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

ГРИНЧУК Андрій Михайлович

Алгоритми управління інформаційною безпекою на основі експертних динамічних систем / Information security management algorithms based on expert dynamic systems

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
А.М. Гринчук

_____

Науковий керівник
к.т.н., доцент Н.Г.Яцків

_____

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2022 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2022

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

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

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ГРИНЧУК Андрій Михайлович

(прізвище, ім'я по-батькові)

1. Тема кваліфікаційної роботи
Алгоритми управління інформаційною безпекою на основі експертних динамічних систем / Information security management algorithms based on expert dynamic systems
керівник роботи: к.т.н., доц. Н.Г.Яцків
затверджені наказом по університету від 31 грудня 2021 року № 606
2. Строк подання студентом закінченої кваліфікаційної роботи
16 листопада 2022 р.
3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.
4. Основні питання, які потрібно розробити

– аналіз міжнародної нормативної документації та типових підходів до питань управління інформаційною безпекою;

– класифікація процесних складових та опрацювання методів прийняття управлінських рішень під час управління інформаційною безпекою;

– розробка алгоритмів та моделей даних процесів управління ризиками та загрозами, аудитом інформаційної безпеки, аналізу ефективності систем захисту інформації;

– розробка комплексної моделі управління взаємодією даних у системі забезпечення ІБ на основі процесного підходу;

– оцінка ефективності системи захисту інформації із застосуванням розробленого методу та моделі управління інформаційної безпеки..

5. Перелік графічного матеріалу у роботі.

Блок-схема алгоритму дії.

Зв'язок параметрів загроз інформаційній безпеці.

Приклад побудови загального дерева загроз для активу, що захищається.

Схема моделі взаємодії даних процесу управління ризиками та загрозами інформаційної безпеки.

Схема моделі взаємодії даних процесу управління аудиту інформаційної безпеки.

Схема моделі взаємодії даних процесу управління аналізом ефективності системи захисту інформації.

Комплексна модель управління взаємодією даних в системі забезпечення ІБ на основі процесного підходу.

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання: 11 жовтня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Роль управління інформаційною безпекою в системах захисту інформації	12.2021 р. – 03.2022 р.	
2	Прийняття рішень при управлінні інформаційною безпекою	03.2022 р. – 05.2022 р.	
3	Алгоритми та моделі управління інформаційною безпекою	05.2022 р. – 11.2022 р.	

Студент _____ Гринчук А.М.
(підпис)

Керівник роботи _____ к.т.н., доц. Яцків Н.Г.
(підпис)

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Алгоритми управління інформаційною безпекою на основі експертних динамічних систем” на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека” освітньо-професійної програми «Кібербезпека» написана обсягом 75 сторінок і містить 13 ілюстрацій, 3 таблиці, 1 додаток та 32 джерела за переліком посилань.

Метою випускної кваліфікаційної роботи є розробка алгоритмів управління інформаційною безпекою на основі експертних динамічних систем.

Методи дослідження. Математичні методи моделювання, методи програмування, методи управління інформаційною безпекою, методи застосування експертних систем.

Результати дослідження: Здійснено аналіз міжнародної нормативної документації з питань управління інформаційною безпекою, що дозволило визначити типові підходи до питань управління інформаційною безпекою. На основі класифікації процесних складових управління інформаційною безпекою визначено методи прийняття управлінських рішень при управлінні інформаційною безпекою. Розроблено алгоритми і моделі даних процесів управління ризиками та загрозами, аудитом інформаційної безпеки, аналізу ефективності систем захисту інформації, що дозволило оцінити ефективність системи захисту інформації із застосуванням експертних динамічних систем. Розроблено комплексну модель управління взаємодією даних у системі забезпечення інформаційної безпеки на основі експертних динамічних систем.

Результати роботи можуть успішно застосовуватися для управління інформаційною безпекою у відповідних установах.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, ЕКСПЕРТНА СИСТЕМА, РИЗИКИ, ЗАГРОЗИ, МОДЕЛЬ ДАНИХ.

ABSTRACT

The graduate work on the topic „Information security management algorithms based on expert dynamic systems” for Master’s degree on speciality 125 "Cybersecurity " is written on 75 pages and contains 13 illustrations, 3 tables, 1 suplements and 32 references.

The aim of graduate work is to develop of information security management algorithms based on expert dynamic systems.

Research methods. Mathematical modeling methods, programming methods, information security management methods, expert systems application methods.

Results of the study. An analysis of international regulatory documentation on information security management issues was made, which made it possible to determine typical approaches to information security management issues. Based on the classification of the process components of information security management, the methods of making managerial decisions in the management of information security are defined. Algorithms and models of data processes of risk and threat management, information security audit, analysis of the effectiveness of information protection systems were developed, which allowed to evaluate the effectiveness of the information protection system using expert dynamic systems. A comprehensive model of data interaction management in the information security system based on expert dynamic systems has been developed.

The results of the work can be successfully applied to information security management in relevant institutions.

Keywords: INFORMATION SECURITY, EXPERT SYSTEM, RISKS, THREATS, DATA MODEL.

ЗМІСТ

ВСТУП…….. 8
1 РОЛЬ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ…… 12
1.1 Аналіз міжнародної нормативної документації з питань управління інформаційною безпекою…….. 12
1.2 Типовий підхід до побудови систем захисту інформації та супутні йому недоліки…… 19
1.3 Місце та роль методу управління інформаційної безпеки на основі динамічних експертних систем підтримки прийняття рішень у рамках системи захисту інформації ……. 23
2 ПРИЙНЯТТЯ РІШЕНЬ ПРИ УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ……. 28
2.1 Класифікація процесних складових управління інформаційною безпекою ……. 28
2.2 Проблема прийняття управлінських рішень під час управління інформаційною безпекою …..... 29
2.3 Управління ризиками та загрозами інформаційної безпеки..... 40
3 АЛГОРИТМИ ТА МОДЕЛІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ …… 44
3.1 Модель даних процесу управління ризиками та загрозами інформаційної безпеки …….. 44
3.2 Модель даних процесу управління аудитом інформаційної безпеки …….. 45
3.3 Модель даних процесу управління аналізом ефективності систем захисту інформації ……..... 48
3.4 Комплексна модель управління взаємодією даних у системі забезпечення ІБ на основі процесного підходу……. 51

3.5 Оцінка ефективності системи захисту інформації із застосуванням розробленого методу та моделі управління інформаційної безпеки…….. 56
ВИСНОВКИ……. 60
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…… 61
ДОДАТОК А Копії публікацій..... 64

ВСТУП

На сучасному етапі розвитку нашого суспільства інформація стає одним із найбільш цінних та затребуваних ресурсів, на збереження та захист яких виділяється все більше часу та коштів [1-4]. У зв'язку з цим захист інформації є одним із важливих процесів будь-якої організації [5]. Процес управління інформаційною безпекою (ІБ) нерозривно пов'язаний із процесами захисту інформації [6], адже повнота та коректність його реалізації багато в чому визначає ефективність системи захисту інформації [7] (СЗІ), однак у типовій СЗІ, підсистема управління ІБ, як правило, відсутня. Кількість засобів і заходів захисту інформації постійно збільшується і спільно із існуючими недоліками типової реалізації СЗІ збільшують навантаження на персонал організації, збільшуючи в такий спосіб час прийняття управлінських рішень [8]. Через неможливість збільшення кількості ресурсів, що виділяються на процеси забезпечення та управління ІБ, до нескінченності, особливо гостро постає проблема раціоналізації їх використання з урахуванням сучасних інформаційних технологій (ІТ) та засобів обробки інформації [9-11].

Одним із перспективних напрямків при вирішенні цієї проблеми є використання експертних систем підтримки прийняття рішень, здатних взяти на себе більшу частину функцій та рутинних операцій, що виконуються персоналом [12]. Це суттєво знизить часові рамки після прийняття управлінських рішень [13]. В умовах постійних змін вимог щодо захисту інформації, зміни методологічних підходів та думок експертів з ІБ, а також зміни факторів, що впливають на інформацію, доцільним є застосування динамічних експертних систем. Проте у процесі реалізації систем управління ІБ на основі динамічних експертних систем підтримки прийняття рішень виникає низка суттєвих труднощів, спричинених відсутністю науково обґрунтованого методичного апарату, що враховує не лише потреби та

особливості управління ІБ, включаючи думку експертів організації, а також існуючу специфіку реалізації ІТ інфраструктури.

Таким чином, актуальність даної роботи зумовлюється відсутністю науково-методичного апарату, що враховує потреби та особливості управління ІБ, а також відсутністю систем\підсистем управління ІБ, здатних підвищити ефективність СЗІ за рахунок зниження часових витрат на виконання процесів забезпечення ІБ та прийняття управлінських рішень на основі динамічних експертних систем.

Проблеми забезпечення інформаційної безпеки, формалізації процесних складових, а також складові елементи управління інформаційною безпекою є предметом дослідження багатьох учених [14-17]. Однак переважна більшість з них розглядають у своїх працях аспекти управління та забезпечення ІБ, принципи побудови систем управління, експертні системи окремо, а питання комплексного застосування експертних систем при побудові систем управління ІБ розглядалися недостатньо.

Мета роботи. Метою даної роботи є розробка алгоритмів управління інформаційною безпекою на основі експертних динамічних систем.

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

– аналіз міжнародної нормативної документації та типових підходів до питань управління інформаційною безпекою;

– класифікація процесних складових та опрацювання методів прийняття управлінських рішень під час управління інформаційною безпекою;

– розробка алгоритмів та моделей даних процесів управління ризиками та загрозами, аудитом інформаційної безпеки, аналізу ефективності систем захисту інформації;

– розробка комплексної моделі управління взаємодією даних у системі забезпечення ІБ на основі процесного підходу;

– оцінка ефективності системи захисту інформації із застосуванням розробленого методу та моделі управління інформаційної безпеки.

Об’єкт дослідження. Процес управління інформаційною безпекою.

Предмет дослідження. Алгоритми та моделі управління інформаційною безпекою на основі експертних динамічних систем.

Методи дослідження. Математичні методи моделювання, методи програмування, методи управління інформаційною безпекою, методи застосування експертних систем.

Наукова новизна одержаних результатів.

1. Здійснено аналіз міжнародної нормативної документації з питань управління інформаційною безпекою, що дозволило визначити типові підходи до питань управління інформаційною безпекою.

2. На основі класифікації процесних складових управління інформаційною безпекою визначено методи прийняття управлінських рішень при управлінні інформаційною безпекою.

3. Розроблено алгоритми і моделі даних процесів управління ризиками та загрозами, аудитом інформаційної безпеки, аналізу ефективності систем захисту інформації, що дозволило оцінити ефективність системи захисту інформації із застосуванням експертних динамічних систем.

Практичне значення отриманих результатів.

Розроблено комплексну модель управління взаємодією даних у системі забезпечення інформаційної безпеки на основі експертних динамічних систем.

Публікації та апробація КР.

1. 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].

2. 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].

1 РОЛЬ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Аналіз міжнародної нормативної документації з питань управління інформаційною безпекою

Управління інформаційною безпекою є досить широко обговорюваною темою у міжнародному співтовариствоі Доказом цього факту є наявність серії міжнародних стандартів [20-25], розроблених спільними зусиллями Міжнародної організації стандартів та Міжнародної електротехнічної комісії. Робота над стандартами була розпочата в 1999 році і у підсумковому варіанті документи побачили світ на початку 2000 року у вигляді першої частини, у якій на досить простому рівні описувалася сформована проблематика сучасних тенденцій розвитку інформаційної безпеки і давалися практичні рекомендації щодо здійснення впровадження механізмів управління інформаційною безпекою. Через кілька років, у 2002 році, була випущена друга частина документа, що описує загальну специфікацію пропонованих першою частиною документа рішень, потім послідували супутні документи серії. Варто зазначити, що серія стандартів продовжує розвиватися, а ряд стандартів, що входять до серії, постійно переглядається та оновлюється. Підсумкова версія другої частини документа отримала широку популярність та схвалення в міжнародному співтоваристві. Результатом даних досліджень послужив вихід стандарту ISO\IEC 27001.

У процесі проведення дослідження стандартам [26] та [27] було приділено особливу увагу. Зокрема, перший стандарт описує основні принципи організації управління інформаційною безпекою для організацій різного роду діяльності, тоді як другий стандарт більше приділяв увагу безпосереднім механізмам управління інформаційною безпекою з послідовним розбиттям кроків щодо реалізації кожного із запропонованих механізмів.

ISO\IEC 27000 є своєрідною передмовою до інших документів серії, основне призначення якого зводиться до опису сфери впливу кожного зі стандартів, а також опису загальних принципів та причин виникнення стандарту. Дається посібник з використання змісту стандартів при введенні системи менеджменту інформаційної безпеки в організації, а також опис основних процесних складових та актуальності застосування цієї системи. Відповідно до структури ISO\IEC 27000, сімейство (серія) стандартів являє собою логічно пов'язані документи, систему менеджменту інформаційної безпеки. Схема зв'язків документів, що входять до серії, представлена на рисунку 1.1. Основною метою цієї серії є введення системи менеджменту інформаційної безпеки в організаціях різної величини та роду діяльності. В додаток до документа представлені слівні форми вираження стандартів, категорований перелік термінів з інформаційної безпеки, що застосовуються в стандарті.

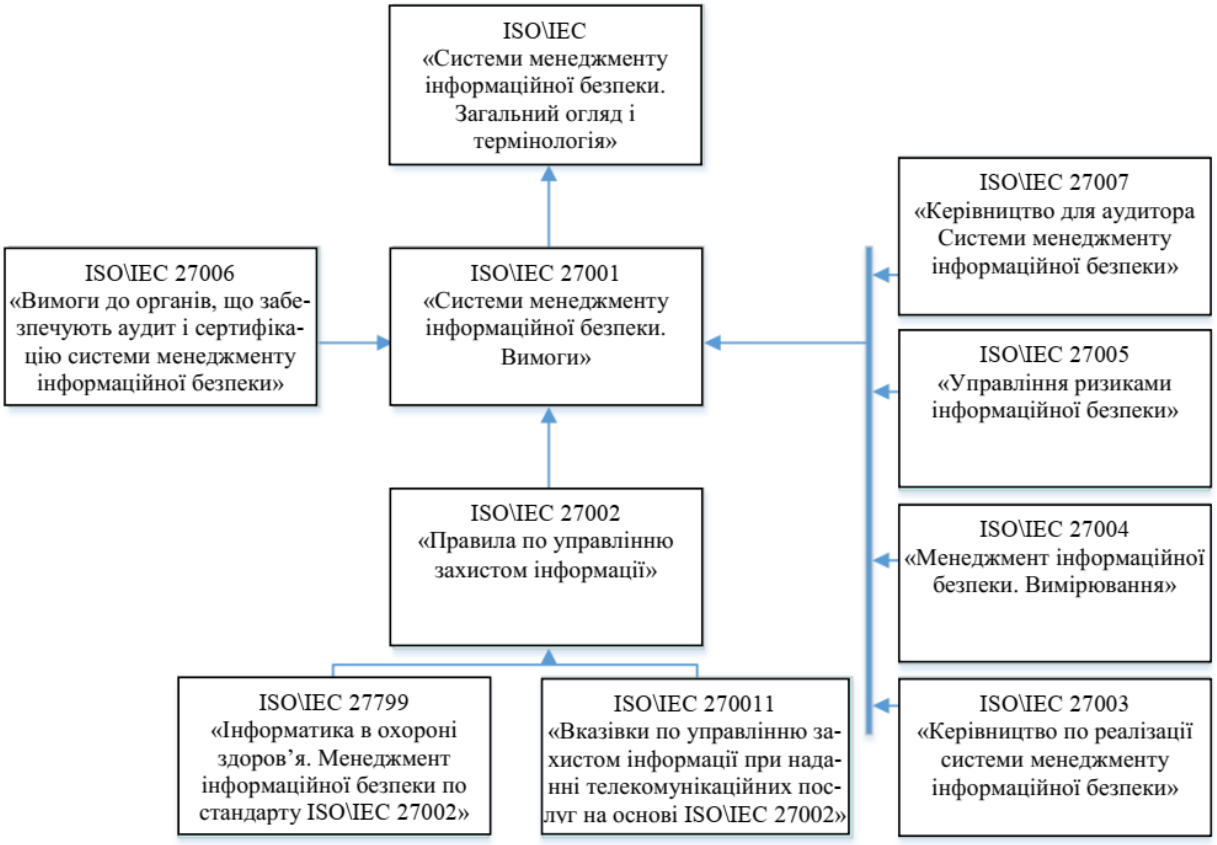

Рисунок 1.1 – Схема логічних зв'язків документів, що входять до складу серії про систему менеджменту інформаційної безпеки

Відповідно до положень ISO\IEC 27001, система менеджменту інформаційної безпеки повинна мати процесний характер, що дотримується положень циклу Демінга - Шухарта, що полягає в послідовності дій щодо планування процесу, його здійсненні та подальшої перевірки. Після цього має йти зміна, що полягає в плавному перегляді підходів та актуалізації уваги на наступне планування. Далі цикл повторюється.

Відповідно до вимог стандарту, керівництво організації має визначити межі дії систем управління інформаційною безпекою, після чого сформувати політику управління інформаційною безпекою, що формує концептуальні характеристики бізнесу організації, сукупність її активів та застосовуваних інформаційних технологій. Наступним ключовим етапом має бути оцінка ризиків та вибір методу їх обробки з метою формування єдиної системи поглядів на питання забезпечення та управління інформаційною безпекою у створенні. Наступним етапом має служити виявлення ризиків згідно з обраним методом, що підходить для конкретної організації. Виявлення ризиків передбачається здійснювати у вигляді формування переліку активів та їх власників з метою виявлення слабких місць, вразливості яких можуть дати поштовх для реалізації загроз інформаційній безпеці, разом із виявленням деструктивних впливів на ці активи з точки зору інформаційної безпеки.

Наступним проміжним етапом є оцінка виявлених ризиків та формування стратегії управлінням ними [28], що полягає в:

− зміні параметрів захисту та управління;

− прийнятті ризиків у разі задоволення умов (раніше описаної) політики;

− порятунок від ризиків;

− покладання відповідальності за дані ризики на сторонні організації, або передача ризиків.

В результаті прийняття певної стратегії управління ризиками, згідно стандарту, має бути зниження рівня ризику до прийнятного рівня –

залишкового ризику. Таким чином, система управління інформаційною безпекою організації є документованою та готовою для впровадження. Відповідно до положень ISO\IEC 27001, процес реалізації та експлуатації системи менеджменту інформаційної безпеки повинен полягати у такому:

1) формулювання плану обробки ризиків;

2) реалізація плану обробки ризиків;

3) формування та застосування засобів управління;

4) оцінка ефективності прийнятих засобів управління;

5) підготовка та здійснення плану підвищення обізнаності персоналу;

6) управління діяльністю системи управління інформаційної безпеки;

7) управління ресурсами системи управління інформаційної безпеки;

8) впровадження у дію систем виявлення інцидентів інформаційної безпеки.

Таким чином, згідно з циклом Демінга – Шухарта, вищеописані дії є процесами планування та здійснення, після яких повинні слідувати процеси перевірки та перегляду попередніх дій (вдосконалення), що й описує інша частина стандарту. Особлива увага приділяється процесам документування вимог та політик організації в галузі інформаційної безпеки та їх захисту, а також формалізації механізмів реагування на інциденти інформаційної безпеки разом із повсюдними «Управлінням записами», яке передбачає постійне ведення журналів, протоколів та форм дозволу доступу, пов'язаних як з активами та їх ризиками, так і з процесами забезпечення інформаційної безпеки організації. Також варто відзначити суттєве акцентування уваги змісту документа на питання вдосконалення системи управління інформаційної безпеки. Згідно даних акцентів, удосконалення має здійснюватися за результатами проведення окремої процедури – власного аудиту системи, метою якого є перевірка відповідності системи бізнес вимогам, ефективності механізмів управління інформаційною безпекою та коректності виконання функцій захисту.

Результатом такої процедури має бути аналітичний висновок можливості покращення, доповнення або видозміни системи, що сприяє подальшому вдосконаленню та розвитку системи управління інформаційною безпекою. У додатку до стандарту надається відповідний перелік, основною метою якого є спроба формалізованого представлення цілей та засобів управління інформаційною безпекою.

Свого роду логічним продовженням вищеописаного стандарту є стандарт ISO\IEC 27002. Насправді цей стандарт дає більш детальний опис дій, представлених у 27001, однак розширює область своєї дії до опису процесів управління активами, описи послідовності прийому в штат та підбору нових працівників з метою виконання вимог щодо інформаційної безпеки та послідовності дій у разі припинення подальшої співпраці з працівниками організації. Також окрему увагу приділено таким аспектам, як фізична та екологічна безпека, включаючи захист периметра, обладнання, працівників від зовнішніх екологічних загроз, розкриваючи особливості процесів утилізації використаних носіїв інформації та обладнання, а також їх повторного використання.

Таким чином, ISO\IEC 27002 формує зведення правил управління інформаційною безпекою, послідовно описуючи дії, подані в ISO\IEC 27001. Особлива увага у стандарті приділяється процедурам управління засобами зв'язку та операцій, які полягають у наступному:

1) формалізація процедур експлуатації IT-обладнання організації, включаючи:

- фіксування змін обладнання;
- формалізації обов'язків персоналу;
- розподіл обов'язків персоналу;
- розмежування коштів розробки, випробувань, експлуатації;

2) визначення механізмів управління надання послуг третім особам, включаючи:

- здійснення надання послуг третім особам;

- контроль за процесом надання послуг третім особам;

- аналіз наданих послуг третім особам та способів їх надання;

- фіксування змін умов надання послуг третім особам;

3) планування реалізації та здійснення приймання нових систем, включаючи управління продуктивністю введених систем та формування способів їх приймання;

4) захист від шкідливого коду, за допомогою опису механізмів та засобів захисту від даних дій;

5) формалізації процедури та здійснення процесів резервного копіювання інформації;

6) формалізації правил поводження з машинними носіями інформації та засобами захисту мережевої інфраструктури;

7) визначення правил здійснення інформаційного обміну як в середині організації, так і при зовнішній взаємодії;

8) опис концептуальних основ захисту інформації при здійсненні та/або використанні послуг електронної торгівлі;

9) опис принципів ведення контрольних журналів подій та їхнього захисту.

Процеси розмежування та управління доступом є одними з основоположних у забезпеченні захисту інформації, що в черговий раз є одним із найбільш детально описаних розділів стандарту – «Керування доступом». Згідно положенням стандарту, управління доступом поділено за такими логічними компонентами:

1) формування політики управління доступом до організації, що формалізує загальне зведення поглядів та вимог до управління доступом. Управління доступом користувачів включає реєстрацію та облік активності користувачів у системі, управління привілеями користувачів у системі, організацію парольної політики та управління паролями користувачів, аналіз діючих систем та привілеїв користувачів у них;

2) формування загального переліку прав та обов'язків користувачів систем організації, включаючи базові засади захисту робочих місць;

3) управління доступом до мереж зв'язку, включаючи управління зовнішніми з'єднаннями та правилами аутентифікації користувачів; захист віддалених з'єднань; управління мережевою інфраструктурою;

4) управління доступом до операційної системи, включаючи обмеження часу активності користувачів; запровадження ліміту дії робочої сесії; систему керування паролями та ідентифікацією\аутентифікацією користувачів на робочих місцях, процедури забезпечення безпеки інформації під час входу до системи організації;

5) управління доступом до інформації та програм, включаючи базові принципи обмеження доступу до інформації та ізоляції найважливіших систем;

6) формалізація принципів обробки інформації за допомогою мобільних та теле-пристроїв.

Заключна частина документа містить у собі базовий набір дій щодо дотримання вимог до інформаційної безпеки при придбанні, розробці та супроводі інформаційних систем організації; виявленні та контролю інцидентів інформаційної безпеки організації загалом та системи захисту інформації зокрема.

Останні глави документа містять дуже просторові рекомендації щодо забезпечення безперервності бізнесу та ролі систем менеджменту інформаційної безпеки в даному процесі, а також поверхневий опис процедур перевірки відповідності юридичним вимогам, внутрішнім політикам і стандартам у сфері захисту інформації, чинним в організації.

Таким чином, підбиваючи підсумки аналізу міжнародної нормативної документації по питаннях управління інформаційною безпекою, можна зробити висновок, що, незважаючи на наявність формалізованих принципів побудови систем управління інформаційною безпекою, розмитість формулювань, поверховість опису ряду суттєвих аспектів у питаннях

управління інформаційною безпекою, а також відсутність обліку специфіки діяльності організацій в умовах сучасних тенденцій розвитку підприємств в інформаційно-телекомунікаційній сфері зводить потребу та доцільність застосування положень даних нормативних документів нанівець.

1.2 Типовий підхід до побудови систем захисту інформації та супутні йому недоліки

Відповідно до чинних положень [29-30], під системою захисту інформації розуміється сукупність органів та виконавців, техніки захисту інформації, яка ними використовується, а також об'єктів захисту інформації, що організована та функціонує за правилами та нормами, встановленим відповідними документами у сфері захисту інформації. При цьому під об'єктом захисту слід розуміти сукупність інформації, носіїв її змісту, а також персоналу та засобів обчислювальної техніки, що забезпечують та здійснюють їх обробку. Такий підхід є типовим у відповідності до положень чинних нормативно-правових документів. Він враховує вимоги, що пред'являються до інформаційної безпеки та захисту інформації, конкретизує сферу дії самої системи захисту інформації та встановлює першорядність персоналу та технічних засобів захисту. З визначення системи захисту інформації слідує, що правила і норми організації і функціонування самої системи встановлені відповідними документами у сфері захисту інформації, однак, як показав аналіз внутрішньої нормативно-правової документації в галузі інформаційної безпеки, дане формулювання є вельми поверхневим і сумнівним. Розглянемо типовий підхід до побудови системи захисту інформації в організації. Згідно з визначенням та загальним розумінням, така система складатиметься із: технічних засобів захисту інформації; об'єкта захисту; органів та виконавців (персоналу, відповідального за забезпечення інформаційної безпеки); організаційних заходів захисту. В залежності від складу оброблюваної інформації (що входить до об'єкту захисту), вимоги

нормативно-правових документів, як внутрішніх для організації, так і зовнішніх встановлюватимуть певні правила взаємодії персоналу, технічних засобів, організаційних заходів та об'єктів захисту. Таким чином, типовий підхід до побудови системи захисту інформації можна подати у схематичному вигляді, зображеному рисунку 1.2.

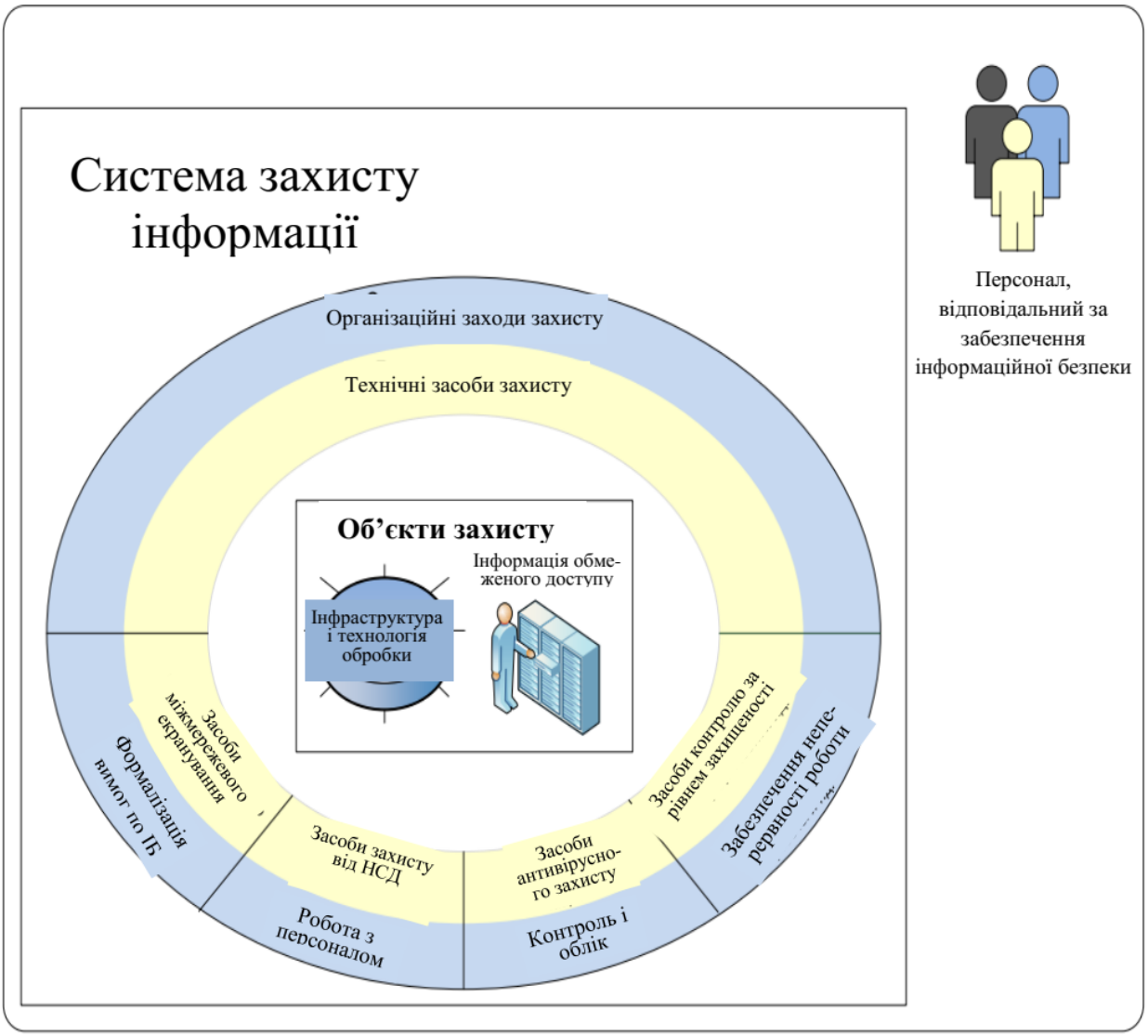

Рисунок 1.2 – Типовий підхід до побудови системи захисту інформації

При типовому підході у складі системи захисту не передбачена єдина підсистема управління організаційними заходами та технічними засобами захисту, яка б дозволяла вести стратегічне, тактичне та оперативне управління інформаційною безпекою, включаючи персонал, засоби захисту, а

також організаційні заходи щодо забезпечення інформаційної безпеки в організації.

Такий стан справ згубно впливає не лише на ефективність окремо взятих застосовуваних організаційних заходів та технічних засобів захисту, а також на сумарний показник ефективності всієї системи захисту інформації в цілому, а також не дозволяє співробітникам організації мати впевненість у своєчасності та доцільності застосування тих чи інших заходів захисту, що насправді на певному етапі роботи може бути сприйнято як сигнал про можливість посереднього ставлення до виконуваних процедур.

Цей недолік характерний для всіх організацій, проте найбільш згубний вплив надає на великі та середні організації, забезпечення інформаційної безпеки яких є однією з невід'ємних складових їх основного виду діяльності.

Також при типовому підході у складі системи захисту інформації не передбачені механізми підтримки та забезпечення зворотного зв'язку, що містить відомості про склад, кількісні, якісні характеристики організаційних заходів та технічних засобів захисту, а також засобів і способів оцінки правильності їх функціонування та застосування.

З урахуванням результатів аналізу нормативно-правової документації у сфері захисту інформації, а також останніх тенденцій у зміні законодавчої та нормативної бази, вказівка на цей недолік та необхідність його усунення у відповідних документах вказана неявно [31]. Однак ці документи лише встановлюють вимоги щодо наявності в системі процесів та механізмів для реєстрації подій інформаційної безпеки, виявлення та реагування на інциденти інформаційної безпеки. При цьому єдиний систематизований підхід до забезпечення даних процесів відсутній.

Наступним суттєвим недоліком типового підходу є практично повна відсутність засобів автоматизації діяльності персоналу з питань застосування та підтримки організаційних заходів захисту [32]. У процесі проведення дослідження та аналізу вимог міжнародної та вітчизняної нормативно-правової документації в галузі інформаційної безпеки було встановлено, що

організаційні заходи захисту інформації становлять близько 80% від загальної кількості реалізованих заходів у системі захисту інформації. При цьому на їх реалізацію буде відводитися лише близько 20% загальних ресурсів організації, включаючи людські, фінансові та часові. У той час, як технічними засобами захисту перекривають лише 20% загальних вимог та реалізованих заходів системи захисту.

Ця статистика показує, що, незважаючи на першорядність прийняття організаційних заходів захисту та відсутність ефективності застосування засобів захисту без належної організаційної підготовки, до організаційних питань щодо забезпечення та управління інформаційною безпекою ставляться формально.

Заключним недоліком, який супроводжує типовий підхід до побудови системи захисту інформації, є відсутність аналітичної складової процесів розвитку та забезпечення системи захисту інформації. Справа в тому, що на сьогоднішній день експертні інформаційно-аналітичні системи аналізу та підтримки прийняття управлінських рішень у галузі інформаційної безпеки відсутні як клас. Наслідком цього є відсутність розвитку підходів та аналітичних викладок щодо вдосконалення систем захисту інформації, побудова яких зводитися до виконання вимог щодо усунення відомих на даний момент каналів витоку інформації, перекриття та усунення базових вразливостей та загроз інформаційній безпеці. При цьому такий підхід є повністю неефективним у плані протидії новим нестандартним діям ймовірних порушників, а також у разі використання ними нетипових методів обходу засобів захисту. Найчастіше роботи з вдосконалення систем захисту інформації, що проводяться в організації, проводяться навіть без урахування поточного стану захищеності об'єктів захисту, а також ефективності застосовуваних методів та способів захисту у конкретних умовах функціонування як самих об'єктів захисту, так і захисних механізмів, що в кінцевому підсумку призводить до нераціонального планування та витрачання бюджету, що виділяється на забезпечення інформаційної безпеки.

Дані фактори також згубно позначаються і на персоналі організації, відповідальному за забезпечення інформаційної безпеки, що відбивається на сукупній ефективності системи захисту інформації в цілому та компетенції працівників організації з інформаційної безпеки зокрема. При типовому підході головне призначення персоналу, відповідального за забезпечення інформаційної безпеки, полягає у протидії всім можливим загрозам, зводиться до обслуговування технічних засобів захисту та часткової реалізації організаційних заходів

1.3 Місце та роль методу управління інформаційної безпеки на основі динамічних експертних систем підтримки прийняття рішень у рамках системи захисту інформації

Грунтуючись на результатах аналізу чинних міжнародних та вітчизняних нормативно-правових документів, були виявлені основні процеси забезпечення та управління інформаційною безпекою, сформульовані та описані ключові недоліки, а також супутні їм проблеми під час побудови системи захисту інформації у межах типового підходу.

При цьому розроблений метод і модель займатимуть ключове місце в рамках реалізації єдиної системи\підсистеми управління інформаційною безпекою у складі системи захисту інформації організації, спрямованої на централізацію\децентралізацію (залежно від основного призначення СЗІ та характеру оброблюваних даних) та спрощення процесів управління та забезпечення інформаційної безпеки. Дані положення схематично представлені рисунку 1.3.

Виходячи із систематизованих уявлень та сформульованих концептуальних принципів формування методу та моделі управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень, роль розробленого методу та моделі в рамках системи захисту інформації полягає в:

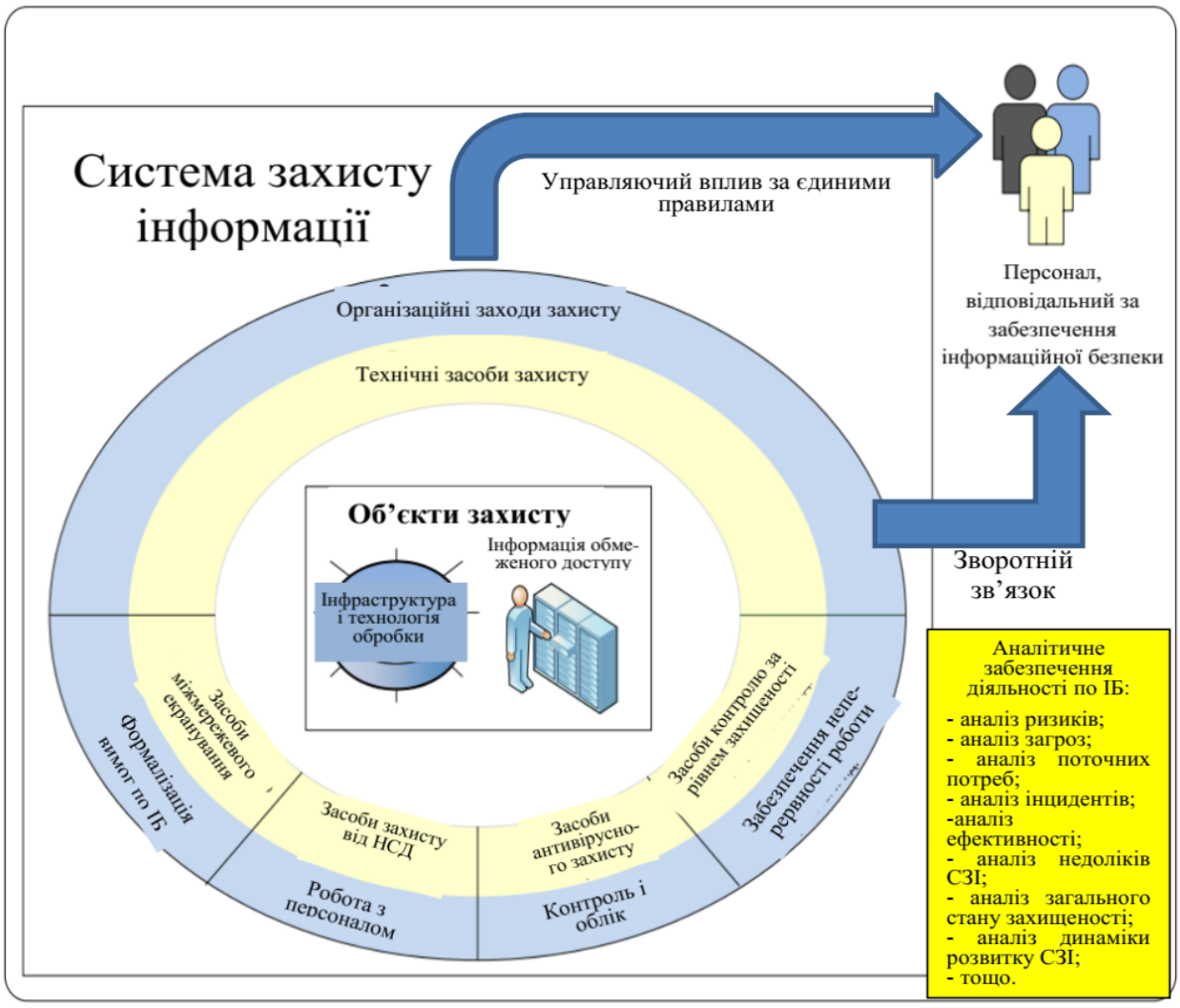

Рисунок 1.3 – Місце методу та моделі управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень, в рамках системи захисту інформації

– формалізації вимог та систематизації процесів забезпечення інформаційної безпеки;

– забезпеченні зворотного зв'язку реалізованих організаційних заходів та технічних засобів захисту із системою захисту інформації;

– автоматизації організаційних заходів захисту та їх співвіднесення з застосовуваними в організації технічними засобами захисту;

– аналітичному забезпеченні діяльності персоналу з інформаційної безпеки.

Залежно від розміру, загального стану та складу системи захисту інформації, а також основного напряму діяльності організації, розроблений метод управління інформаційною безпекою матиме різну архітектуру побудови, а також різний набір основних процесів управління та забезпечення інформаційної безпеки. При цьому, виходячи з типової інформаційно-телекомунікаційної структури організації, реалізація доданих методу та моделі управління інформаційною безпекою дозволить зв'язати розрізнені сервіси інформаційної безпеки організації з організаційними заходами та технічними засобами захисту, а також встановити зв'язок між спеціалізованими інструментами керування технічними засобами та управлінням персоналом організації, що відповідає за забезпечення інформаційної безпеки. На рисунку 1.4 представлена схема функціональної структури центру управління інформаційною безпекою на основі цього методу.

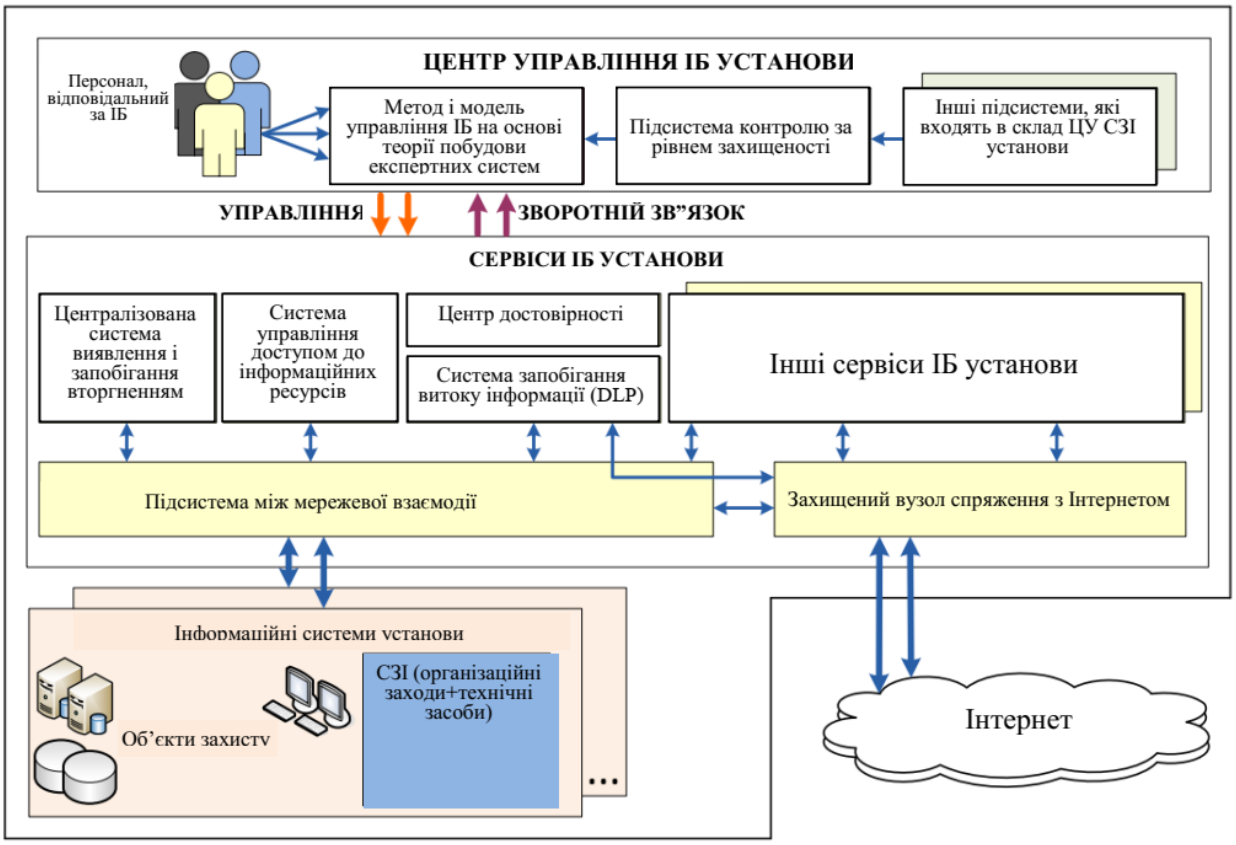

Рисунок 1.4 – Центр управління інформаційною безпекою організації

Створення єдиного центру управління інформаційною безпекою організації на основі запропонованого методу управління інформаційною безпекою буде кінцевою, найбільш повною реалізацією основних положень методу та моделі управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень. При цьому центр управління інформаційною безпекою матиме виділене становище у складі організації, у якому вже сама система захисту інформації буде складовою єдиного центру управління інформаційної безпекою.

Таким чином, реалізація методу та моделі управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень може призвести до:

− систематизації вимог щодо управління інформаційною безпекою, виходячи зі складу процесів забезпечення інформаційної безпеки в організації;

− пов'язаного застосування організаційних заходів та технічних засобів захисту інформації, що діють у рамках системи захисту інформації організації;

− формуванню аналітичної бази проведення досліджень та аналізу стану інформаційної безпеки;

− здійсненню раціонально обґрунтованого стратегічного, тактичного та оперативного управління процесами забезпечення інформаційної безпеки;

− можливості своєчасного застосування коригувальних та попереджуючих впливів на основі комплексного аналізу стану інформаційної безпеки в цілому та об'єктів захисту зокрема;

− забезпечення планування розвитку та підтримки системи захисту інформації;

− формалізації основних та другорядних процесних складових управління та забезпечення інформаційної безпеки в організації;

− підвищення загального рівня інформаційної безпеки організації за рахунок формалізації та систематизації основних процесів інформаційної безпеки;

− зниження операційних ризиків за рахунок зменшення ймовірності реалізації загроз інформаційної безпеки через підвищення загального рівня інформаційної безпеки в організації;

− підвищення прозорості процесів інформаційної безпеки в рамках системи захисту в організації;

− підвищення оперативності при вирішенні завдань забезпечення інформаційної безпеки;

− зниження трудомісткості операцій із забезпечення інформаційної безпеки;

− підвищення рівня компетенції персоналу організації та спеціалістів із захисту інформації у питаннях інформаційної безпеки;

− підвищення оперативності реагування на інциденти інформаційної безпеки;

− мінімізації витрат на експлуатацію системи захисту інформації організації.

2 ПРИЙНЯТТЯ РІШЕНЬ ПРИ УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

2.1 Класифікація процесних складових управління інформаційною безпекою

Відсутність загальноприйнятої класифікації процесів управління ІБ та їх складових є однією з проблем під час побудови системи управління ІБ в організації. Відсутність даної класифікації згубно позначається на можливості визначення та контролю зв'язків між процесами, а також визначення їх основної ролі в рамках систем управління, що розробляються. При проведенні аналізу нормативно-правової бази були виявлені основні класифікаційні ознаки процесних складових управління ІБ, що описують характер їх реалізації в рамках СЗІ організації у вигляді наступного формального правила: $K=<F, Z, I, K, G, N>$, яке складається з таких класифікаційних ознак:

1) за функціональною приналежністю (*F*):
   - − формування вимог;
   - − систематизація інформації;
   - − актуалізація інформації;
   - − аналітичне оброблення інформації;
   - − прийняття управлінських рішень;
2) за характером обробки інформації (*Z*):
   - − із використанням засобів автоматизації;
   - − без використання засобів автоматизації;
3) за характером одержуваної інформації (*I*):
   - − вихідна інформація;
   - − інформація для подальшої обробки;
   - − підсумкова інформація;
4) у зв'язку із засобами захисту (*K*):
   - − антивірусний захист;

− парольний захист;

− криптографічний захист;

− міжмережне екранування;

− інженерні споруди;

− захист від несанкціонованого доступу;

− системи моніторингу подій;

− системи контролю доступу;

− системи аутентифікації;

− засоби аналізу інформації;

5) у зв'язку з реальним часом (*G*):

− динамічна зміна даних;

− періодична зміна даних;

− статичне накопичення даних;

6) за пріоритетом виконання (*N*):

− високий;

− середній;

− низький.

Ця класифікація має велике значення при побудові моделей взаємодії та управління даними як між усіма процесами, так і для конкретного процесу окремо.

2.2 Проблема прийняття управлінських рішень під час управління інформаційною безпекою

Розглянемо окрему організацію, що обробляє критично важливу інформацію. Нехай у цій організації протікає i=1, ..., n рівноправних процесів управління інформаційною безпекою та існує обмежена кількість ресурсів r_i, які витрачаються на їх реалізацію. Кожен із процесів i визначається параметрами $t_i(r_i)$ – час отримання інформації під час виконання процесу, $f_i(x_i)$ – кількість одержуваної інформації під час виконання процесу. У рамках

своєї діяльності організація зазнала атаки з боку зловмисників, що загрожує неперервності діяльності всієї організації. Керівництву організації потрібно прийняти відповідне управлінське рішення для припинення атаки за час t_{max}, при цьому склад наявних ресурсів R є незмінним.

Розглянемо поточний стан справ у організації. В організації існує СЗІ, яка, зіткнувшись з виникненням загрози Y, не може їй протистояти в поточному стані. Нехай поточний (вихідний) стан аналізованої системи - X_0, тоді множина всіх можливих станів - X_1, X_2, X_3, ..., X_k, при цьому P - ймовірність знаходження в k-му стані. Ймовірності усіх станів будуть однакові:

$P_0=P_1=P_2=P_3=\cdots P_k$;

$P_0+P_1+P_2+P_3+\cdots P_k=1$.

Припустимо, що існує такий стан системи $X_Y \in Xk$, коли вона здатна протистояти загрозі Y, таким чином суть прийнятого рішення повинна зводитися до вибору такого стану з множини можливих станів. Згідно положенням теорії інформації, невизначеність знаходження системи в рівно ймовірнісних станах визначатиметься максимальною ентропією H, тоді ентропія для розглянутих випадків, коли невідомий і відомий стан аналізованої системи, у якому вона здатна протистояти загрозі Y, буде H_0 і H_Y відповідно. Згідно з Шенноном, різниця H_0 і H_Y буде кількістю інформації, тоді $F=H_0-H_Y$ буде кількість інформації, необхідна для ухвалення рішення про перехід аналізованої системи з поточного стану X_0 у стан $X_Y \in X_k$, для протистояння загрозі Y.

Позначимо загальну кількість всіх можливих загроз як $Y_{заг}$, очевидно, що виникнута загроза $Y \in Y_{заг}$. Нехай кожна з можливих загроз $Y_x \in Y_{заг}$ (де x=1, 2, …, m – номер загрози) описується сукупним рядом незалежних параметрів α_j (де j=1, 2, …, n – номер параметра), тоді множина $Y_{заг}$ описуватиметься сукупною множиною всіх можливих унікальних параметрів α_{jx}, властивих загрозам. Таким чином можна скласти повну матрицю відповідності загрози та їх параметрів розмірності m на n.

Перш, ніж приймати рішення про переведення СЗІ у певний стан, необхідно визначити загрозу Y. У даному випадку ми стикаємося з невизначеністю вибору, адже ймовірності виникнення кожної із зазначених вище загроз будуть рівними. Таким чином, маємо проблему при прийнятті управлінського рішення, адже у цьому випадку невизначеність, а значить і ентропія H необхідного нам вибору, буде максимальною: $H(Y_x)=-\ln P(Y_x)$, де P – ймовірність виникнення загрози Y_x.

Оскільки отримана максимальна ентропія буде повною (сумісною) ентропією низки незалежних випадкових загроз Y_1, Y_2, ..., Y_m, можна скористатися властивістю адитивності ентропії та представити їх сумісну ентропію як повну суму ентропій щодо кожної загрози:

$H(Y_x)=H(Y_1)+H(Y_2)+H(Y_3)+\dots$.

Для того, щоб знизити отриману невизначеність і прийняти рішення про переведення СЗІ у стан, здатний протистояти загрозі Y, необхідно зробити збір інформації, здатної описати загрозу, тобто визначити один із сукупних параметрів α_{jx}. Кожен із процесів ІБ, що протікають в організації, здатний надати інформацію про значення поточного параметра для загрози, що виникла, а грунтуючись на співвідношенні параметрів, вказаних у таблиці 2.1, залежно від отриманих значень ряд загроз із загальної множини $Y_{\text{заг}}$ буде відхилятися через невідповідність отриманого параметра, таким чином підвищуючи кількість визначених параметрів загрози, невизначеність вибору стану захисту зменшується. Розглянемо випадок, коли загальна кількість можливих загроз дорівнює 5, а загальна кількість унікальних параметрів загроз дорівнює 7. Представимо матрицю співвідношення загроз та їх параметрів у таблиці 2.1.

У разі необхідності визначення загрози Y, що належить розглянутій множині, необхідно звернутися до одного з процесів ІБ для визначення випадково вибраного параметра α_n. Загальна ентропія для цього випадку буде обчислюватися як повна сума ентропій за кожною загрозою:

$H(\text{Заг})=H(Y_1)+H(Y_2)+H(Y_3)+H(Y_4)+H(Y_5)+H(Y_6)+H(Y_7)$.

Таблиця 2.1 - Матриця співвідношення загроз та їх параметрів для розглянутого прикладу

	α_1	α_2	α_3	α_4	α_5	α_6	α_7
Y_1	1	0	0	1	0	0	1
Y_2	0	1	0	0	0	0	1
Y_3	0	0	1	0	0	1	0
Y_4	0	0	0	1	0	0	0
Y_5	0	1	0	0	1	0	0

Нехай першому кроці визначається параметр α_4=1. Виходячи з таблиці 2.1, очевидно, що лише загрози Y_1 та Y_4 задовольняють отриманому значенню параметра, а отже загрози, що залишилися, виключаються. Таким чином отримана ентропія знижується і буде обчислюватися так:

$$H(1)=H(Y1)+H(Y2)+H(Y3)+H(Y4)+H(Y5)+H(Y6)+H(Y7)-H(Y2)-H(Y3)-H(Y5)=$$
$$=H(Y1)+H(Y4).$$

Очевидно, що $H(\text{Заг})>H(1)$. На другому і наступному кроках потрібно вибирати новий параметр загрози доти, поки не залишиться єдино можливої загрози Y, яка і буде шуканою. Слід звернути увагу на те, що в даному випадку немає обмежень в ресурсних і часових рамках, таким чином можна знизити невизначеність вибору нанівець. Однак у загальному випадку, через обмеженість у часі та ресурсах однозначне визначення загрози може бути неможливим. Таким чином невизначеність вибору буде зменшена, але все ще збережеться. В даному випадку розглянутий приклад, у якому враховується лише наявність параметра α, а чи не його реальне значення, тепер перейдемо до розгляду ситуації, що склалася в аналізованій організації.

Нехай за кожен із процесів ІБ, що протікають у СЗІ організації, відповідає окремо взятий фахівець чи експерт. Припустимо, що кожен з експертів, ґрунтуючись на власній логіці та професійному досвіді здатний заповнити таблицю співвідношення загроз та їх параметрів у частині, що

його стосується. Таким чином, отримається повна таблиця 2.2 апріорних ймовірностей виникнення загрози, заснованої на сукупній експертній думці.

Таблиця 2.2 – Співвідношення загроз та їх параметрів, заснована на експертних оцінках

	α_1	α_2	α_3	α_4	α_5	α_6	α_7	...	α_n
Y_1	0,04	0	0,06	0,1	0,04	0,06	0,04	…	0
Y_2	0	0,06	0	0,04	0,6	0	0	…	0,35
Y_3	0,6	0,1	0,04	0	0	0,1	0,04	…	0
...	…	…	…	…	…	…	…	…	…
Y_5	0,04	0	0,1	0,06	0	0,04	0,1	…	0,6

Оскільки число параметрів, що визначають загрозу, суворо визначено, а їх сукупність дає повний опис загрози, то повну суму всіх параметрів, що описують конкретну загрозу, можна отримати рівною 1. Нехай після n ітерацій визначення параметрів α загальна ентропія зменшилася і відсікла частина загроз $Y_{\text{від}}$ через явну невідповідність передбачуваних параметрів апостеріорним значенням, але не звелася до 1. Тоді загальні показники апріорної невизначеності знизилися і стали дорівнювати апостеріорній ентропії. Отримана апостеріорна ентропія менша апріорної, тобто область можливих рішень зменшилася відповідно до їх різниці і дорівнює кількості отриманої інформації від процесів ІБ. З урахуванням наявних умов, кількість ітерацій вибору обмежена часовими та ресурсними рамками. Грунтуючись на зібраній інформації за відведений час, отримуємо необхідність прийняття рішення з урахуванням невизначеності, що змінилася, коли шукана загроза $Y(\alpha_1, \alpha_2, \ldots, \alpha_n) \in (Y\text{заг} - Y\text{від})$. Це завдання можна подати у вигляді скінченого дерева вибору, представленого на рисунку 2.1. При цьому кожна скінчена гілка, одержана в результаті перебору, однозначно описуватиме загрозу, а, отже, і стан СЗІ, у якому вона здатна їй протистояти. Таким чином,

вирішення даного завдання спричинить зниження невизначеності вибору та прийняття відповідного керуючого впливу на усунення виниклої загрози з урахуванням наявних вимог та обмежень, включаючи умови використання часу та ресурсів, які відводяться на прийняття управлінського рішення.

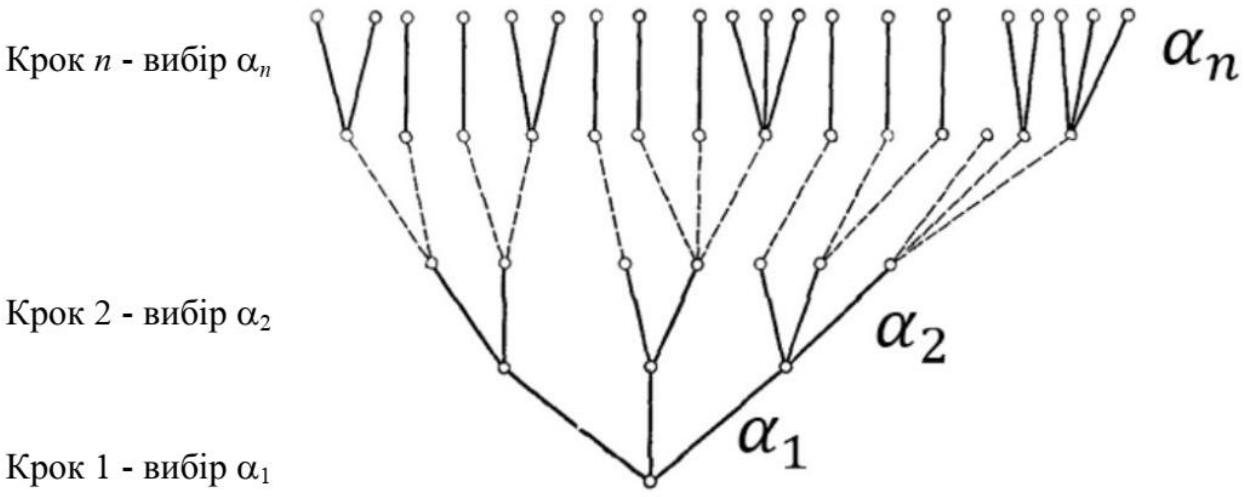

Рисунок 2.1 – Дерево вибору загрози, що шукається, за визначеними параметрами

З точки зору теорії управління, рішення, яке потрібно ухвалити, буде описуватися параметрами *F* – сукупним обсягом інформації, необхідним для прийняття рішення, *T* - час, необхідний для прийняття рішення та обробки інформації, R – склад ресурсів на виконання завдання, а також аналітичними алгоритмами, що використовуються для обробки інформації та прийняття рішення. З урахуванням наявних умов та приймаючи до уваги рівноправність процесів у аналізованій системі, можна отримати:

$$\sum_{i=1}^{n} r_i = R = const .$$

Таким чином, керівництву розглянутої організації потрібно зібрати таку кількість інформації *f* від діючих процесів управління ІБ, щоб перевести СЗІ до стану, при якому вона здатна протистояти загрозі *Y*, використовуючи наявні ресурси та обмежуючись максимальним часом, відведеним для

прийняття рішення. Сформулюємо отримане завдання у математичному вигляді:

$$\begin{cases} \sum_{i=1}^{n} f_i(x_i) \to \max(x_1, x_2, ..., x_n), x_i \in Z_+^n \\ \sum_{i=1}^{n} t_i(r) x_i \le t_{\max} \end{cases} \quad (2.1)$$

Розглянемо загальний алгоритм дій при настанні цієї ситуації. Після визначення формальних умов здійснення завдання при розрахунку мінімально необхідного часу отримання інформації від процесів ІБ для вирішення задачі можливі ситуації, коли:

1) мінімальний час отримання інформації min(t) не дозволяє отримати достатню кількість інформації $f_i(x_i)$:

$$\max \sum_{i=1}^{n} f_i(x_i) < F ;$$

2) мінімальний час отримання інформації min(t) може дозволити отримати достатню кількість інформації $f_i(x_i)$:

$$\max \sum_{i=1}^{n} f_i(x_i) \le F ;$$

3) мінімальний час отримання інформації min(t) дозволяє отримати достатню кількість інформації $f_i(x_i)$:

$$\max \sum_{i=1}^{n} f_i(x_i) = F ;$$

4) мінімальний час отримання інформації min(t) дозволяє отримати достатню або надмірну кількість інформації $f_i(x_i)$:

$$\max \sum_{i=1}^{n} f_i(x_i) \ge F .$$

Для ситуації 1 необхідно визначити існування такого часу t, для якого б виконувалася умова $\sum_{i=1}^{n} f_i(x_i) = F$. Якщо таке t існує, то завдання може вирішуватись далі, відповідно до представленого на рисунку 2.2 алгоритму. В іншому випадку задача не може бути повністю вирішена, і сенс розв'язання задачі буде зводитись до знаходження максимально наближеної кількості інформації $f \rightarrow F$ при $t=t_{max}$.

Для ситуації 2 необхідно визначити, чи існує такий час t, при якому дотримуються необхідні умови для отриання необхідної кількості інформації F. Якщо таке t існує, то задача може вирішуватися далі, інакше задача не може бути повністю вирішена, і сенс її розв'язання зводиться до знаходження максимально наближеної кількості інформації $f \rightarrow F$ при $t=t_{max}$.

Для ситуацій 3, 4 існує такий час $\min(t)$, при якому дотримуються необхідні умови для досягнення необхідної кількості інформації F. У такому разі в свою силу вступає обмеження t_{max}, якщо $\min(t) \leq t_{max}$, то задача має підсумкове рішення з урахуванням виконання всіх умов (це справедливо і для позитивного сценарію ситуації 2, в іншому випадку розв'язання задачі зводиться до знаходження максимально наближеної кількості інформації $f \rightarrow F$ при $t=t_{max}$ для подальшого ухвалення рішення.

Розглянемо розв'язання цієї задачі для найбільш складної ситуації 2. Загальний вигляд даної ситуації може бути представлений як (1), позначимо наш окремий випадок n, $f \leq t_{max}$ і помістимо його в загальне сімейство подібних завдань $\{i, f \leq K, i=1, \ldots, n, 0 \leq K \leq t_{max}\}$.

Нехай $S_i(K)$ – оптимальне значення цільової функції задачі i, $f \leq K$, тоді справедливі наступні рекурентні співвідношення:

$S_1(K) = \max f_1(x_1)$, $0 \leq K \leq t_{max}$, $x_1=0, 1, \ldots, [K/t_1]$;

$S_i(K)=\max\{S_{i-1}(K-t_i x_1)+f_i(x_i)\}$, $i=2, 3, \ldots, n$, $0 \leq K \leq t_{max}$, $x_i=0, 1, \ldots, [K/t_i]$;

Рисунок 2.2 – Загальний алгоритм розв'язання задачі

Тоді в результаті прямого ходу значень $S_i(K)$, K=0, 1, …, t_{max}, необхідно відновити оптимальний вектор x, що відображає хід виконання процесу для досягнення результату. Нехай спочатку x=0, K=0, потім послідовно виконаємо кроки на кожному з яких знайдемо такий індекс i, при якому виконувалася б рівність $S_i(K)=S(K-t_i)+f_i$, $t_i \le K$. Нехай $x_i=x_i+1$; $K=K-t_i$ і

повторимо крок до тих пір, поки не стане допустимих індексів i. Підсумковий вектор x буде оптимальним, а значить і рішенням нашої задачі. Вирішення ситуацій 1, 3 та 4 практично співпадатиме.

Виходячи з умов задачі, а також представленого рішення, можна судити про те, що для ситуації 1 реалізована СЗІ, а також механізми управління нею, недостатні. Поєднання використовуваних процесів неефективне і не може виконувати поставлені перед нею завдання у повному обсязі. Для негативного сценарію ситуації 2 стан справ схожий, однак у випадку реалізації позитивного сценарію, підсумкова мета може бути досягнута. Крім неефективності реалізації та управління СЗІ, може постати питання про недостатність ресурсів на їх реалізацію або неможливість вкластися у строки у зв'язку з використання неоптимальних алгоритмів обробки даних.

Розглянемо алгоритм дій при настанні цієї ситуації з урахуванням того, що кількість процесів i та одержувана в них інформація $f_i(x_i)$ достатня для вирішення задачі при дотриманні умови $T(R)=\leq t_{max}$. Ця ситуація є ідеальною і свідчить про те, що всі процеси, що беруть участь у забезпеченні ІБ аналізованої організації, коректно виконують свої функції, а їх склад відповідає цілям реалізації СЗІ. При цьому ресурсів, виділених для виконання цих процесів, достатньо. Умова дотримання $f_i(x_i)=F$, при $T(r)=T(R)=\leq t_{max}$ свідчить про правильність побудови процесу управління ІБ. Блок-схема алгоритму дій представлена на рисунку 2.3.

У цьому випадку після визначення мінімально необхідного часу для збору та обробки даних для прийняття рішення $\min(t)$ необхідно переконатися в тому, що час повного виконання завдання, яке задовольняє всім умовам, менший від максимального заданого часового відрізку на виконання задачі t_{max}. Якщо ця умова виконується, то отримується вирішена задача, інакше вирішення даної задачі не може бути знайдено за відведений час. У такому разі потрібно запропонувати найбільш ефективне вирішення існуючої проблеми $\max(f)$ з врахуванням наявних ресурсів r та запасу часу

t_{max}. Як видно з блок-схеми, навіть для цього ідеального випадку може мати місце факт невідповідності термінів вирішення задачі максимальному часовому коридору, відведеному на її виконання.

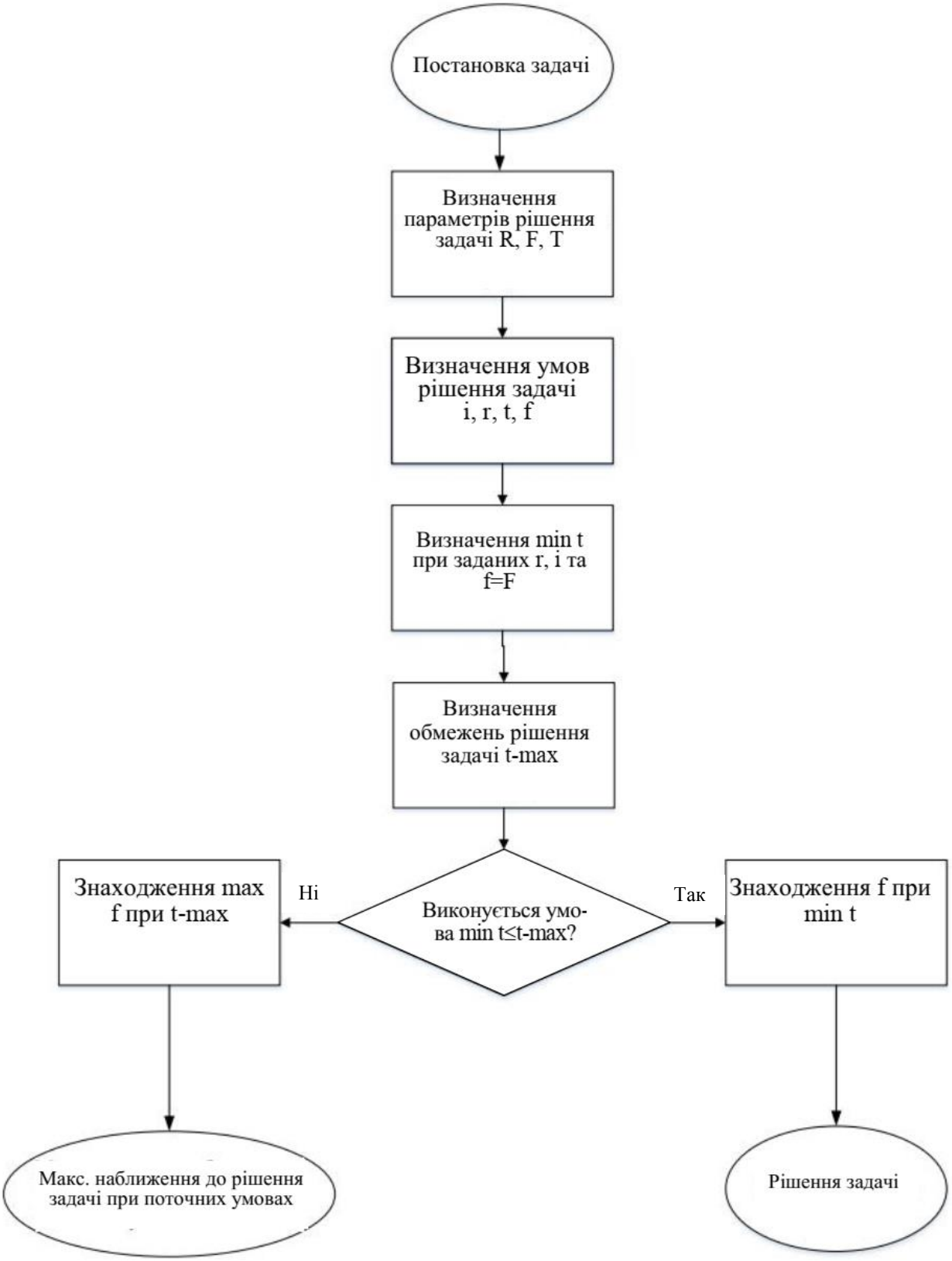

Рисунок 2.3 – Блок-схема алгоритму дії

З урахуванням відсутності можливості впливу на дані часові рамки залишається лише три шляхи для усунення цієї проблеми:

1) збільшувати кількість ресурсів, що виділяються на вирішення проблеми;

2) оптимізувати використання виділених ресурсів за рахунок застосування ефективних методів управління ІБ;

3) скорочувати час, необхідний для отримання необхідної кількості інформації.

Таким чином, вирішення даної проблеми можливе за рахунок розробки методу та моделі управління ІБ, заснованих на застосуванні сучасних засобів автоматизації діяльності та логічних алгоритмів, зафіксованих у вигляді узагальненого набору динамічних правил експертної системи підтримки прийняття рішень, здатних суттєво скоротити час на збирання, систематизацію та обробку інформації, необхідної для прийняття відповідного управлінського рішення.

2.3 Управління ризиками та загрозами інформаційної безпеки

Грунтуючись на багаточисельних опитуваннях експертів в області інформаційної безпеки було встановлено, що кожний з параметрів загроз інформаційної безпеки являється пов’язаним з іншими, дані зв’язки представлені на рисунку 2.4.

Таким чином, незалежно від обраної методики оцінки ризиків та визначення загроз інформаційній безпеці, у процесі управління ризиками та загрозами інформаційної безпеки можлива побудова спільного дерева ризиків-загроз для конкретно обраного активу, що дає повну картину, необхідну для їхнього аналізу. Приклад цього дерева представлений рисунку 2.5.

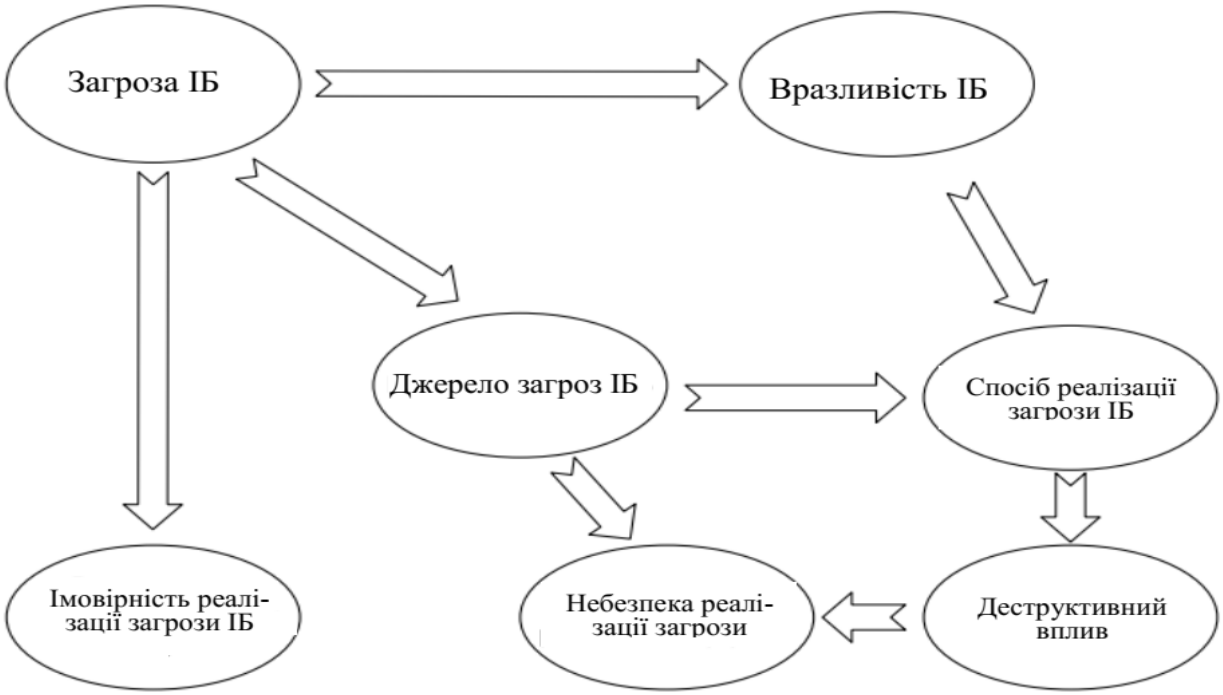

Рисунок 2.4 – Зв’язок параметрів загроз інформаційній безпеці

Залежно від важливості активу, ймовірності реалізації загрози та джерела загрози, гілки дерева будуть змінюватися для кожної конкретної загрози, виходячи з типу активу та моделі порушника (як одного з основних джерел загроз). На актуальність загрози впливатимуть у загальному випадку ймовірність реалізації загрози та ступінь її небезпеки, а у разі ризикового підходу до уваги братимуться і можливі наслідки деструктивного впливу, наданого на аналізований актив.

Як видно з рисунка 2.5, при використанні такого підходу до процесу управління ризиками та загрозами інформаційної безпеки, чим детальніше обрана методика описує загрози інформаційної безпеки та чим вища компетенція аналітика з інформаційної безпеки, що здійснює визначення актуальності загроз та величини ризиків, тим більшою буде кількість гілок дерева.

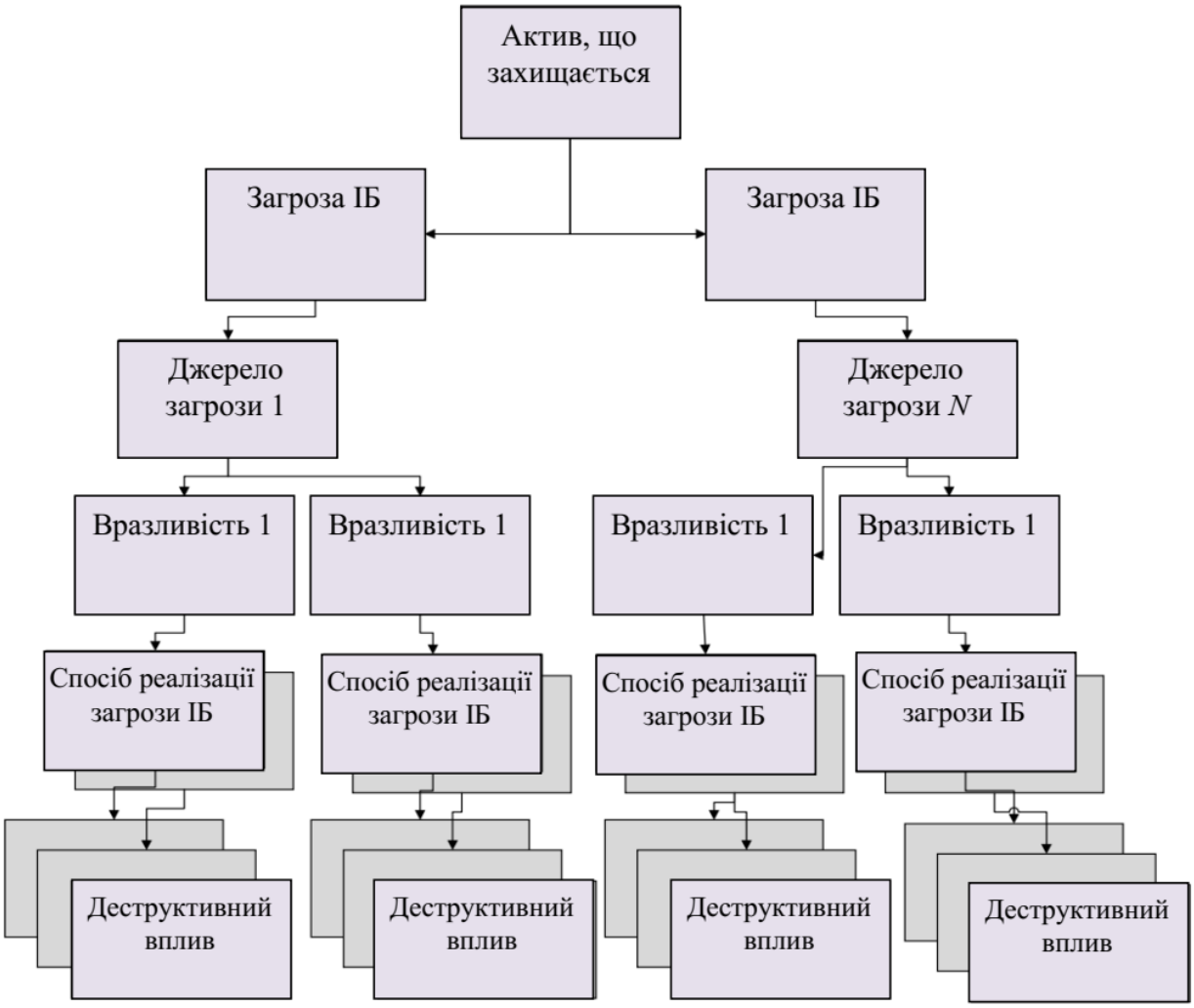

Рисунок 2.5 – Приклад побудови загального дерева загроз для активу, що захищається

Одним із ключових завдань при управлінні ризиками та загрозами інформаційної безпеки є контроль та облік заходів щодо забезпечення захисту активу. У багатьох термінологіях дані заходи, при розгляді їх у прив'язці до загроз, називаються контрзаходами. Залежно від загрози набір контрзаходів, що перекривають цю загрозу, може суттєво змінюватись. Залежно від контрзаходів та їх параметрів аналітики в галузі інформаційної безпеки можуть судити про ймовірність реалізації тієї чи іншої загрози, значення якої є ключовим як при побудові моделі загроз, так і при розрахунку ризиків Загалом такий розрахунок проводиться на основі

сукупної думки експертів за допомогою використання методу експертної оцінки. Цей підхід має ряд істотних недоліків, а саме:

− суб'єктивна оцінка заснована на особистому досвіді експерта;

− розрізненість параметрів, які використовуються експертами;

− рутинність перебігу процесу;

− тривалість періоду проведення оцінки;

− сумнівність отриманих результатів з урахуванням людського фактора;

− трудомісткість процесу;

− відсутність можливості подальшого використання та актуалізації зібраної інформації.

Таким чином, найчастіше зустрічається підхід, що використовується в методиках оцінки ризиків та визначення актуальності загроз інформаційній безпеці (методом експертної оцінки) має ряд суттєвих проблем та незручностей для використання. Рішенням даних проблем може бути розробка нового методу оцінки можливості реалізації та небезпеки загроз з використанням засобів автоматизації на основі динамічних експертних систем підтримки ухвалення рішень. У запропонованому методі формалізовано основні ознаки, що впливають на визначення можливості реалізації та небезпеки загроз інформаційної безпеки, отримані в результаті проведення інженерії знань та відповідного опитування експертів у галузі інформаційної безпеки

3 АЛГОРИТМИ ТА МОДЕЛІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

3.1 Модель даних процесу управління ризиками та загрозами інформаційної безпеки

Процес управління ризиками та загрозами інформаційної безпеки в організації є основним елементом під час управління інформаційною безпекою. На основі результатів його роботи формується колосальна кількість керуючих впливів, як при створенні системи захисту інформації, так і на наступних етапах її існування. В основу цього процесу закладається два базові механізми, що діють в організації: це механізм прорахунку ризиків та механізм обробки ризиків, залежно від яких і будуватимуться основні дії із системою захисту інформації.

У рамках виконання цього процесу в організації повинні бути визначені на підставі чинних внутрішніх та зовнішніх нормативно-правових документів такі складові елементи:

− склад аналізованих загроз інформаційній безпеці;

− передбачувані об'єкти впливу в організації;

− найбільш ймовірні джерела загроз;

− характер впливу на об'єкти захисту.

З урахуванням обраних організацією механізмів прорахунків ризиків мають бути визначені:

− небезпека загрози;

− ймовірність реалізації загрози;

− уразливості, що використовуються при реалізації загрози;

− способи реалізації загрози;

− можливі деструктивні дії;

− ризики та їх характеристики.

А з урахуванням прийнятих в організації методик обробки ризиків мають бути сформовані відповідні коригувальні та запобіжні впливи. На

завершальних стадіях роботи процесу формується ряд критично важливої інформації, яка безпосередньо впливає на ефективність системи захисту інформації, повноту реалізації заходів щодо захисту інформації, коректність та правила функціонування засобів захисту інформації. Виконання цього процесу є одним з найбільш складних і ресурсоємних дій при забезпеченні інформаційної безпеки, проте даний процес може бути суттєво полегшений у разі використання засобів автоматизації діяльності персоналу або засобів управління інформаційною безпекою, реалізованих відповідно до вимог запропонованого методу управління інформаційною безпекою на основі динамічних експертних систем підтримки ухвалення рішень. Інформація, що обробляється та формується в рамках виконання даного процесу, передається для подальшої обробки у суміжних процесах управління інформаційною безпекою і матиме ключове значення при визначенні параметрів керуючих, корегувальних та попереджувальних впливів в організації. З точки зору методу управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень цей процес буде одним із складових частин у межах функціональної групи процесів, які стосуються «Вирішувача». Загальна схема моделі взаємодії даних процесу управління ризиками та загрозами інформаційної безпеки в рамках реалізації методу управління інформаційною безпекою на основі динамічних експертних систем прийняття рішень представлена на рисунку 3.1.

3.2 Модель даних процесу управління аудитом інформаційної безпеки

Процес управління аудитом інформаційної безпеки в організації є складовим елементом управління інформаційною безпекою та забезпечує повноту виконання вимог, правильність та коректність реалізації заходів щодо захисту інформації, а також повноту, правильність та коректність налаштувань засобів захисту інформації.

Рисунок 3.1 – Схема моделі взаємодії даних процесу управління ризиками та загрозами інформаційної безпеки

Цей процес має відбуватися відповідно до прийнятих в організації методик проведення аудиту, а також з урахуванням вимог зовнішньої та внутрішньої документації з питань інформаційної безпеки. У рамках цієї документації повинні бути визначені терміни, відповідальні та критерії для проведення аудиту.

Відповідно до чинних методик проведення аудиту, при виконанні даного процесу мають бути сформульовані:

− умови проведення аудиту;

− порядок проведення аудиту;

− склад аудиторської групи;

− нормативна база аудиту;

− мета проведення аудиту;

− склад та критерії залучення сторонніх технічних експертів;

− об'єкти аудиту;

− листи аудиту, включаючи доказову базу, опитувальні листи та ін.

В результаті виконання цього процесу мають бути сформовані підсумкові результати аудиту, залежно від складу яких протікатиме подальша обробка та ухвалення управлінських рішень. Інформація, що обробляється та формується в рамках виконання даного процесу, передається для подальшої обробки у суміжних процесах управління інформаційною безпекою та матиме ключове значення при визначенні параметрів керуючих, корегувальних та попереджувальних впливів в організації.

Цей процес є одним із трьох ключових процесів у рамках методу управління інформаційної безпеки. Слід звернути особливу увагу на той факт, що зважений комплексний підхід до проведення аудиту може бути заснований на ризик-орієнтованому підході, що дозволить суттєво збільшити ефективність процесу управління ризиками та загрозами інформаційної безпеки, а також підвищити ефективність системи захисту інформації в цілому, що безпосередньо буде показано в рамках процесу аналізу ефективності системи захисту інформації, включаючи можливість документального підтвердження фактів відповідності вимогам щодо інформаційної безпеки.

З погляду методу управління інформаційною безпекою на основі динамічних експертних систем для підтримки прийняття рішень цей процес буде однією із складових частин у рамках функціональної групи процесів, які стосуються «Вирішувача».

Загальна схема моделі взаємодії даних процесу для управління аудитом інформаційної безпеки у рамках реалізації методу управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень представлені на рисунку 3.2.

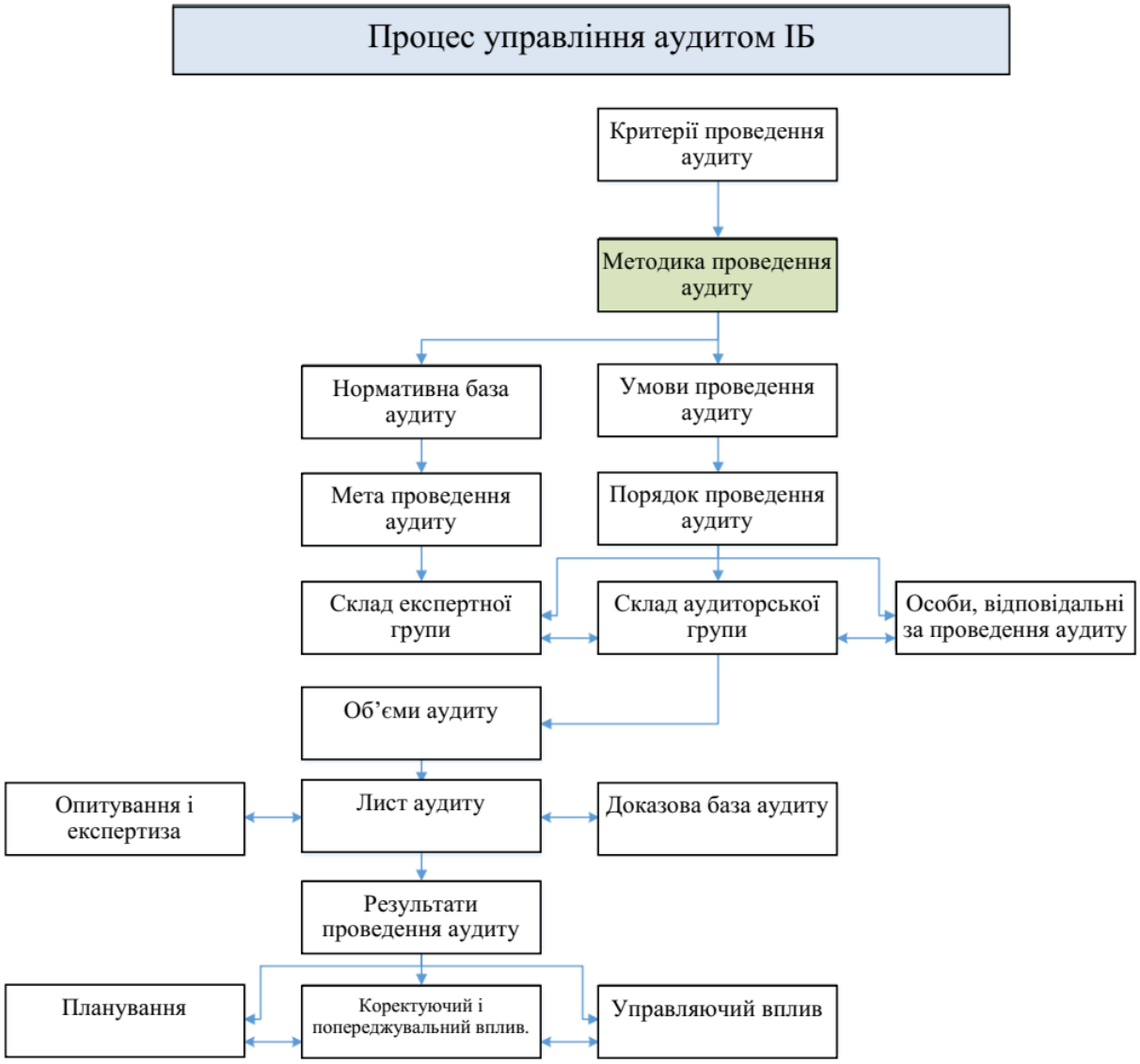

Рисунок 3.2 – Схема моделі взаємодії даних процесу управління аудиту інформаційної безпеки

3.3 Модель даних процесу управління аналізом ефективності систем захисту інформації

Процес управління аналізом ефективності системи захисту інформації є однією з складових з елементів управління інформаційною безпекою в організації та відповідає за надання аналітичних викладок, що показують поточний рівень інформаційної безпеки організації щодо введених у ній еталонних значень, які формуються за результатами застосування прийнятої в організації методики проведення аналізу ефективності.

У рамках реалізації цього процесу згідно з діючою в організації методикою проведення аналізу ефективності мають бути однозначно визначені:

− документальна база;

− математична основа проведення аналізу ефективності;

− критерії оцінки ефективності;

− відповідальні особи за проведення аналізу;

− шкали виставлення кількісних та якісних оцінок ефективності системи захисту інформації;

− критерії оцінки повноти, достатності та адекватності застосовуваних механізмів та заходів захисту інформації;

− порядок проведення тестування з інформаційної безпеки.

В результаті виконання цього процесу мають бути сформовані підсумкові показники ефективності, які відображають реальну картину стану системи захисту інформації, що діє в організації і підкріплюються даними зі сполучених процесів управління та забезпечення інформаційної безпеки. Такий підхід буде найбільш ефективним для великих організацій, у рамках системи захисту інформації яких повноцінно реалізовані всі описані процеси, при цьому відсутність одного чи ряду процесів може суттєво позначитися на достовірності отримуваних результатів аналізу ефективності. Відсутність одного з процесів вплине на підсумкові показники ефективності. Інформація, що обробляється та формується в рамках виконання даного процесу, передається для подальшої обробки у суміжних процесах управління інформаційною безпекою і матиме ключове значення щодо параметрів керуючих, корегувальних та попереджувальних впливів в організації. З точки зору методу управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень цей процес буде одним із складових частин у межах функціональної групи процесів, які стосуються «Вирішувача». Загальна схема моделі взаємодії даних процесу управління аналізом ефективності систем захисту інформації в рамках реалізації методу

управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень подано на рисунку 3.3.

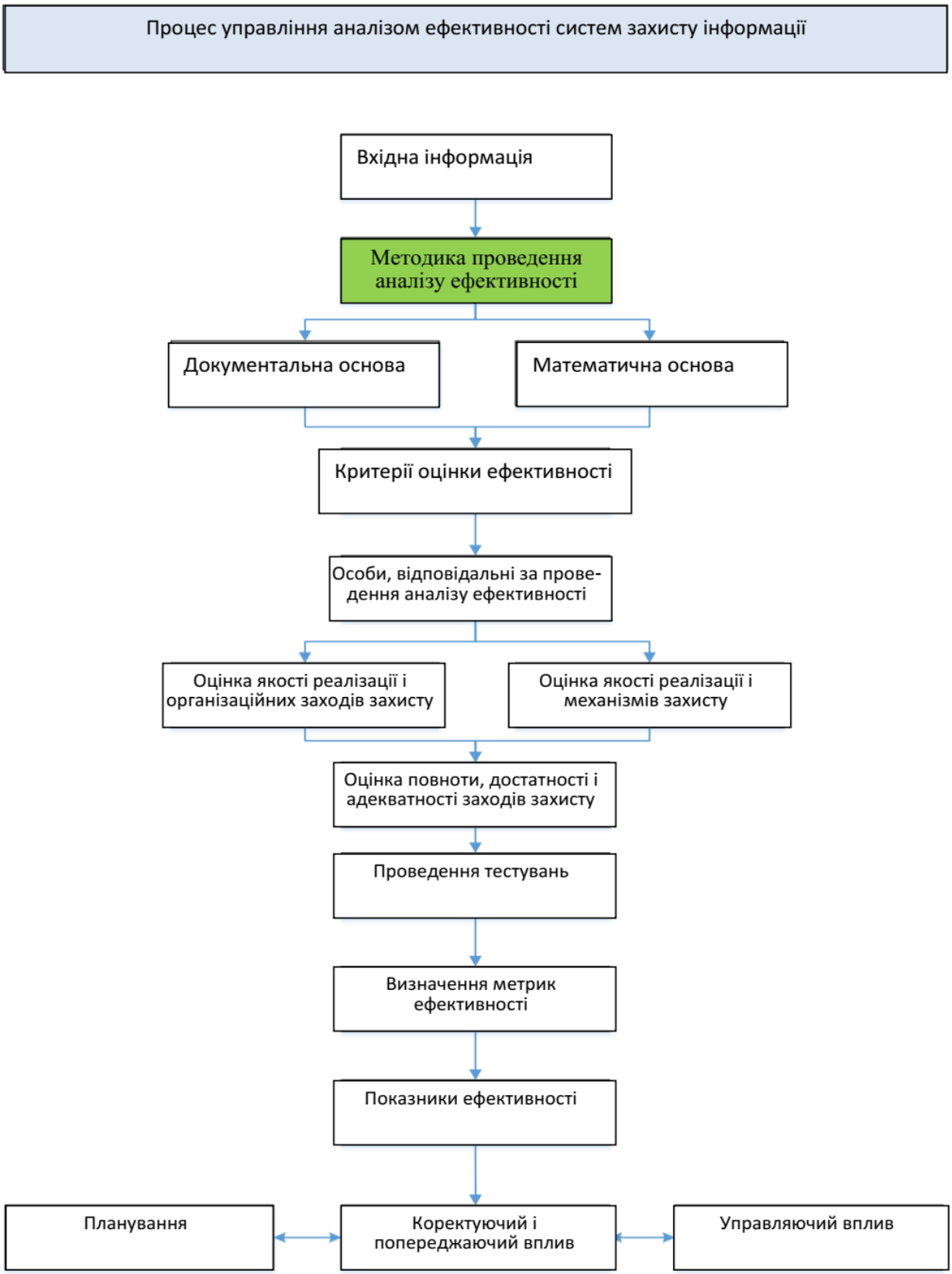

Рисунок 3.3 – Схема моделі взаємодії даних процесу управління аналізом ефективності системи захисту інформації

3.4 Комплексна модель управління взаємодією даних у системі забезпечення ІБ на основі процесного підходу

Розглянувши кожен із процесів, що входить до складу запропонованого методу управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень окремо та показавши їх внутрішній взаємозв'язок один з одним у рамках чинної в організації системи захисту інформації, слід показати комплексну модель управління взаємодією даних у системі забезпечення ІБ на основі процесного підходу. Першорядне значення у комплексній моделі матимуть:

− вимоги зовнішніх та внутрішніх нормативно-правових документів щодо інформаційної безпеки та захисту інформації;

− система захисту інформації, включаючи всі наявні в ній дані;

− експертна група фахівців, які забезпечують інформаційну безпеку в організації.

Вимоги зовнішніх та внутрішніх нормативно-правових документів щодо інформаційної безпеки та захисту інформації є складовою процесу формування та актуалізації інформаційно-довідкової системи організації з питань інформаційної безпеки. Експертна група фахівців, які забезпечують інформаційну безпеку в організації, може бути віднесена як до процесу управління інформаційною безпекою при роботі з персоналом, так і до процесу управління інформаційною безпекою при інформаційному обміні та співпраці з третіми сторонами в залежності від того, яким чином ця група була сформована. Проте в даному випадку це не має особливого значення, адже найчастіше системи управління інформаційної безпеки в організації відсутні як клас, роблячи неспроможною частину процесів забезпечення інформаційної безпеки в організації. При цьому у разі залучення сторонніх фахівців з інформаційної безпеки на етапі розподілу зібраних вихідних даних процес управління інформаційною безпекою при інформаційному обміні та співпраці з третіми сторонами повинен бути запущений раніше за інших.

Виходячи з вимог внутрішніх та зовнішніх нормативно-правових документів щодо інформаційної безпеки та захисту інформації, група експертів витягує вихідні дані щодо системи захисту інформації та об'єктів захисту, а також формує повний перелік відсутніх даних. Після збору всіх необхідних даних має відбуватися первинна логічна систематизація за такими процесами управління інформаційною безпекою:

− процес управління активами, що захищаються;

− процес управління ресурсами системи захисту інформації;

− процес управління інформаційною безпекою при роботі з персоналом;

− процес управління інформаційною безпекою при інформаційному обміні та співробітництві з третіми сторонами.

Після чого відбувається розподіл та формалізація інформації щодо основних структурних одиниць з інформаційної безпеки в організації, автоматизованих або інформаційних системах, а також систематизація даних по допоміжних процесах, що дозволяють проводити своєчасну зміну та актуалізацію інформації щодо поточного стану системи захисту інформації в цілому та протікаючими у ній процесами зокрема, а саме:

− процес управління інформаційною безпекою при здійсненні життєвого циклу інформаційних систем;

− процес управління забезпеченням безперервності функціонування автоматизованих та інформаційних систем;

− процес управління доступом до інформаційних активів, що захищаються, та інформаційних систем;

− процес управління інцидентами інформаційної безпеки.

Наступним логічним елементом у моделі буде розподіл інформації та систематизація вимог щодо проведення аналітичних робіт із системою захисту інформації, за яку в рамках цього методу управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень відповідають такі процеси:

− процес управління ризиками та загрозами інформаційної безпеки;

− процес управління аудитом інформаційної безпеки;

− процес управління аналізом ефективності систем захисту інформації.

Після чого вся інформація, задіяна у вище перерахованих процесах, передається для обробки у процес управління завданнями щодо забезпечення інформаційної безпеки, ґрунтуючись на правилах, що визначаються експертною групою. Даний процес розподіляє її за трьома основними складовими:

− за складовою планування, що відповідає за внесення змін та коригування у внутрішні нормативно-правові документи щодо забезпечення інформаційної безпеки в організації, а також за процеси планування робіт із захисту інформації, що відноситься до стратегічного управління інформаційною безпекою;

− за складовою керуючого впливу, що відповідає за проведення поточних робіт та реалізації критично важливих в даний момент дій та заходів із захисту інформації, що належать до оперативного управління інформаційною безпекою.

На заключних етапах вся інформація повертається за механізмами зворотного зв'язку або безпосередньо до процесів, що потребують втручання, або опосередковано через зміни вимог у внутрішніх нормативно-правових документах чи систему захисту інформації в цілому, замикаючи таким чином цикл і повторюючи його знову, свідчивши про яскраво виражений процесний характер управління інформаційною безпекою Комплексна модель управління взаємодією даних у системі забезпечення ІБ на основі процесного підходу представлена рисунку 3.4. Для простоти розуміння та відображення, а також з метою підвищення читабельності рисунка, повні назви процесів під час управління інформаційною безпекою були змінені на скорочені, що мають схоже або однакове смислове значення у межах запропонованого методу.

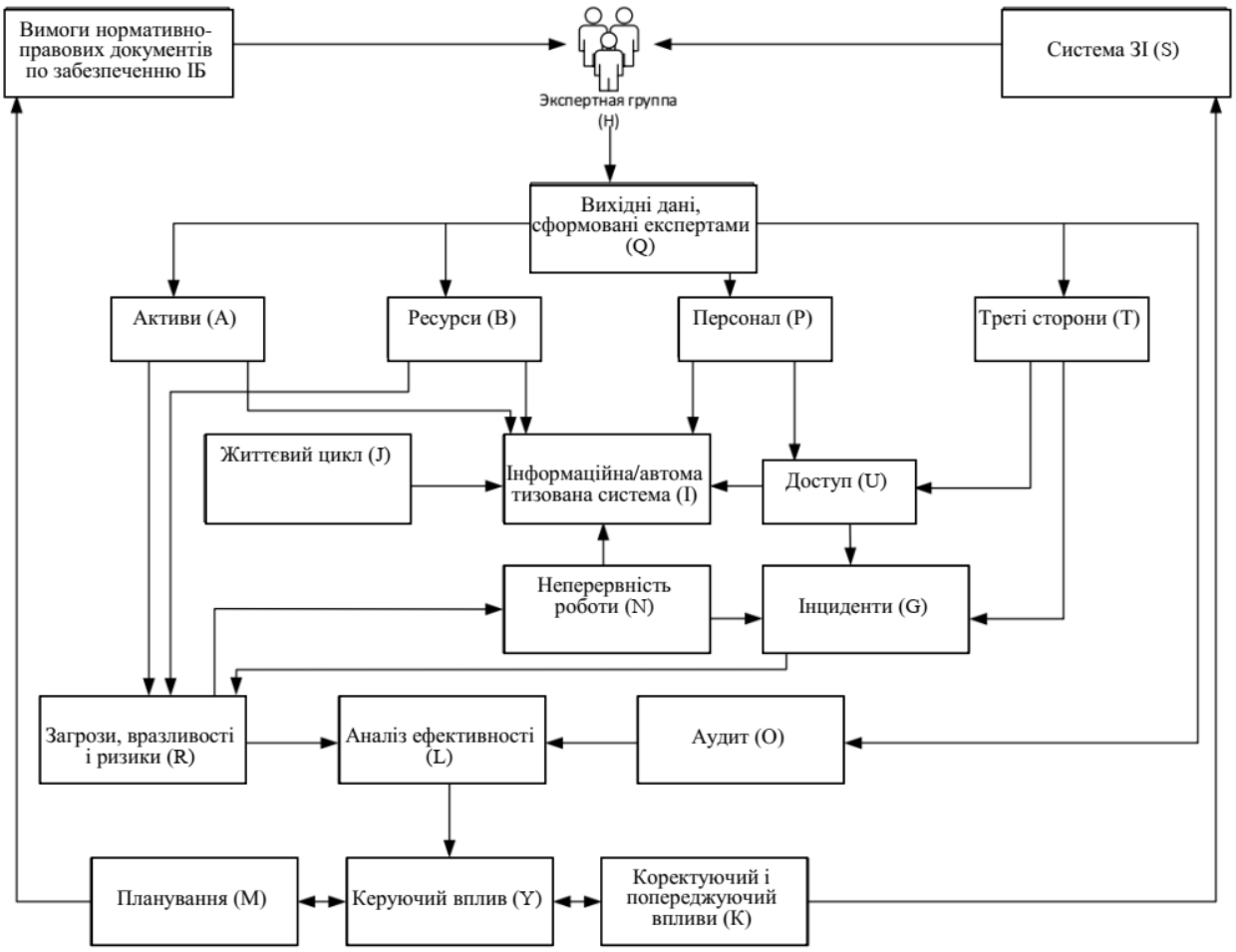

Рисунок 3.4 - Комплексна модель управління взаємодією даних в системі забезпечення ІБ на основі процесного підходу

Виходячи з концептуальних принципів методу управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень, модель взаємодії даних має яскраво виражену процесно-орієнтовану спрямованість, складові елементи якої можуть бути використані в рамках окремо взятого механізму управління кінцевими процесами забезпечення інформаційної безпеки в організаціях різної величини та роду діяльності.

Таким чином, згідно даної моделі всі дані, необхідні для забезпечення та управління інформаційною безпекою, виявлені в рамках опису процесних складових, розподіляться за групами, що забезпечують свою функціональну роль в рамках застосування методу, після чого пройдуть обов'язкову

систематизацію та розподіляться по чотирьом основним інформативним блокам (Активи, Ресурси, Персонал, Треті сторони). Після цього відбувається логічне групування систематизованих даних у рамках найбільш оптимального уявлення по складових частинах організації – інформаційним або автоматизованим системам. Після сортування інформації щодо складових частин організації відбувається формалізація основних процесів забезпечення інформаційної безпеки в рамках застосовності до даних складових частин (Загрози, Вразливості та ризики, Аналіз ефективності, аудит). На основі проведеного аналізу формуються три основні вихідні сигнали з управління інформаційною безпекою в організації (Планування, Керуючі впливи, Коригувальні та попереджувальні впливи), дані про які повертаються каналами зворотного зв'язку до системи захисту інформації та нормативно-правових вимог, закріплених у зовнішній та внутрішній документації організації, після чого процес відбувається знову.

Таким чином дотримується підхід до захисту інформації як до безперервного процесу, спрямованого на забезпечення інформаційної безпеки, при цьому низка процесів спрямована на забезпечення актуалізації та збору нових даних по складових частинах організації (Життєвий цикл, Безперервність роботи) та забезпечення відповідного контролю за дотриманням загальних вимог до забезпечуючих процесів (Доступ, Інциденти).

Формалізацію даної моделі Z можна подати у вигляді взаємодіючих процесів управління ІБ G_i, i=1, …, n, при цьому згідно пропонованого методу, Z: <G_1, G_2, … G_n>. Кожна з множин має сукупний обсяг вхідної інформації e_i, необхідної для його виконання, та зведенням встановлених правил внутрішньої взаємодії інформаційних потоків g_i. Результатом виконання кожного із i процесів є інформація f_i=e_i(g_i). Залежно від належності процесу до функціональних груп, f_i може входити до складу вхідної інформації для суміжних процесів управління ІБ, при цьому

сукупність інформації всієї моделі $f_Z=F$ буде описувати відповідне управлінське рішення.

Виходячи з розглянутого випадку, шукана величина *F*, необхідна для ухвалення відповідного управлінського рішення, буде описуватися в даній моделі як inf *Z=F*. Відповідно до розробленого методу управління ІБ, кожна з функціональних груп процесів визначатиме загальну кількість інформації, яка описує поточний і можливий стан СЗІ, ґрунтуючись на інформації від суміжних процесів.

3.5 Оцінка ефективності системи захисту інформації із застосуванням розробленого методу та моделі управління інформаційної безпеки

У рамках розробки будь-якого науково обґрунтованого методу виникає потреба оцінки його ефективності та доцільності його застосування в реальних умовах. Метод і модель управління інформаційною безпекою не є винятком, однак у нашому випадки при відсутності аналогів, що описують підхід до управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень, ряд методів оцінки ефективності не може бути застосований. Для проведення оцінки ефективності розроблених методу та моделі управління необхідно порівняти ефективність СЗІ із застосуванням положень цих методів і моделі управління та СЗІ без застосування таких. Під час проведення цього порівняння необхідно визначити основні чинники, що впливають ефективність СЗІ. Ці фактори повинні бути досить важливими і істотно впливати на якість і ефективність керування інформаційною безпекою. Порівняння необхідно проводити з допомогою математичного розрахунку, використовуючи адитивний метод. Адитивний метод розрахунку ваги СЗІ з використанням методу та моделі управління ІБ на основі динамічних експертних систем підтримки прийняття рішень складатиметься із виваженої суми часткових факторів (критеріїв). Коефіцієнт ефективності СЗІ, яким вона буде володіти

при використанні методу та моделі управління ІБ на основі динамічних експертних систем підтримки прийняття рішень, матиме вигляд:

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

де S_1 – вихідні метод і модель управління ІБ;

S_2 – розроблені метод і модель управління ІБ на основі динамічних експертних систем підтримки прийняття рішень;

W(S_i) – коефіцієнт ефективності (вага) СЗІ;

f – індекс, який позначає номер фактора (критерія);

N – кількість факторів (критеріїв);

a_f – коефіцієнт, який характеризує вклад кожного з факторів $c_f(S_i)$ у вазі ефективності СЗІ, при цьому $\sum_{f=1}^{N} a_f = 1$; $0 \le a_f \le 1$;

$c_f(S_i)$ – часткові показники (коефіцієнти) конкретного фактора (критерія), який характеризує ефективність СЗІ з використанням метода і моделі управління ІБ, при цьому $0 \le c_f(S) \le 1$.

Для визначення факторів (критеріїв), які будуть мати високий вплив на ефективність СЗІ з використанням методу та моделі, було опитано низку експертів, відповідальних за реалізацію процесів ІБ та прийняття управлінських рішень, в результаті чого були визначені наступні критерії оцінки ефективності:

− часові витрати на впровадження процесу ІБ;

− часові витрати на збір вихідних даних від процесу ІБ;

− часові витрати на обробку зібраної від процесу ІБ інформації;

− часові витрати на актуалізацію зібраної від процесу ІБ інформації;

− часові витрати на прийняття управлінського рішення;

− часові витрати на аналіз отриманих результатів.

Сформувавши загальні критерії оцінки ефективності СЗІ з використанням методу та моделі управління ІБ, експертам було запропоновано виставити оцінки щодо кожного з критеріїв.

При цьому максимальний коефіцієнт присвоювався тій реалізації СЗІ, в якій час на виконання повного циклу управління процесом ІБ був мінімальним. Результати експертної оцінки подано у таблиці 3.1.

Таблиця 3.1 - Значення коефіцієнтів та часткових показників для підсумкових значень ефективності еталонних та розроблених методів та моделей управління інформаційною безпекою

Фактори, які впливають на ефективність СЗІ		Ступінь значимості коефіцієнта	Частковий показник вихідних метода і моделі	Частковий показник розроблених метода і моделі
1	Часові затрати на впровадження процесу ІБ	0,25	1	1
2	Часові затрати на збір вихідних даних від процесу ІБ	0,1	0,5	1
3	Часові затрати на обробку зібраної від процесу ІБ інформації	0,15	0,3	1
4	Часові затрати на актуалізацію зібраної від процесу ІБ інформації	0,15	0,4	1
5	Часові затрати на прийняття управлінського рішення	0,25	0,6	1
6	Часові затрати на аналіз отриманих результатів	0,1	0,3	1
Підсумковий коефіцієнт ефективності			0,58	1

Формула для підсумкового коефіцієнта ефективності СЗІ з використанням вихідних метода і моделі управління ІБ S_1 має вигляд:

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

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 обчислень та отриманих результатів можна зробити висновок про те, що розроблені метод та модель управління ІБ на основі динамічних експертних систем підтримки прийняття рішень суттєво скорочують час виконання процесів ІБ та час на ухвалення управлінських рішень, що збільшує ефективність СЗІ на 42%.

ВИСНОВКИ

1. Здійснено аналіз міжнародної нормативної документації з питань управління інформаційною безпекою, що дозволило визначити типові підходи до питань управління інформаційною безпекою.

2. На основі класифікації процесних складових управління інформаційною безпекою визначено методи прийняття управлінських рішень при управлінні інформаційною безпекою.

3. Розроблено алгоритми і моделі даних процесів управління ризиками та загрозами, аудитом інформаційної безпеки, аналізу ефективності систем захисту інформації, що дозволило оцінити ефективність системи захисту інформації із застосуванням експертних динамічних систем.

4. Розроблено комплексну модель управління взаємодією даних у системі забезпечення інформаційної безпеки на основі експертних динамічних систем.

.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики: Вибр. наук. праці. К. : НІСД, 2016. 528 с.
2. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. Житомир: ЖНАЕУ, 2016. 636 с.
3. 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.
4. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. К.: ДУТ, 2015. 449 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. 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.
7. Лісовська Ю. Кібербезпека. Ризики та заходи. К.: Кондор, 2019. 272 с.
8. http://www.leta.ru/services/information-security-management/isms-iso-27001.html
9. Савенко О.С., Кльоц Ю.П., Лисенко С.М. Системне програмне забезпечення. – Хмельницький: ХНУ, 2016. 403с.
10. 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
11. 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.

12. Максимчук М.А. Модуль аналітичної обробки даних програмних засобів підтримки процесу оптимізації покриття оператора мобільного зв’язку. Інженерія програмного забезпечення. 2011. №2(6). С.106-110.

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

14. Козловський А.В., Паночишин Ю.М., Погрішук Б.В. Комп'ютерна техніка та інформаційні технології: навч. посіб. К.: Знання, 2014. 463с.

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

16. 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.

17. Cryptology and information security - past, present, and future role in society/ S. Bhattacharya. International Journal on Cryptography and Information Security (IJCIS). Vol. 9, No.1/2, 2019. P. 13-36.

18. 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.

19. 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.

20. http://www.iso27000.ua/

21. https://ua.wikipedia.org/wiki/Информаційна_безпека

22. http://itteach.ua/predstavlennya-znan/ekspertni-systemy

23. http://www.infosecurity.ua/iprotect/audit/suib/

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

25. http://tpl-it.wikispaces.com/

26. Aaron Russell. What Is an X.509 Certificate? 2019 [Електронний ресурс]. URL: https://www.ssl.com/faqs/what-is-an-x509-certificate/

27. Advantages and Disadvantages of Certificate Authentication. [Електронний ресурс] URL: https://www.ssh.com/manuals/server-zosproduct/55/ch06s03s05.html

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

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

30. HTTP - Status Codes. [Електронний ресурс] URL: https://www.tutorialspoint.com/http/http_status_codes.htm

31. RFC 7519: JSON Web Token. [Електронний ресурс] URL: https://oauth.net/2/jwt/

32. https://ua.wikipedia.org/wiki/Автоматизація

АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

проблемно-наукова міжгалузева конференція молодих науковців аспірантів та студентів

м. Тернопіль

2022

ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
НАДВІРНЯНСЬКИЙ КОЛЕДЖ НТУ
ГАЛИЦЬКИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

Проблемно-наукова міжгалузева конференція

АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

(АКІТ – 2022)

21—23 лютого 2022 року

Тернопіль

БЕЗПЕКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Продан Т.І. Івасьєв С.В.
СУЧАСНІ МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ…… 62

Хомич О.В.
ДОСЛІДЖЕННЯ ПОДІЙ ФАЙЛОВОЇ СИСТЕМИ……... 65

Кулина С.В.
ВИЯВЛЕННЯ ТА ВИПРАВЛЕННЯ ПОМИЛОК У ЗАХИЩЕНИХ СИСТЕМАХ ЗБЕРІГАННЯ ДАНИХ МЕТОДОМ ОБЧИСЛЕННЯ СИНДРОМУ……... 67

Ігнатєв І.В., Кондратюк В.М.
АЛГОРИТМИ ПЕРЕВІРКИ ЧИСЛА НА ПРОСТОТУ……. 70

Олійник Н.П.
ВИКОРИСТАННЯ СИМЕТРОЧНОГО ШИФРУ AES З РЕАЛІЗАЦІЄЮ НА JAVASCRIPT…… 73

Кондіус І.С.
ОЦІНКА ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ……. 76

Ковальчук О.В., Михайлевський О.А., Глинська І.К., Шандалюк С.А.
ВИБІР МЕТОДУ ВБУДОВУВАННЯ У ЗОБРАЖЕННЯ-КОНТЕЙНЕР…. 79

Недзельський Р.В,., Архитко О.В., Бодак С.В., Тихоліз М.В., Якименко І.З.
ЕВОЛЮТИВНИЙ АЛГОРИМТ ГЕНЕРУВАННЯ ПАРАМЕТРІВ ЕЛІПТИЧНИХ КРИВИХ……... 84

Гринчук А.М., Пилипів С.І., Войтенко О.О., Черняк В.А.
СТРУКТУРА ЦЕНТРУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЛЯ ПРОТИДІЇ ЗАГРОЗАМ……. 88

Миколишин П.П
СИСТЕМА ЗАПОБІГАННЯ ПРОНИКНЕННЮ В МЕРЕЖІ ІНТЕРНЕТ-РЕЧЕЙ……... 91

Концевич О.О., Бойко Н.З., Савіцький Т.Д.
МОДЕЛЮВАННЯ ТА ДОСЛІЖЕННЯ АТАКИ ЕНЕРГОСПОЖИВАННЯ НА ОСНОВІ ВАГИ ХЕМІНГА…….. 94

Гавриляк М.В., Цаволик Т.Г., Ігнатєв І.В.
ФУНКЦІЇ ТА ПЕРЕВАГИ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА БАЗІ SNORT…… 97

Терещенко О.С., Яцків В.В.
СУЧАСНІ ПЛАТФОРМИ РОЗВІДКИ КІБЕРЗАГРОЗ З ВІДКРИТИМ КОДОМ 100

Яцків Н.Г., Вівчар Д.В.
АНАЛІЗ ПІДХОДІВ ДО ОЦІНКИ РИЗИКІВ……... 104

Михайлишин Д.А., Цаволик Т.Г., Драпак В.І.
СИСТЕМА МОНІТОРИНГУ БЕЗПЕКИ КІНЦЕВИХ ПРИСТРОЇВ……. 107

Філіпчук М.М.
АЛГОРИТМ ЗАХИСТУ ВЕБ-РЕСУРСІВ……...…….. 110

УДК 004.5

Гринчук А.М.[1], Пилипів С. І.[2], Войтенко О.О.1, Черняк В.А.[3]

[1]Західноукраїнський національний університет
[2]Збаразький ліцей №3імені Михальського Т. Р.
[3]Рівненський державний аграрний коледж

СТРУКТУРА ЦЕНТРУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЛЯ ПРОТИДІЇ ЗАГРОЗАМ

Вступ. На сучасному етапі розвитку нашого суспільства інформація стає одним із найбільш цінних та затребуваних ресурсів, на збереження та захист яких виділяється все більше часу та коштів. У зв'язку з цим захист інформації є одним із важливих процесів будь-якої організації.

Процес управління інформаційною безпекою (ІБ) нерозривно пов'язаний із процесами захисту інформації [1], адже повнота та коректність його реалізації багато в чому визначає ефективність системи захисту інформації (СЗІ), однак у типовій СЗІ, підсистема управління ІБ, як правило, відсутня.

Одним із перспективних напрямків при вирішенні цієї проблеми є використання експертних систем підтримки прийняття рішень [2], здатних взяти на себе більшу частину функцій та рутинних операцій, що виконуються персоналом.

Мета: розробка структури центру управління інформаційною безпекою для протидії загрозам.

1. Структура центру управління інформаційною безпекою установи

Залежно від розміру, загального стану та складу системи захисту інформації, а також основного напряму діяльності установи, розроблений метод управління інформаційною безпекою матиме різну архітектуру, а також різний набір основних процесів управління та забезпечення інформаційної безпеки. При цьому, виходячи з типової інформаційно-телекомунікаційної структури організації, реалізація доданих методу та моделі управління інформаційною безпекою дозволить зв'язати розрізнені сервіси інформаційної безпеки організації з організаційними заходами та технічними засобами захисту, а також встановити зв'язок між спеціалізованими інструментами керування технічними засобами та управлінням персоналом організації, що відповідає за забезпечення інформаційної безпеки.

На рисунку 1 представлена схема функціональної структури центру управління інформаційною безпекою на основі цього методу.

Створення єдиного центру управління інформаційною безпекою установи на основі запропонованого методу управління інформаційною безпекою буде кінцевою, найбільш повною реалізацією основних положень методу та моделі управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень.

При цьому центр управління інформаційною безпекою матиме виділене становище у складі організації, у якому вже сама система захисту інформації буде складовою єдиного центру управління інформаційної безпекою.

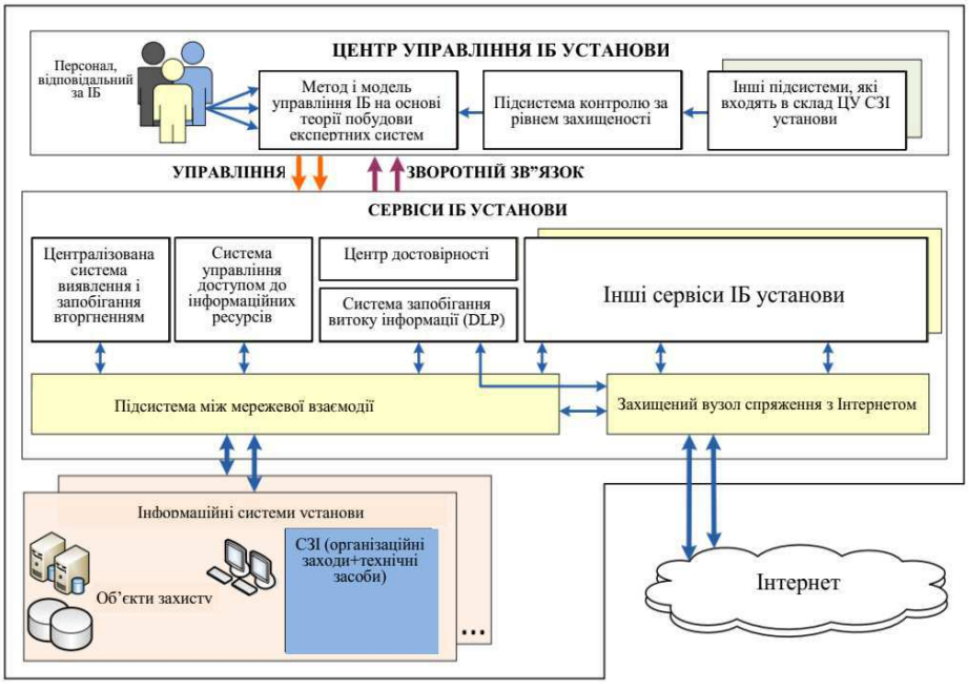

Рисунок 1 – Структура центру управління інформаційною безпекою установи

Таким чином, реалізація методу та моделі управління інформаційною безпекою на основі динамічних експертних систем підтримки прийняття рішень може призвести до:– систематизації вимог щодо управління інформаційною безпекою, виходячи зі складу процесів забезпечення інформаційної безпеки в організації;

- пов'язаного застосування організаційних заходів та технічних засобів захисту інформації, що діють у рамках системи захисту інформації організації;
- формуванню аналітичної бази проведення досліджень та аналізу стану інформаційної безпеки;
- здійсненню раціонально обґрунтованого стратегічного, тактичного та оперативного управління процесами забезпечення інформаційної безпеки;
- можливості своєчасного застосування коригувальних та попереджуючих впливів на основі комплексного аналізу стану інформаційної безпеки в цілому та об'єктів захисту зокрема;
- забезпечення планування розвитку та підтримки системи захисту інформації;
- формалізації основних та другорядних процесних складових управління та забезпечення інформаційної безпеки в організації;
- підвищення загального рівня інформаційної безпеки організації за рахунок формалізації та систематизації основних процесів інформаційної безпеки;
- зниження операційних ризиків за рахунок зменшення ймовірності реалізації загроз інформаційної безпеки через підвищення загального рівня інформаційної безпеки в організації;
- підвищення прозорості процесів інформаційної безпеки в рамках системи захисту в організації;

- підвищення оперативності при вирішенні завдань забезпечення інформаційної безпеки;
- підвищення рівня компетенції персоналу організації та спеціалістів із захисту інформації у питаннях інформаційної безпеки;
- підвищення оперативності реагування на інциденти інформаційної безпеки;
- мінімізації витрат на експлуатацію системи захисту інформації організації.

2. Управління ризиками та загрозами інформаційної безпеки

Грунтуючись на багаточисельних опитуваннях експертів в області інформаційної безпеки було встановлено, що кожний з параметрів загроз інформаційної безпеки являється пов'язаним з іншими, дані зв'язки представлені на рисунку 2.

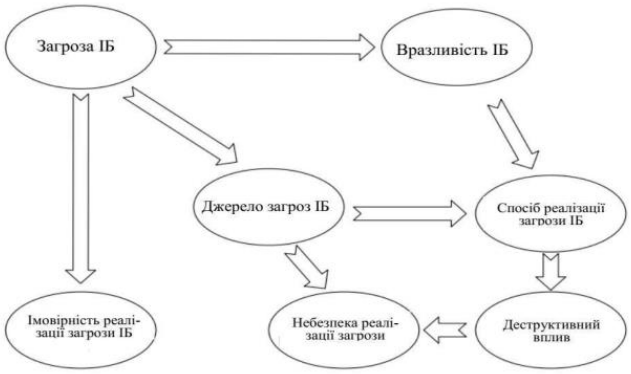

Рисунок 2 – Зв'язок параметрів загроз інформаційній безпеці

Таким чином, незалежно від обраної методики оцінки ризиків та визначення загроз інформаційній безпеці, у процесі управління ризиками та загрозами інформаційної безпеки можлива побудова спільного дерева ризиків-загроз для конкретно обраного активу, що дає повну картину, необхідну для їхнього аналізу.

Залежно від важливості активу, ймовірності реалізації загрози та джерела загрози, гілки дерева будуть змінюватися для кожної конкретної загрози, виходячи з типу активу та моделі порушника (як одного з основних джерел загроз). На актуальність загрози впливатимуть у загальному випадку ймовірність реалізації загрози та ступінь її небезпеки, а у разі ризикового підходу до уваги братимуться і можливі наслідки деструктивного впливу на аналізований актив.

Висновки. Розроблено структуру центру управління інформаційною безпекою установи. Встановлено взаємозв'язок між параметрами загроз інформаційній безпеці установи.

Перелік використаних джерел.

1. Bender David. Bender on Privacy and Data Protection. LexisNexis, 2020. - 2940 p.
2. Schreider Tari. Building an Effective Security Program. 2nd Edition. - Rothstein Associates Inc., 2020. - 406 p.


КІБЕРБЕЗПЕКА ТА
КОМП'ЮТЕРНО-ІНТЕГРОВАНІ
ТЕХНОЛОГІЇ
КБКІТ-2022
науково-практична конференція
молодих вчених
аспірантів та студентів
м.Тернопіль

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2022)

науково-практична конференція
молодих вчених, аспірантів та студентів

29–31 серпня 2022
Тернопіль

ЗМІСТ

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

Хомич О.В.
СИСТЕМА РЕАГУВАННЯ НА ІНЦИДЕНТИ В ОС LINUX 7

Яцків Н.Г., Вівчар Д.В.
АНАЛІЗ ПІДХОДІВ ДО ОЦІНКИ РИЗИКІВ 10

Кулина С.В.
ВИЯВЛЕННЯ ТА ВИПРАВЛЕННЯ ПОМИЛОК У ЗАХИЩЕНИХ СИСТЕМАХ ЗБЕРІГАННЯ ДАНИХ МЕТОДОМ ОБЧИСЛЕННЯ ПРОЕКЦІЇ ЧИСЛА 13

Кондіус І.С.
ДОСЛІДЖЕННЯ МЕТОДИК ОЦІНКИ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ 17

Бовнегра Л.В., Тимошенко Л.М., Накоряков О.Г.
ДОСЛІДЖЕННЯ СИСТЕМ ОЦІНЮВАННЯ КІБЕР-СИТУАЦІЙНОЇ ОБІЗНАНОСТІ 22

Іваницький Б.О., Павловський С,. Горошко Н.М, Куць Т.І., Куць І.С
РЕЖИМИ РОБОТИ АЛГОРИТМУ AES 26

Бондарчук В.Р., Сегін А.І., Давлетова А.Я.
МЕТОДИ ЗАХИСТУ ЦИФРОВИХ ДАНИХ НА ОСНОВІ КОРЕЛЯЦІЙНИХ ФУНКЦІЙ 31

Надозірний С.В.
СУЧАСНІ ЗАГРОЗИ В СФЕРІ БЛОКЧЕЙН ПРОЕКТІВ 36

Яцків В.В., Терещенко О.С.
РОЗВІДКА КІБЕРЗАГРОЗ З ВИКОРИСТАННЯМ МОВИ ОПИСУ ПРАВИЛ YARA 40

Гринчук А.М., Лисобей Л.В., Черняк В.А.
МАТЕМАТИЧНА МОДЕЛЬ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ УСТАНОВИ 43

Бабич С.В.
ТЕХНОЛОГІЯ ОБМАНУ НА ОСНОВІ ФАЙЛІВ…… 46

БЕЗПЕКА ТА ІНТЕРНЕТ РЕЧЕЙ

Костючко С.М., Якименко І.З., Поліщук М.М., Конкевич Л.М.
СИСТЕМА ЗАХИСТУ ВІД ВНУТРІШНІХ ЗАГРОЗ ЗАСОБАМИ МАШИННОГО НАВЧАННЯ 48

Хомицький А.А.
АНАЛІЗ КО КАТЕГОРІЙ ПРИМАНОК ДЛЯ ВИЯВЛЕННЯ АТАК НА ІНТЕРНЕТ РЕЧЕЙ 51

УДК 519.7

Гринчук А.М.[1], Лисобей Л.В.[2], Черняк В.А.[3]

[1]Західноукраїнський національний університет
[2]Тернопільська українська гімназія імені Івана Франка
[3]Рівненський державний аграрний коледж

МАТЕМАТИЧНА МОДЕЛЬ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ УСТАНОВИ

Вступ. На даний час кількість засобів і заходів захисту інформації постійно збільшується і спільно із існуючими недоліками типової реалізації системи захисту інформації (СЗІ) збільшують навантаження на персонал, збільшуючи час прийняття управлінських рішень. Через неможливість збільшення кількості ресурсів, що виділяються на процеси забезпечення та управління інформаційної безпеки ІБ [1], до нескінченності, особливо гостро постає проблема раціоналізації їх використання з урахуванням сучасних інформаційних технологій та засобів обробки інформації. Тому актуальність даної роботи зумовлюється відсутністю науково-методичного апарату, що враховує потреби та особливості управління ІБ, а також відсутністю систем управління ІБ [2], здатних підвищити ефективність СЗІ за рахунок зниження часових витрат на виконання процесів забезпечення ІБ та прийняття управлінських рішень на основі динамічних експертних систем.

Мета: розробити математичну модель управління ІБ установи.

1. Розробка математичної моделі управління інформаційною безпекою

Розглянемо окрему установу, що обробляє критично важливу інформацію. Нехай у цій організації протікає i=1, ..., n рівноправних процесів управління інформаційною безпекою та існує обмежена кількість ресурсів r_i, які витрачаються на їх реалізацію. Кожен із процесів i визначається параметрами $t_i(r_i)$ – час отримання інформації під час виконання процесу, $f_i(x_i)$ – кількість одержуваної інформації під час виконання процесу. У рамках своєї діяльності установа зазнала атаки, що загрожує неперервності діяльності всієї організації. Керівництву організації потрібно прийняти відповідне управлінське рішення для припинення атаки за час t_{max}, при цьому склад наявних ресурсів R є незмінним.

Розглянемо поточний стан справ установи, у якій існує СЗІ, що, зіткнувшись з виникненням загрози Y, не може їй протистояти в поточному стані. X_0. Тоді множина всіх можливих станів - X_1, X_2, X_3, ..., X_k, при цьому P - ймовірність знаходження в k-му стані. Ймовірності усіх станів є однакові: $P_0=P_1=P_2=P_3=\cdots P_k$; $P_0+P_1+P_2+P_3+\cdots P_k=1$. Припустимо, що існує такий стан системи $X_Y \in Xk$, коли вона здатна протистояти загрозі Y, таким чином суть прийнятого рішення повинна зводитися до вибору такого стану з множини можливих станів. Згідно положенням теорії інформації, невизначеність знаходження системи в рівно ймовірнісних станах визначатиметься максимальною ентропією H, тоді ентропія для розглянутих випадків, коли невідомий і відомий стан аналізованої системи, у якому вона здатна протистояти загрозі Y, буде H_0 і H_Y відповідно. Згідно з Шенноном, різниця H_0 і H_Y буде кількістю інформації, тоді $F=H_0-H_Y$ буде кількість інформації, необхідна для

ухвалення рішення про перехід аналізованої системи з поточного стану X_0 у стан $X_Y \in X_k$, для протистояння загрозі Y. Позначимо загальну кількість всіх можливих загроз як $Y_{заг}$, очевидно, що виникнута загроза $Y \in Y_{заг}$. Нехай кожна з можливих загроз $Y_x \in Y_{заг}$ (де x=1, 2, …, m – номер загрози) описується сукупним рядом незалежних параметрів α_j (де j=1, 2, …, n – номер параметра), тоді множина $Y_{заг}$ описуватиметься сукупною множиною всіх можливих унікальних параметрів α_{jx}, властивих загрозам. Таким чином можна скласти повну матрицю відповідності загрози та їх параметрів розмірності m на n. Перш, ніж приймати рішення про переведення СЗІ у певний стан, необхідно визначити загрозу Y. У даному випадку ми стикаємося з невизначеністю вибору, адже ймовірності виникнення кожної із зазначених вище загроз будуть рівними. Таким чином, маємо проблему при прийнятті управлінського рішення, адже у цьому випадку невизначеність, а значить і ентропія H необхідного нам вибору, буде максимальною: $H(Y_x) = -\ln P(Y_x)$, де P – ймовірність виникнення загрози Y_x. Оскільки отримана максимальна ентропія буде повною (сумісною) ентропією низки незалежних випадкових загроз Y_1, Y_2, ..., Y_m, можна скористатися властивістю адитивності ентропії та представити їх сумісну ентропію як повну суму ентропій щодо кожної загрози: $H(Y_x)=H(Y_1)+H(Y_2)+H(Y_3)+\dots$.

Щоб знизити отриману невизначеність і прийняти рішення, необхідно зробити збір інформації, здатної описати загрозу, тобто визначити один із параметрів α_{jx}. Кожен із процесів ІБ, що протікають в організації, здатний надати інформацію про значення поточного параметра для загрози, що виникла, а грунтуючись на співвідношенні параметрів, вказаних у таблиці 1, залежно від отриманих значень ряд загроз із загальної множини $Y_{заг}$ буде відхилятися через невідповідність отриманого параметра, таким чином підвищуючи кількість визначених параметрів загрози, невизначеність вибору стану захисту зменшується. Розглянемо випадок, коли загальна кількість можливих загроз дорівнює 5, а загальна кількість унікальних параметрів загроз дорівнює 7. Представимо матрицю співвідношення загроз та їх параметрів у таблиці 1.

Таблиця 1 - Матриця співвідношення загроз та їх параметрів

	α_1	α_2	α_3	α_4	α_5	α_6	α_7
Y_1	1	0	0	1	0	0	1
Y_2	0	1	0	0	0	0	1
Y_3	0	0	1	0	0	1	0
Y_4	0	0	0	1	0	0	0
Y_5	0	1	0	0	1	0	0

Для визначення загрози Y, що належить розглянутій множині, необхідно звернутися до одного з процесів ІБ для визначення параметра α_n. Загальна ентропія для цього випадку буде обчислюватися як повна сума ентропій за кожною загрозою: $H(\text{Заг})=H(Y_1)+H(Y_2)+H(Y_3)+H(Y_4)+H(Y_5)+H(Y_6)+H(Y_7)$.

Нехай першому кроці визначається параметр α_4=1, тобто лише загрози Y_1 та Y_4 задовольняють отриманому значенню параметра, а отже загрози, що залишилися, виключаються. Отримана ентропія знижується:
$H(1)=H(Y1)+H(Y2)+H(Y3)+H(Y4)+H(Y5)+H(Y6)+H(Y7)-H(Y2)-H(Y3)-H(Y5)=H(Y1)+H(Y4)$.

Очевидно, що H(Заг)>H(1). На наступних кроках потрібно вибирати новий параметр загрози доти, поки не залишиться єдино можливої загрози Y, яка і буде шуканою. Слід звернути увагу, що в даному випадку немає обмежень в ресурсних і часових рамках, таким чином можна знизити невизначеність вибору нанівець. Однак у загальному випадку, через обмеженість у часі та ресурсах однозначне визначення загрози може бути неможливим. Таким чином невизначеність вибору буде зменшена, але все ще збережеться. В даному випадку розглянутий приклад, у якому враховується лише наявність параметра α, а чи не його реальне значення, тепер перейдемо до розгляду ситуації, що склалася в аналізованій організації.

Нехай за кожен із процесів ІБ, що протікають у СЗІ організації, відповідає окремо взятий експерт. Припустимо, що кожен з експертів здатний заповнити таблицю співвідношення загроз та їх параметрів у частині, що його стосується. Таким чином, отримається повна таблиця 2 апріорних ймовірностей виникнення загрози, заснованої на сукупній експертній думці.

Таблиця 2 – Співвідношення загроз та їх параметрів, заснована на експертних оцінках

	α_1	α_2	α_3	α_4	α_5	α_6	α_7	…	α_n
Y_1	0,04	0	0,06	0,1	0,04	0,06	0,04	…	0
Y_2	0	0,06	0	0,04	0,6	0	0	…	0,35
Y_3	0,6	0,1	0,04	0	0	0,1	0,04	…	0
…	…	…	…	…	…	…	…	…	…
Y_5	0,04	0	0,1	0,06	0	0,04	0,1	…	0,6

Оскільки число параметрів, що визначають загрозу, суворо визначено, а їх сукупність дає повний опис загрози, то повна сума всіх параметрів конкретної загрози рівна 1. Нехай після n ітерацій визначення параметрів α загальна ентропія зменшилася і відсікла частину загроз $Y_{\text{від}}$ через невідповідність передбачуваних параметрів апостеріорним значенням, але не рівна 1. Тоді показники апріорної невизначеності знизилися і стали рівні апостеріорній ентропії. Отримана апостеріорна ентропія менша апріорної, тобто область можливих рішень зменшилася і дорівнює кількості отриманої інформації від процесів ІБ. Грунтуючись на зібраній інформації за відведений час, отримуємо необхідність прийняття рішення з урахуванням невизначеності, коли шукана загроза $Y(\alpha_1, \alpha_2, \ldots, \alpha_n) \in (Y\text{заг} - Y\text{від})$. Вирішення даного завдання спричинить зниження невизначеності вибору та прийняття відповідного керуючого впливу на усунення загрози з урахуванням наявних вимог та обмежень, включаючи умови для часу та ресурсів, які відводяться на прийняття управлінського рішення

Висновок. Розроблено математичну модель управління інформаційною безпекою установи.

Перелік використаних джерел.

1. [Електронний ресурс].- Режим доступу: http://www.infosecurity/iprotect/audit/suib/

2. [Електронний ресурс].- Режим доступу: http://www.e4group/about/control-system/the-system-of-information-security-management/