації. У рамках цього методу управління інформаційною безпекою та з метою спрощення розуміння принципів систематизації інформації дана функціональна група буде збірним компонентом елементів кожного з процесів, задіяних у першій функціональній групі з єдиним полем систематизації. Результатом роботи даної функціональної групи буде розподіл потоків вихідних даних та укрупнення їх у рамках найпростішої складової частини в організації – інформаційної та/або автоматизованої системи До цієї функціональної групи належать вихідні дані щодо наступних процесів:

− процес управління документацією та інформаційною довідковою системою в установі;

− процес управління активами організації;

− процес управління ресурсами системи захисту інформації, реалізованої в організації;

− процес управління процесами забезпечення інформаційної безпеки при здійсненні роботи зі співробітниками організації, підвищення їх кваліфікації та загальної компетенції з питань інформаційної безпеки;

− процес управління процесами забезпечення інформаційної безпеки при здійсненні інформаційного обміну та взаємодії з третіми сторонами;

− процес управління процесами забезпечення розмежування прав доступу до інформації та інформаційних систем користувачів організації, а також подальшого контролю за цим процесом.

Основним результатом роботи даної функціональної групи буде систематизований перелік вихідних даних щодо системи захисту інформації та об'єктів захисту з розподіленими класифікаторами за типами даних та правил їх взаємодії усередині організації. З точки зору динамічних експертних систем дана функціональна група буде сукупністю «Експертної групи» та «Групи інженерів знань».

Група актуалізації інформації щодо системи захисту інформації та об'єктів захисту призначена для внесення своєчасних змін, доповнень та розширення загальної інфраструктурної інформації щодо об'єктів та механізмів захисту, а також для підтримки загального рівня заданих параметрів за вимогами нормативно-правової документації, в поєднанні з моніторингом протікаючих процесів у рамках основних складових організації у прив'язці як до внутрішнього, так і зовнішнього персоналу інформаційної та\або автоматизованої системи, а також представникам третіх сторін. Основна мета даної функціональної групи полягає у своєчасному оновленні інформації в процесі роботи організації, а також моніторинг, виявлення та реагування на події інформаційної безпеки, що також є одним із способів актуалізації інформації та відображення стану системи захисту інформації та об'єктів захисту. До даної функціональної групи належать:

− процес управління процесами забезпечення інформаційної безпеки на різних етапах розвитку інформаційних систем, а також підтримка та продовження життєвих циклів інформаційних систем організації;

− процес управління процесами забезпечення безперервності роботи інформаційних систем та інформаційно-телекомунікаційних сервісів;

− процес управління процесами забезпечення моніторингу, виявлення та реагування на події інформаційної безпеки;

− процес управління процесами забезпечення розмежування прав доступу до інформації та інформаційних систем користувачів організації, а також подальшого контролю за цим процесом.

Основним результатом роботи даної функціональної групи буде актуалізація всіх даних про систему захисту інформації та об'єкти захисту, а також визначення нових або недостатніх параметрів для визначення тих чи інших залежностей та правил поведінки системи захисту інформації, необхідних для найбільш коректної та ефективної роботи наступних функціональних груп. З точки зору динамічних експертних систем дана функціональна група буде «Редактором бази знань».

Група аналітичної обробки, контролю та аналізу ефективності реалізації механізмів захисту, що діють у рамках системи захисту інформації, призначена для проведення структурованого аналізу даних, що збираються і актуалізуються в ході роботи перших трьох функціональних груп, контролю за дотриманням вимог нормативно-правової документації та комплексного аналізу ефективності засобів захисту інформації. Основна мета даної функціональної групи полягає у побудові складних аналітичних розрахунків, поведінкових прогнозів, побудові моделей поведінки об'єктів захисту та потенційних порушників у прив'язці до реального стану справ в організації. Ця функціональна група спирається виключно на досвід, кваліфікацію та відповідальність експертної групи, що залучається до процесу управління інформаційною безпекою, і є найбільш важливою та ресурсомісткою групою в рамках даного методу управління інформаційною безпекою. З точки зору динамічних експертних систем та типової структури експертної системи, дана функціональна група буде «Вирішувачем» або механізмом виведення даних на основі їх аналізу для подальшого прийняття рішень. До цієї групи належать:

− процес управління ризиками та загрозами інформаційній безпеці;

− процес управління аудитом системи захисту інформації;

− процес управління аналізом ефективності системи захисту інформації.

Група прийняття рішень з управління інформаційною безпекою та застосування коригувальних та попереджувальних впливів у поєднанні з плануванням та вдосконаленням механізмів захисту, що діють у рамках системи захисту інформації, призначена для тактичного та стратегічного управління інформаційною безпекою на основі одержуваних даних від інших функціональних груп, формування своєчасного пулу дій для застосування коригувальних та попереджувальних впливів на систему захисту інформації, а також планування робіт з удосконалення механізмів захисту інформації, реалізованих у рамках чинної системи захисту в організації. До цієї функціональної групи належить процес управління завданнями та діяльністю співробітників, які здійснюють процеси забезпечення інформаційної безпеки в організації. З точки зору динамічних експертних систем дана функціональна група буде «Підсистемою пояснення», а також підсистемою підтримки-ухвалення рішень з управління інформаційною безпекою в установі.

Загальна структура методу управління інформаційною безпекою, з розбиттям по функціональних групах та їх узагальненням з урахуванням використання динамічних експертних систем представлений на рисунку 2.1. Для спрощення візуального відображення процесів їх повні назви замінені на більш короткі позначення.

Таким чином, першою основною дією в рамках розробленого методу управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень буде поділ процесних складових управління та забезпечення інформаційної безпеки в організації з функціональних груп, які реалізують скінченну множину дій. В результаті виконання першої дії відбувається формування елементів бази знань експертної системи підтримки прийняття рішень.

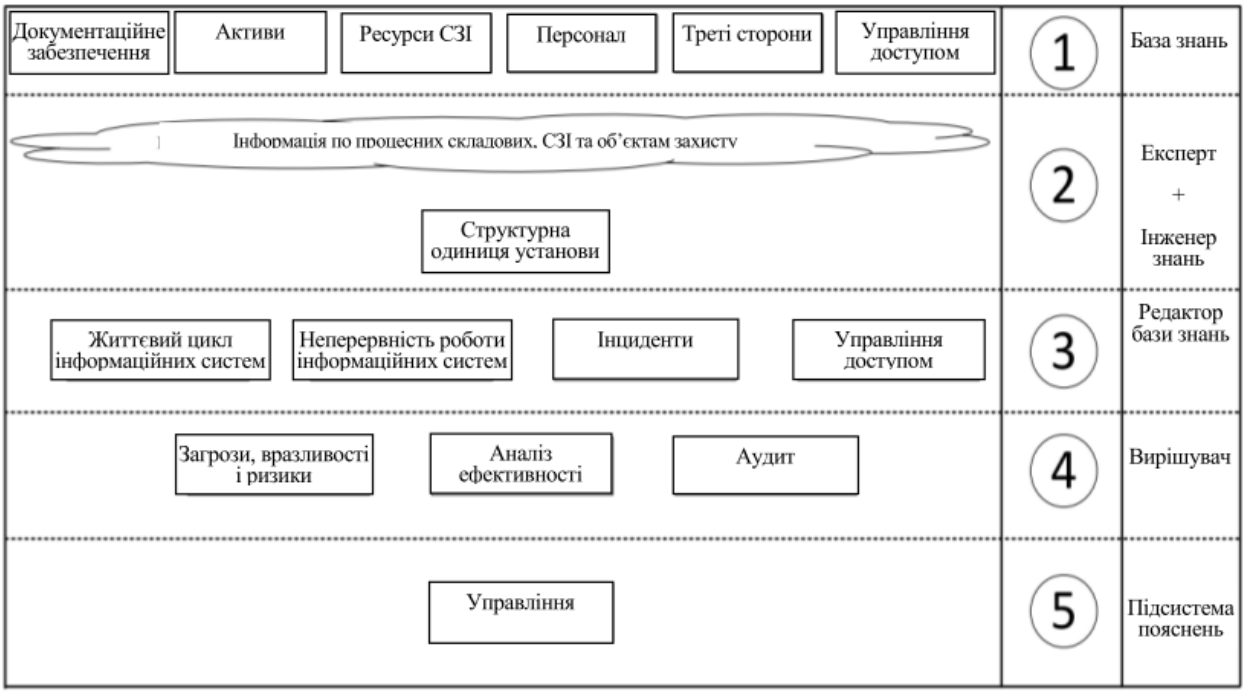

Рисунок 2.1 – Структура методу управління інформаційною безпекою

Другою дією буде формалізація загальних та часткових вимог до процесів управління та забезпечення інформаційної безпеки в організації, виходячи з вимог внутрішніх та зовнішніх нормативно-правових документів щодо інформаційної безпеки. Залежно від типу даних, розміру організації та основної діяльності організації формалізація часткових вимог може мати значну відмінність, проте формалізація загальних вимог збігатиметься. В результаті виконання другої дії відбувається формування логічних правил взаємодії елементів бази знань експертної системи підтримки ухвалення рішень.

Третьою дією буде збір вихідної інформації щодо об'єктів захисту та системі захисту інформації загалом. В рамках цієї дії необхідно визначити початковий перелік інформації з пріоритетних напрямків, а саме:

− інформацію про активи організації, що захищаються;

− інформацію про ресурси системи захисту інформації, включаючи технічні та організаційні заходи, а також інформацію про межі їх застосування у межах організації;

− інформацію про склад та функції обслуговуючого персоналу організації та користувачів автоматизованих та\або інформаційних систем;

− інформацію про склад та характер взаємодії та\або інформаційного обміну із сторонніми організаціями та третіми особами;

− інформацію про правила та привілеї доступу до інформаційних активів, що захищаються, ресурсів системи захисту інформації та автоматизованих і\або інформаційних систем організації.

Внаслідок виконання третьої дії відбудеться наповнення бази знань первинними знаннями експертної системи підтримки ухвалення рішень.

Четвертою дією буде систематизація отриманих вихідних даних по мінімально значимим складовим частинам організації, а також присвоєнням визначених класифікаторів взаємодії і взаємозалежності даних за їх типом. Такими частинами можуть бути автоматизовані та інформаційні системи, відповідальні особи організації, адміністративний персонал тощо. Залежно від складу та характеру певних мінімально значущих складових частин організації залежатимуть поведінкові правила роботи системи захисту інформації. Ці правила можуть бути описані у вигляді політик, регламентів та концепцій з інформаційної безпеки. Внаслідок виконання четвертої дії відбувається визначення метаданих або класифікаторів даних, встановлення взаємозалежності інформації за даними класифікаторами, і навіть формалізація принципів формування нових знань.

П'ятою дією буде визначення складу та ступеня можливого коригування класифікаторів та моделей взаємодії, а також складу інформації за основними мінімально значимими складовими частинами організації, а також наступна формалізація даної дії, закріпленої у керівних та організаційно- розпорядчих документах організації з інформаційної безпеки. В результаті виконання п'ятої дії формуються логічні правила динамічної зміни експертних оцінок за можливими класифікаторами та взаємозалежностями знань, динамічна зміна змісту бази знань експертної системи підтримки прийняття рішень під час виконання процесів ІБ.

Шостою дією буде визначення, обґрунтування та застосування методик визначення актуальності загроз, уразливостей та ризиків інформаційної безпеки в організації, а також методик оцінки ефективності роботи системи захисту інформації та її складових частин, методик проведення аудиту та оцінки ступеня відповідності вимогам зовнішніх та внутрішніх регулюючих органів. В результаті виконання шостої дії відбувається визначення правил оцінки відповідності СЗІ вимогам щодо ІБ та прийняття рішень на основі динамічної зміни інформації від процесів ІБ з часом.

Сьомою дією буде визначення параметрів та вироблення основних управлінських концепцій та регламентів з реагування та своєчасного застосування керуючих, корегувальних та попереджуючих впливів на події як усередині організації, так і всередині СЗІ. В результаті виконання сьомої дії відбувається прийняття рішень та формування оперативного керуючого впливу на СЗІ та процеси ІБ.

Восьмою дією буде формування та обґрунтування планів подальшого розвитку та вдосконалення системи захисту інформації в цілому та механізмів захисту зокрема, а також перегляд застосовності раніше обраних методик з метою підвищення ефективності системи захисту інформації, що діє. В результаті виконання восьмої дії відбувається аналіз динамічних змін інформації від процесів ІБ після прийняття рішень, після чого відбувається формування планів подальшого вдосконалення СЗІ.

Дев'ятою дією буде формування окремої системи\підсистеми управління інформаційною безпекою в організації, яка відповідає за виконання вищеописаних дій як з використанням засобів автоматизації, так і без їх використання, після чого процес має бути повторений у зв'язку з необхідністю забезпечення безперервності процесу забезпечення інформаційної безпеки та захисту інформації.

3 МОДЕЛІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

3.1 Модель даних процесу формування та підтримання актуальності інформаційно-довідкової системи з питань інформаційної безпеки

Управління процесом формування та підтримки актуальності інформаційно-довідкової системи з питань інформаційної безпеки в організації є основною складовою частиною всього процесу управління інформаційноюбезпекою. В рамках цього процесу формуються вимоги до системи захисту інформації, досвіду, кваліфікації та посадових функціональних обов'язків співробітників організації, формується перелік заходів та механізмів захисту інформації, порядок проведення перевірок, правила та принципи прийняття рішень у різних ситуаціях, а також відбувається аналіз та коригування вимог для подальшого використання, спираючись на результати роботи та введення суміжних процесів управління інформаційною безпекою. З погляду методу управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень цей процес буде одним із першочергових у рамках функціональної групи процесів, що належать до «Бази знань».

Основним підходом до управління цим процесом має бути суворий поділ загального потоку документів на два основні типи: зовнішні нормативно-правові документи та внутрішні документи організації, а також подальша їх структуризація, що базується на результатах діяльності адміністративного персоналу організації, функціонування інформаційних та автоматизованих систем, взаємодії із сторонніми організаціями (включаючи зовнішні регулюючі органи), змін у законодавчій базі тощо. Загальна схема моделі взаємодії даних процесу формування та підтримання актуальності інформаційно-довідкової системи з питань інформаційної безпеки при реалізації методу управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень представлена рисунку 3.1.

Рисунок 3.1 – Схема моделі взаємодії даних процесу формування та підтримки актуальності інформаційно-довідкової системи з питань інформаційної безпеки

Управління потоком даних даного процесу є ключовим аспектом у діяльності організації та підрозділів із захисту інформації при реалізації системи захисту інформації та служить плацдармом для побудови подальшої взаємодії між процесами інформаційної безпеки.

3.2 Модель даних процесу управління активами, що захищаються, для організацій, різного роду діяльності

Процес управління активами, що захищаються, для організацій різного роду діяльності є наступною складовою загального процесу управління

інформаційною безпекою у межах запропонованого методу. Загальна схема моделі взаємодії даних процесу управління активами, що захищаються, для організації при реалізації методу управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень представлені на рисунку 3.2.

Рисунок 3.2 – Схема моделі взаємодії даних процесу управління захищеними активами організації

Грунтуючись на діяльності групи експертів, які формують вимоги до справжнього процесу у прив'язці до вимог інформаційно-довідкової системи організації з питань інформаційної безпеки, проводиться первинне визначення

загальної кількості, складу та класифікації активів, що захищаються в організації. Визначаються власники активів у рамках бізнес-процесів організації, а також відповідальні за актив особи. Визначаються правила надання доступу до активу з боку внутрішніх користувачів організації та зовнішніх залучених співробітників сторонніх організацій, що здійснюється в рамках інформаційної взаємодії

Таким чином формується паспорт активів, що захищаються, в яких у будь-який момент часу має відображатися актуальна інформація щодо поточного стану всіх активів, що захищаються, яка використовується в рамках суміжних процесів управління інформаційною безпекою.

В рамках запропонованого методу для управління інформаційною безпекою на основі динамічних експертних СППР активам, що захищаються в організації, експертною групою будуть визначатися основні мінімально значимі структурні одиниці організації, щодо яких збудується подальше керування. До таких одиниць можуть належати автоматизовані чи інформаційні системи, що функціонують в організації. Цей підхід дає можливість структурувати та систематизувати вимоги в галузі забезпечення інформаційної безпеки як всій системі в цілому, так і до конкретних аспектів зокрема. Слід зазначити, що з точки зору методу управління інформаційною безпекою на основі динамічних експертних СППР цей процес буде одним із складових частин у рамках функціональної групи процесів, що належать до «Бази знань», а процес формування структурних одиниць - до групи «Експерт та інженер знань».

3.3 Модель даних процесу управління ресурсами системи захисту інформації

Процес управління ресурсами системи захисту є складовою загального процесу управління інформаційною безпекою у межах запропонованого методу. Цей процес багато в чому схожий з процесом управління активами,

що захищаються в організації і пояснюється схожістю даних понять. Також, як і для захищених активів, група експертів формує вимоги до ресурсів СЗІ, ґрунтуючись на вимогах зовнішньої та внутрішньої документації організації, сформованих у рамках інформаційно-довідкової системи організації з питань інформаційної безпеки. Далі йде визначення складу, кількості та переліку виконуваних функцій даних ресурсів, після чого визначається відповідальний за функціонування даних ресурсів, а також визначаються загальні та приватні правила доступу до ресурсу як з боку внутрішнього персоналу, так і з боку представників сторонніх організацій. Загальна схема моделі взаємодії даних процесу управління ресурсами СЗІ при реалізації методу управління інформаційною безпекою на основі динамічних експертних СППР представлена рисунку 3.3.

Сукупна інформаційна картина, що відображає відомості про склад, кількісні та якісні характеристики ресурсів СЗІ, включаючи наявність залежних ресурсів, визначення групи ресурсів, що реалізують кінцеву множину функцій захисту, а також перелік інформаційних активів, що захищаються, захист яких забезпечується ресурсами системи захисту, формує паспорт ресурсу.

Після цього відбувається подальша обробка даної інформації з боку суміжних процесів управління інформаційною безпекою згідно з запропонованим методом. Дані про визначені ресурси системи захисту інформації також мають брати участь у рамках визначення мінімально значимих структурних одиниць системи з питань інформаційної безпеки організації.

Як і для інформаційних активів, що захищаються, з точки зору методу управління інформаційною безпекою на основі динамічних експертних СППР цей процес буде однією з складових частин у рамках функціональної групи процесів, що належать до «Бази знань», а процес формування структурних одиниць - до групи «Експерт та інженер знань».

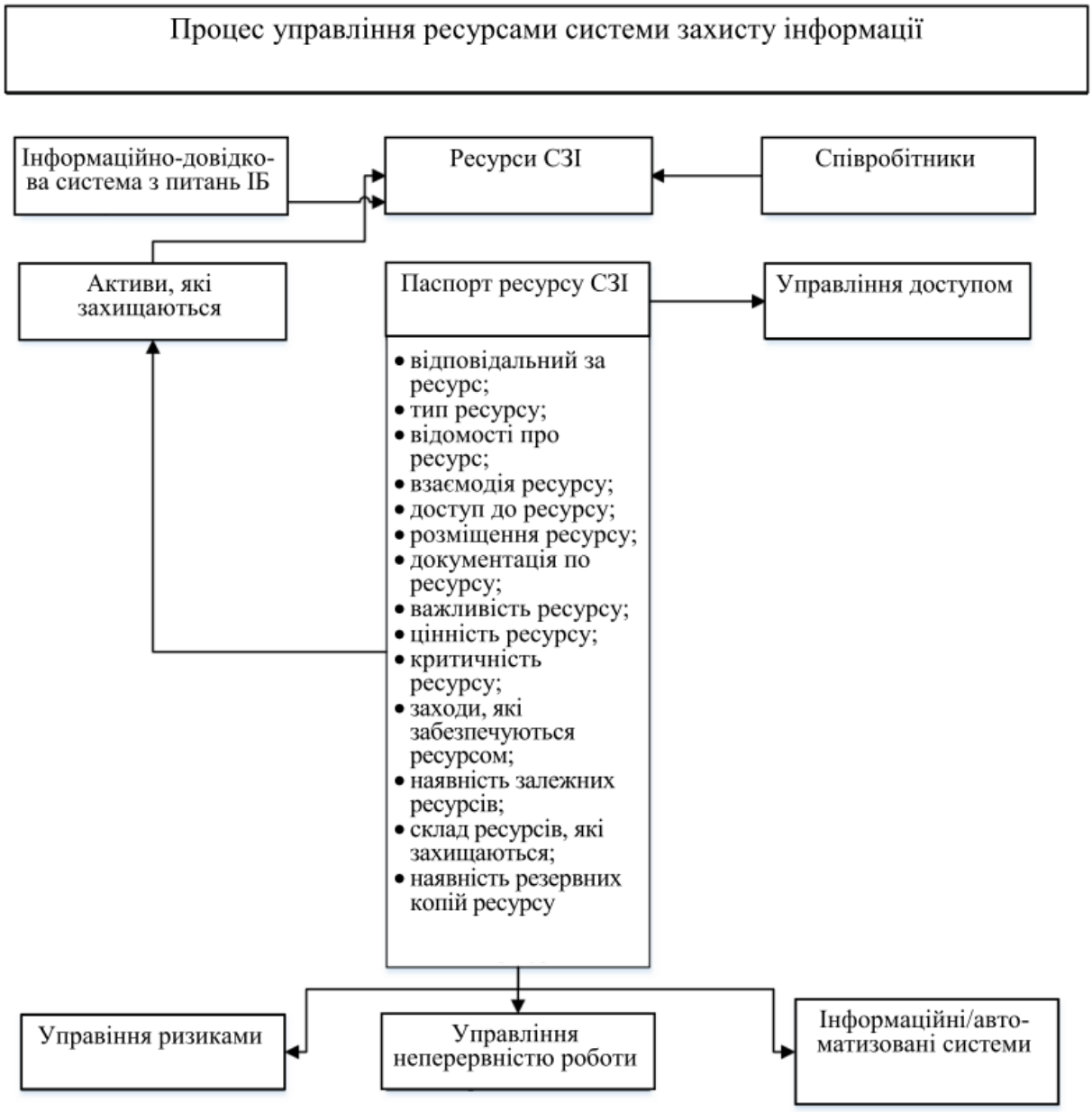

Рисунок 3.3 – Схема моделі взаємодії даних процесу управління ресурсами системи захисту інформації

3.4 Модель даних процесу управління інформаційною безпекою при роботі з персоналом організацій різного роду діяльності

Процес управління інформаційною безпекою під час роботи з персоналом організацій різного роду діяльності є одним із складових процесів управління інформаційною безпекою загалом. Цей процес є ключовим у рамках забезпечення інформаційної безпеки при найму нових співробітників,

підтримці загального рівня інформаційної безпеки в організації, а також під час здійснення взаємодії суміжних процесів управління інформаційною безпекою. Цей процес можна розглядати щодо самого циклу трудових відносин, починаючи з відбору кандидатів та закінчуючи звільненням працівника. Загальна схема моделі взаємодії даних процесу управління інформаційною безпекою під час роботи з персоналом у рамках методу управління інформаційною безпекою на основі динамічних експертних СППР представлена рисунку 3.4.

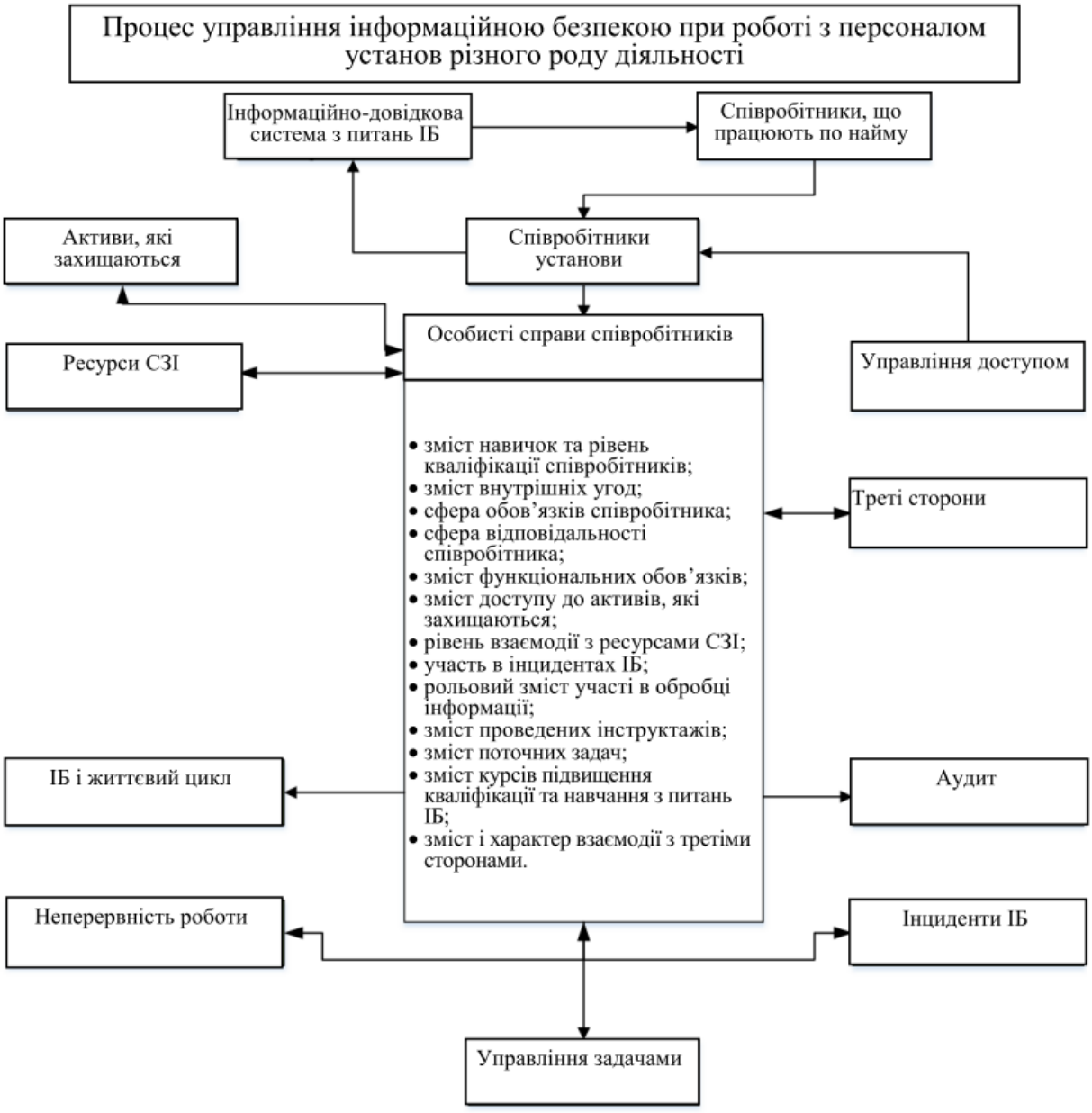

Рисунок 3.4 – Схема моделі взаємодії даних процесу управління інформаційною безпекою під час роботи з персоналом організації

Незалежно від поточного етапу трудових відносин співробітників та організації в рамках цього процесу необхідний раціональний підхід до ведення особових справ працівників, у складі якої, крім загального рівня кваліфікації та підготовки працівників, необхідно вести облік та своєчасну актуалізацію таких відомостей, як:

− склад та утримання внутрішніх угод організації та її співробітників;

− сферу посадових та функціональних обов'язків співробітника;

− сферу відповідальності співробітника;

− склад і привілеї доступу співробітника до активів і ресурсів, що захищаються у системі захисту інформації;

− участь в інцидентах інформаційної безпеки;

− наявність та склад проведення ознайомлення та підвищення обізнаності щодо ключових питань інформаційної безпеки в організації;

− можливості та характер взаємодії зі сторонніми організаціями;

− перелік поточного навантаження та основних завдань.

Даний підхід дозволить мати актуальну інформацію не тільки про навантаження та особливості трудових взаємовідносин співробітника, а й про його реальну участь у питаннях забезпечення інформаційної безпеки в організації.

Загальний перелік даних буде використовуватися для подальшої обробки та систематизації в рамках суміжних процесів управління інформаційною безпекою відповідно до положень запропонованого методу, а також при систематизації та розподілі інформації по структурних одиницях інформаційної безпеку організації. З погляду методу управління інформаційною безпекою на основі динамічних експертних СППР цей процес буде однією з складових частин у рамках функціональної групи процесів, що належать до «Бази знань», а процес формування структурних одиниць - до групи «Експерт та інженер знань».

3.5 Модель даних процесу управління інформаційною безпекою при інформаційному обміні та співпраці з третіми особами

Процес управління інформаційною безпекою при інформаційному обміні та співробітництво з третіми особами є одним із ключових процесів у рамках діяльності будь-якої організації. Наявність системного підходу до побудови цього процесу дає можливість суттєво збільшити загальний рівень інформаційної безпеки в організації, виключити чи суттєво утруднити несанкціоноване використання інформації, а також найбільш ефективно оцінювати ризики, що виникають при інформаційному обміні. В межах цього процесу необхідно визначити перелік організацій, із якими передбачається здійснення інформаційного обміну чи взаємодії. Найбільш простим та повним вирішенням даного аспекту є формування типових угод та порядків надання доступу до активів, що захищаються для абстрактної організації.

У цих документах мають бути відображені підстави для інформаційного обміну або співробітництва з сторонніми організаціями або третіми сторонами, що виникають у рамках основної діяльності організації. З урахуванням вимог зовнішньої та внутрішньої документації, що діє в організації, мають бути укладені типові угоди між взаємодіючими організаціями, у яких мають бути однозначно визначені:

− характер здійснюваної взаємодії;

− склад активів, що захищаються, до яких матимуть доступ сторонні організації;

− ресурси системи захисту інформації, які забезпечуватимуть безпечну взаємодію із сторонніми організаціями;

− порядок та правила доступу до інформаційних та автоматизованих систем організації;

− склад та відповідальність персоналу, що здійснює взаємодію;

− відповідальність за порушення правил взаємодії організацій при інформаційному обміні та співробітництві;

− порядок розбору, закриття та розслідування інцидентів інформаційної безпеки, що сталися з вини або за участю представників третіх сторін.

Сувора регламентація всіх аспектів інформаційного обміну та взаємодії з сторонніми організаціями є не простою необхідністю. Даний аспект безпосередньо впливає на загальний рівень інформаційної безпеки в організації, а відсутність цього процесу як складової СЗІ може нівелювати всі використовувані заходи та механізми захисту інформації.

Слід зазначити, що цей процес практично повністю реалізується організаційними заходами щодо захисту інформації в організації, проте технічна складова не менш важлива. Інформація про взаємодію із сторонніми організаціями безпосередньо впливає на процеси управління активами, що захищаються ресурсами СЗІ, доступом, забезпеченням безперервності діяльності організації, інцидентами інформаційної безпеки, а також має непрямий вплив на суміжні процеси управління інформаційною безпекою в установі. Також слід враховувати, що цей процес має рівну спрямованість і має на увазі його використання для всіх організацій, що беруть участь в інформаційному обміні та співробітництві.

З погляду методу управління інформаційною безпекою на основі динамічних експертних СППР цей процес буде одним із складових частин у рамках функціональної групи процесів, що належать до «Бази знань». Загальна схема моделі взаємодії даних процесу управління інформаційною безпекою при інформаційному обміні та співпраці з третіми сторонами в рамках реалізації методу управління інформаційною безпекою на основі динамічних експертних СППР представлена на рисунку 3.5.

3.6 Модель даних процесу управління інформаційною безпекою при здійсненні життєвого циклу автоматизованих та інформаційних систем

Процес управління інформаційною безпекою під час здійснення життєвого циклу інформаційних систем є одним із ключових у рамках

запропонованого методу управління інформаційною безпекою на основі динамічних експертних СППР. Цей процес акумулює цілу низку сукупних даних по поточному стану автоматизованих та інформаційних систем, що діють в організації.

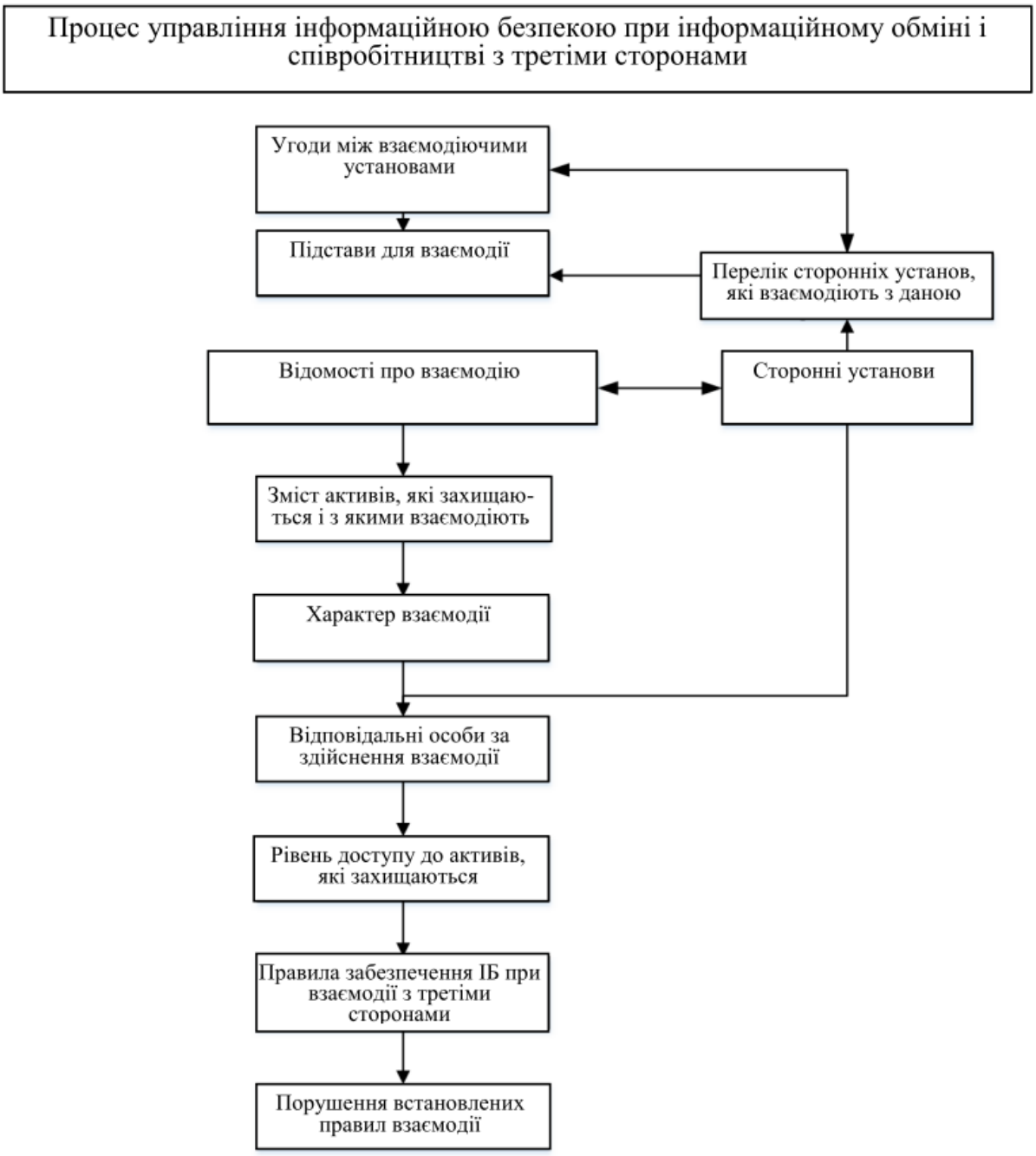

Рисунок 3.5 – Схема моделі взаємодії даних процесу управління інформаційною безпекою при інформаційному обміні та співпраці з третіми особами

Цей процес безпосередньо залежить від складу та вимог внутрішніх та зовнішніх нормативно-правових документів, що діють в організації, та систематизованих у рамках процесу формування та актуалізації інформаційно-довідкової системи організації. У рамках даного процесу визначаються, систематизуються та надалі актуалізуються:

− склад активів, що захищаються, згрупованих у рамках аналізованої автоматизованої чи інформаційної системи;

− склад та функції ресурсів СЗІ, що реалізують захисні функції в рамках аналізованої автоматизованої чи інформаційної системи;

− склад і характер функціонального навантаження аналізованої автоматизованої чи інформаційної системи;

− правила та привілеї доступу користувачів до систем;

− перелік співробітників, які взаємодіють із системами;

− відповідальні особи за обслуговування систем;

− наявність, склад та характер взаємодії систем одна з одною.

В результаті функціонування даного процесу інформація, що збирається та оброблюється в ньому, передаватиметься для подальшої обробки у суміжні процеси управління інформаційною безпекою.

З погляду методу управління інформаційною безпекою на основі динамічних експертних СППР цей процес буде одним із складових частин у рамках функціональної групи процесів, що належать до "Редактору бази знань". Загальна схема моделі взаємодії даних процесу управління інформаційною безпекою при здійсненні життєвого циклу автоматизованих та інформаційних систем у рамках реалізації методу управління інформаційною безпекою на основі динамічних експертних СППР представлено рисунку 3.6.

Слід враховувати, що від цього процесу залежатиме актуальність та коректність подальшої обробки інформації не лише в рамках методу управління інформаційною безпекою на основі динамічних експертних СППР, а також у рамках всього підходу до забезпечення інформаційної безпеки, у зв'язку з чим необхідність впровадження та підтримки даного процесу є

однією з першочергових задач у рамках діяльності будь-якої організації. Крім управління інформаційною безпекою, цей процес суттєво полегшує подальший розвиток СЗІ та позначає найбільш пріоритетні напрями у її розвитку, а також полегшує виконання цілого ряду суміжних процесів управління та забезпечення інформаційної безпеки, знижуючи та розподіляючи навантаження на персонал організації захисту інформації, що істотно відбивається на ефективності СЗІ в цілому, та механізмах захисту зокрема.

Рисунок 3.6 – Схема моделі взаємодії даних процесу управління інформаційною безпекою при здійсненні життєвого циклу автоматизованих та інформаційних систем

3.7 Комплексна модель управління інформаційною безпекою на основі систем підтримки прийняття рішень та розрахунок її ефективності

Узагальнюючи розглянуті процеси, можна побудувати комплексну модель управління інформаційною безпекою на основі СППР (рисунок 3.7).

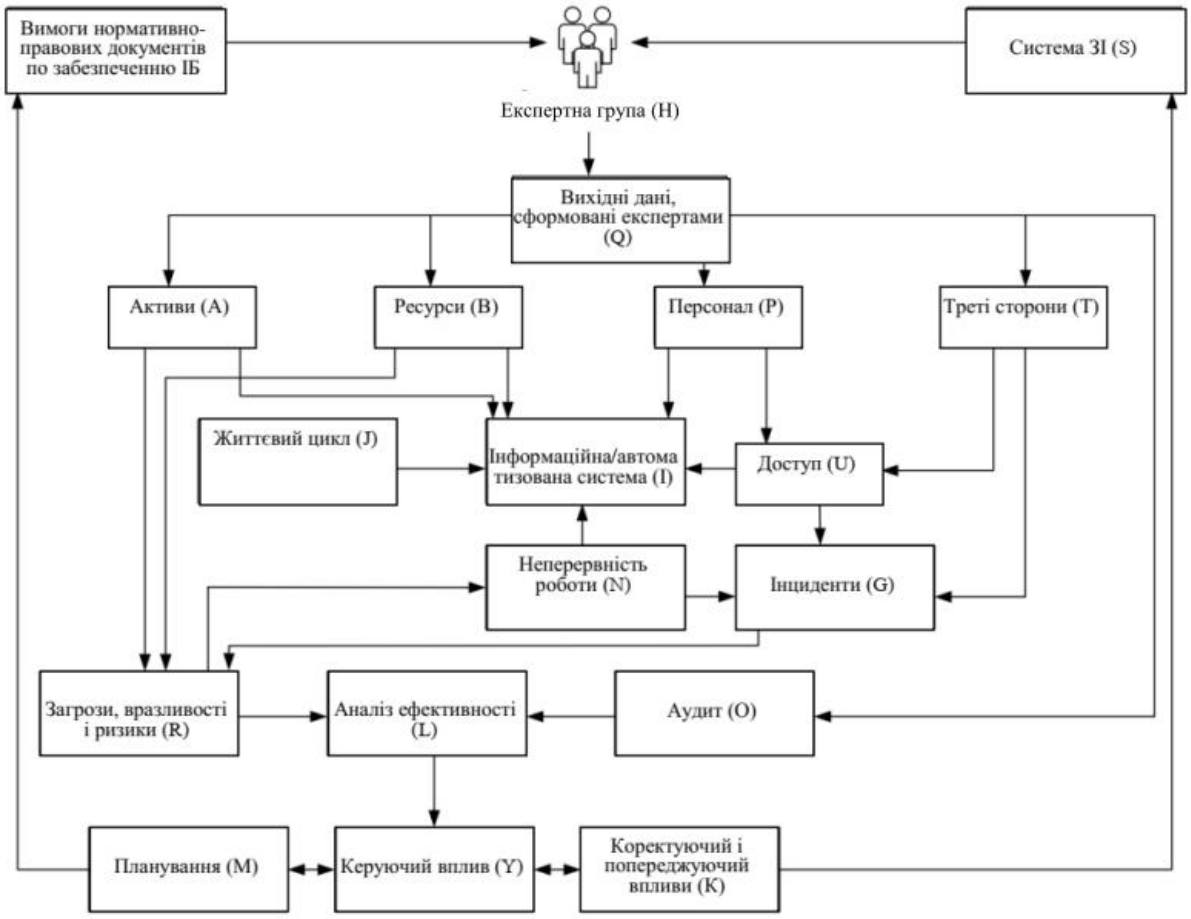

Рисунок 3.7 - Комплексна модель управління інформаційною безпекою на основі СППР

Ефективність побудованої моделі визначається як зважене додавання втановлених факторів (або критеріїв). Тоді коефіцієнт ефективності, яким володітиме СЗІ при використанні розробленого методу та моделі управління на основі динамічних експертних СППР, буде мати такий вигляд:

$$W(S_i) = \sum_{f=1}^{n} a_f s_f(S_i), \tag{3.1}$$

де S_1 – вихідні модель та метод управління ІБ;

S_2 – розроблені модель та метод управління ІБ на основі динамічних експертних СППР;

W(S_i) – коефіцієнт ефективності або вага СЗІ;

f – індекс, що встановлює номер фактору (або критерію);

N – кількість становлених факторів (критеріїв);

a_f – коефіцієнт, що характеризує вклад кожного із факторів $c_f(S_i)$ у вагових коефіцієнтах для визначення ефективності СЗІ, причому $\sum_{f=1}^{N} a_f = 1$; $0 \le a_f \le 1$;

$c_f(S_i)$ – часткові коефіцієнти (або показники) ддя конкретного фактору чи критерію, який характеризуватиме ефективність СЗІ із використанням моделі та методу управління ІБ, причому $0 \le c_f(S) \le 1$.

В таблиці 3.1 наведено фактори (критерії), які мають значний вплив на ефективність СЗІ, та відповідні показники для розрахунку ефективності.

Таблиця 3.1 - Значення вагових коефіцієнтів для визначення ефективності еталонних і розроблених моделей управління інформаційною безпекою

Фактори, що впливають на СЗІ		Ступінь важливості коефіцієнта	Коефіцієнт для вихідних метода і моделі	Коефіцієнт для розроблених метода і моделі
1	Час на впровадження методу ІБ	0,25	1	1
2	Час на збір вихідних даних	0,1	0,5	1
3	Час на обробку інформації	0,15	0,3	1
4	Час на актуалізацію інформації	0,15	0,4	1
5	Час на прийняття управлінського рішення	0,25	0,6	1
6	Час на аналіз отриманих результатів	0,1	0,3	1
Підсумковий коефіцієнт ефективності			0,58	1

Коефіцієнт ефективності СЗІ S_1 обчислюється за такою формулою:

$$W(S_1) = 0{,}25 \cdot s_1(S_1) + 0{,}1 \cdot s_2(S_1) + 0{,}15 \cdot s_3(S_1) + 0{,}15 \cdot s_4(S_1) + 0{,}25 \cdot s_5(S_1) + 0{,}1 \cdot s_6(S_1).$$

Тобто $W(S_1) = 0{,}25 \cdot 1 + 0{,}1 \cdot 0{,}5 + 0{,}15 \cdot 0{,}3 + 0{,}15 \cdot 0{,}4 + 0{,}25 \cdot 0{,}6 + 0{,}1 \cdot 0{,}3 = 0{,}58.$

Формула для підсумкового коефіцієнта ефективності СЗІ з використанням розроблених метода і моделі управління ІБ S_2 має вигляд:

$$W(S_2) = 0{,}25 \cdot s_1(S_2) + 0{,}1 \cdot s_2(S_2) + 0{,}15 \cdot s_3(S_2) + 0{,}15 \cdot s_4(S_2) + 0{,}25 \cdot s_5(S_2) + 0{,}1 \cdot s_6(S_2).$$

Тобто $W(S_2) = 0{,}25 \cdot 1 + 0{,}1 \cdot 1 + 0{,}15 \cdot 1 + 0{,}15 \cdot 1 + 0{,}25 \cdot 1 + 0{,}1 \cdot 1 = 1.$

На основі наведених розрахунків та отриманих результатів випливає висновок, що запропоновані метод і модель управління ІБ на основі динамічних експертних СППР суттєво зменшують час на ухвалення управлінських рішень і збільшують ефективність СЗІ на 42%.

ВИСНОВКИ

1. Визначено основні напрямки заходів щодо забезпечення захисту інформації та управління інформаційною безпекою, що дозволило розробити схему взаємозв’язку ризиків з використанням систем підтримки прийняття рішень та встановити типові підходи до застосування систем підтримки прийняття рішень для управління інформаційною безпекою.

2. Визначено апріорну можливість реалізації загроз інформаційній безпеці на основі систем підтримки прийняття рішень, що дозволило встановити ступінь небезпеки та оцінку можливості реалізації загроз інформаційній безпеці з урахуванням систем підтримки прийняття рішень.

3. Розроблено структуру методу управління інформаційною безпекою на основі систем підтримки прийняття рішень, що дозволило побудувати часткові та комплексну моделі даних процесу управління інформаційною безпекою.

4. Розроблено часткові та комплексну модель для управління інформаційною безпекою на основі систем підтримки прийняття рішень.

.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. К.: ДУТ, 2015. 449 с.
2. Дузь-Крятченко О. П., Грицай П. М., Грищенко В. П., Клименко В. С. та ін. Основи стратегії національної безпеки та оборони держави: підруч. К. : НУОУ ім. Івана Черняховського, 2015. – 620 с.
3. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики: Вибр. наук. праці. К. : НІСД, 2016. 528 с.
4. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. Житомир: ЖНАЕУ, 2016. 636 с.
5. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. К.: ДУТ, 2015. 288 с.
6. Волокітін А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Інформаційна безпека державних організацій і комерційних фірм. К.: Юніор, 2012. 303 с.
7. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
8. Рекомендації ITU – T [Електронний ресурс]. Режим доступу до ресурсу: https://www.itu.int/ITU-T/recommendations/index.aspx?ser=H .
9. ITU-R Recommendation E.800 Terms and definitions, related to Quality of Services and network performance including dependability.
10. ITU-T Recommendation P.862: "Perceptual evaluation of Speech Quality (PESQ), an objective method for End to end speech quality assessment of narrowband telephone networks and speech codecs".

11. Рекомендації ETSI [Електронний ресурс]. Режим доступу до ресурсу: https://www.etsi.org/ .

12. Бовда Е.М., Сальник В.В. Методи забезпечення якості обслуговування в сучасних телекомунікаційних мережах військового призначення. Збірник наукових праць Харківського національного університету Повітряних Сил. 2017. № 2(51). С. 85-94.

13. QoS [Електронний ресурс]. Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/QoS.

14. Пількевич І.А., Лобанчикова Н.М.,. Молодецька К.В. Захист інформації в автоматизованих системах управління: посібник. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

15. Лісовська Ю. Кібербезпека. Ризики та заходи. К.: Кондор, 2019. 272 с.

16. Антонюк А.О., Жора В.В. Теоретичні основи моделювання та аналізу систем захисту інформації: [монографія] / Ірпінь Національний університет ДПС України, 2010. 310 с.

17. Гринчук А.М., Пилипів С.І., Войтенко О.О., Черняк В.А. Структура центру управління інформаційною безпекою для протидії загрозам. Збірник матеріалів проблемної наукової міжгалузевої конференції «Автоматизація та комп’ютерно-інтегровані технології» (АКІТ-2022). Тернопіль, 2022. С.88-90.

18. Гринчук А.М., Лисобей Л.В., Черняк В.А. Математична модель управління інформаційною безпекою установи. Збірник матеріалів проблемної наукової міжгалузевої конференції «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2022). Тернопіль, 2022. С.43-45.

19. Петраков А.В. Основи практичного захисту інформації. К.: Юніор, 2009. 395 с.

20. Остапов С. Технології захисту інформації. Посібник. Родовід, 2014. 428 с.

21. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. К.: КПІ ім. Ігоря Сікорського, 2018. 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/ TZI_book.pdf

22. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. К.: ДУТ, 2015. 288 с.

23. http://www.leta/services/information-security-management/isms-iso-27001.html

24. http://www.e4group.ru/about/control-system/the-system-of-information-securitymanagement/

25. https://ua.wikipedia.org/wiki/Інформаційна_безпека

26. Рак А., Залужна В. Структура методу управління інформаційною безпекою на основі систем підтримки прийняття рішень. Матеріали науково-практичного симпозіуму «Захист інформації» (ЗІ-2024). Тернопіль, 2024. С.82-84 [26].

27. Рак А., Прончук Д. Комплексна модель управління інформаційною безпекою та розрахунок її ефективності. Збірник матеріалів проблемної наукової міжгалузевої конференції «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2024). Тернопіль, 2024. С.156-157 [27].

28. Юдін О.К., Богуш В.М. Інформаційна безпека держави. Харків: Консум, 2005. 576 с.

29. Довгань О.Д. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. 2018. № 1 (24). С. 89-103.

30. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник. Київ: ООО «Д.В.К.», 2014. 508 с.

31. Лужецький В.А. Інформаційна безпека: навч. посіб. Вінниця: УНІВЕРСУМ-Вінниця, 2009. 240 с.