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

ПІДЛИСЬКИЙ Петро Йосифович

Модель центра інтелектуального управління мережевою безпекою / Model of the centre of intelligent control of network security

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
П.Й. Підлиський

_____

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

_____

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2024 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2024

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 2023 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ПІДЛИСЬКИЙ ПЕТРО ЙОСИФОВИЧ

1. Тема кваліфікаційної роботи:
Модель центра інтелектуального управління мережевою безпекою / Model of the centre of intelligent control of network security

керівник роботи д.т.н., професор М.М. Касянчук
затверджені наказом по університету від «12» грудня 2023 року №753.
2. Строк подання студентом закінченої кваліфікаційної роботи 12 грудня 2024 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– аналіз методики побудови та функціонування типового ЦІУМБ;
– розробка функціональної та зональної архітектури забезпечення інформаційної безпеки в ЦІУМБ;
– розробка схеми процесу отримання знань ЦІУМБ;
– побудова моделі обробки даних у ЦІУМБ за допомогою «Озера даних»;
– дослідження функціональної стійкості ЦІУМБ в єдиному інформаційному просторі.

5. Перелік графічного матеріалу у роботі:
– узагальнена модель процесів забезпечення ІБ в ЦІУМБ;
– схема процесу отримання знань про ІБ ІТКМ для ЦІУМБ;
– процес використання ІБ-аналітики в ЦІУМБ з точки зору ІТ великих даних;
– спрощена архітектура обробки даних у ЦІУМБ;
– складові процесу управління функціональною стійкістю ЦІУМБ;
– процес відновлення функціональної стійкості типового ЦІУМБ після інциденту ІБ;
– основні елементи системи управління функціональною стійкістю ЦІУМБ.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 12 грудня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз роботи Центру інтелектуального управління мережевої безпеки	12.2023 р. – 03.2024 р.	
2	Архітектура Центру інтелектуального управління мережевою безпекою	03.2024 р. – 06.2024 р.	
3	Розробка моделі Центра інтелектуального управління мережевою безпекою	06.2024 р. – 11.2024 р.	

Студент _____ Підлиський П.Й.
(підпис)

Керівник роботи _____ д.т.н., професор М.М.Касянчук

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Модель центра інтелектуального управління мережевою безпекою” на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека та захист інформації” освітньо-професійної програми «Кібербезпека» написана обсягом 81 сторінка і містить 8 ілюстрацій, 3 таблиці, 1 додаток та 30 джерел за переліком посилань.

Метою випускної кваліфікаційної роботи є розробка моделі Центра інтелектуального управління мережевою безпекою.

Методи дослідження. Математичні методи моделювання, методи дослідження мереж, методи дослідження стійкості до атак.

Результати дослідження. Здійснено аналіз сучасних методик побудови типових Центрів інтелектуального управління мережевою безпекою, що дозволило виявити їх недоліки та обгрунтувати необхідність використання нових підходів до комплексного управління інформаційною безпекою. Розроблено функціональну та зональну архітектуру забезпечення інформаційної безпеки в Центрі інтелектуального управління мережевою безпекою, що дозволило побудувати схему отримання знань Центром управління. Розроблено модель обробки даних у Центрі інтелектуального управління мережевою безпекою за допомогою «Озера даних», що дозволило продемонструвати функціональну стійкість Центру в єдиному інформаційному просторі. Розроблено функціональну та зональну архітектуру забезпечення інформаційної безпеки в Центрі інтелектуального управління мережевою безпекою та побудовано модель обробки даних за допомогою «Озера даних».

Результати роботи можуть успішно застосовуватися в різних установах для захисту інформації за допомогою Центру інтелектуального управління мережевою безпекою.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, МЕРЕЖЕВА БЕЗПЕКА, ЦЕНТР УПРАВЛІННЯ, МОДЕЛЬ, ОЗЕРО ДАНИХ.

ABSTRACT

The graduate work on the topic „Model of the centre of intelligent control of network security” for Master’s degree on speciality 125 "Cybersecurity and Information Protection" is written on 81 pages and contains 8 illustrations, 3 tables, 1 suplement and 30 references.

The aim of graduate work is to develop a model of the Intelligent Network Security Management Center.

Research methods. Mathematical modeling methods, network research methods, methods for researching resistance to attacks.

Results of the study. An analysis of modern methods for building typical Intelligent Network Security Management Centers was carried out, which allowed to identify their shortcomings and justify the need to use new approaches to comprehensive information security management. A functional and zonal architecture for ensuring information security in the Center for Intelligent Network Security Management has been developed, which allowed building a scheme for obtaining knowledge by the Control Center. A data processing model has been developed in the Center for Intelligent Network Security Management using the “Data Lake”, which allowed demonstrating the functional stability of the Center in a single information space. A functional and zonal architecture for ensuring information security in the Center for Intelligent Network Security Management has been developed and a data processing model has been built using the “Data Lake”.

The results of the work can be successfully applied in various institutions to protect information using the Center for Intelligent Network Security Management.

Keywords: INFORMATION SECURITY, NETWORK SECURITY, CONTROL CENTER, MODEL, DATA LAKE.

ЗМІСТ

ВСТУП

Інтенсивний розвиток та використання сучасних інформаційно-комунікаційних технологій (ІКТ) для обробки цифрової інформації [1-3] призвели до серйозних якісних змін в економічній, соціально-політичній і духовній сферах життя суспільства [4-6]. Цей феномен зростаючого впливу формування цифрового суспільства XXI століття було вперше відзначено в «Окінавській Хартії глобального інформаційного суспільства», ухваленій у 2000 р. лідерами «вісімки». В основі ІКТ лежить інформаційно-телекомунікаційна система, яка базується на інформаційно-телекомунікаційній мережі (ІТКМ) – технологічній системі (ТС), яка призначена для передачі по лініях зв'язку інформації, доступ до якої здійснюється з використанням засобів обчислювальної техніки [7-10].

ІТКМ, інформаційні системи (ІС), автоматизовані системи управління (АСУ), а також мережі електрозв'язку, що використовуються для організації взаємодії таких об'єктів, відносяться до об'єктів критичної інформаційної інфраструктури (КІІ) [11-12]. Суб’єкти КІІ – державні органи і установи, юридичні особи та (або) індивідуальні підприємці, яким на праві власності, оренди або на іншій законній підставі належать ІС, ІТКМ, АСУ, що функціонують у різних сферах діяльності та областях промисловості, а також юридичні особи та (або) індивідуальні підприємці, які забезпечують взаємодію зазначених систем чи мереж.

Отже, для ІТКМ як невід'ємної частини забезпечення діяльності організацій необхідно забезпечити функціональну стійкість та безпеку їх інформаційних ресурсів і послуг, що надаються [13].

У той же час, в останнє десятиліття ризики порушення безпеки для об'єктів КІІ, включаючи ІТКМ її суб'єктів, набули статусу компонентів системного ризику [14-15]. В якості основних причин даної тенденції можна виділити, в першу чергу, складність і різнорідність ІТКМ різних суб'єктів за функціями, структурою та організаційно-правовими формами, зростаючу роль різних

технологій у наданні послуг та все більшу залежність останніх від уразливостей ІКТ [16-17]. Крім того, потрібно врахувати що посилюється взаємозалежність між всіма учасниками інформаційних взаємодій, а також зростання складності, широкої спрямованості та різноманітності комп'ютерних атак, а також поява нових категорій зловмисників і цілей, які вони переслідують [18].

Численні щорічні дослідження в області інформаційної безпеки (ІБ) ІТКМ показують, що стратегії забезпечення ІБ, які традиційно були засновані на дотриманні нормативних та правових вимог [19] і обмежувалися лише «захистом периметра», не встигають за зростаючою кількістю і все більш витонченими методами, що застосовуються зловмисниками [20-21].

З вище викладеного очевидний висновок, що наразі актуальним є пошук рішення для побудови Центру інтелектуального управління мережевою безпекою (ЦІУМБ) [22, 23], за рахунок якого досягається дотримання для ІТКМ відповідних вимог щодо забезпечення ІБ (наприклад, для суб'єкта КІІ відповідно до присвоєної йому категорії значимості). Таке рішення забезпечить інформаційну захищеність ІТКМ – таку її здатність, за якої в єдиному інформаційному просторі (ЄІП) створено адекватне захищене середовище функціонування ІТКМ, що забезпечує необхідний рівень ІБ для отримання (пошуку та збору), обробки, зберігання, поширення (передачі та надання) та знищення інформації [24-25]. Захищеність досягається забезпеченням сукупності властивостей ІБ - конфіденційності, цілісності, доступності, справжності, підзвітності, невідмовності та достовірності, пріоритетність яких визначається значимістю інформації.

Мета роботи. Метою даної роботи є розробка моделі Центра інтелектуального управління мережевою безпекою.

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

– аналіз методики побудови та функціонування типового ЦІУМБ;

– розробка функціональної та зональної архітектури забезпечення інформаційної безпеки в ЦІУМБ;

– розробка схеми процесу отримання знань ЦІУМБ;

– побудова моделі обробки даних у ЦІУМБ за допомогою «Озера даних»;

– дослідження функціональної стійкості ЦІУМБ в єдиному інформаційному просторі.

Об’єкт дослідження. Процес захисту інформації на основі побудови ЦІУМБ.

Предмет дослідження. Методи і засоби захисту інформації на основі ЦІУМБ.

Методи дослідження. Математичні методи моделювання, методи дослідження мереж, методи дослідження стійкості до атак.

Наукова новизна одержаних результатів.

1. Здійснено аналіз сучасних методик побудови типових Центрів інтелектуального управління мережевою безпекою, що дозволило виявити їх недоліки та обгрунтувати необхідність використання нових підходів до комплексного управління інформаційною безпекою.

2. Розроблено функціональну та зональну архітектуру забезпечення інформаційної безпеки в Центрі інтелектуального управління мережевою безпекою, що дозволило побудувати схему отримання знань Центром управління.

3. Розроблено модель обробки даних у Центрі інтелектуального управління мережевою безпекою за допомогою «Озера даних», що дозволило продемонструвати функціональну стійкість Центру в єдиному інформаційному просторі.

Практичне значення отриманих результатів. Розроблено функціональну та зональну архітектуру забезпечення інформаційної безпеки в Центрі інтелектуального управління мережевою безпекою та побудовано модель обробки даних за допомогою «Озера даних».

Публікації та апробація КР.

1. Підлиський П., Лисик М. Модель функціональної стійкості Центру інтелектуального управління мережевою безпекою. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека

та комп’ютерно-інтегровані технології» (КБКІТ-2024), Тернопіль, 2024. С.153-155 [26].

2. Підлиський П., Залужна Н. Функціональна інфраструктура типового Центру інтелектуального управління мережевою безпекою. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2024. С.80-81 [27].

1 АНАЛІЗ РОБОТИ ЦЕНТРУ ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ

1.1 Методика побудови типового Центру інтелектуального управління мережевої безпеки

Розробка типового ЦІУМБ як спеціалізованого структурного елемента, вбудованого в ІТКМ установи, також означає необхідність відображення його системотворчої ролі в забезпечення ІБ цієї установи. Іншими словами, будучи частиною ІТКМ, типовий ЦІУМБ також служити основою системи управління мережевою безпекою установи як частини її системи управління ІБ (СУІБ), а отже, і системи забезпечення ІБ (СЗІБ) ІТКМ. Досвід розробки подібних систем свідчить про те, що створення багатокомпонентних центрів управління безпекою можливе лише при обов'язковому дотриманні загальносистемної методології побудови всіх складових частин типового ЦІУМБ у структурі ІТКМ установи та ЦІУМБ як єдиної системи загалом.

Розроблена методика побудови типового ЦІУМБ установи як впорядкована сукупність методів та засобів його створення та подальшої еволюції становить собою теоретичну основу, необхідну для багаторазово повторення різними організаціями реалізації цілей та завдань створення типового ЦІУМБ. Вона забезпечує зниження складності та неоднозначності процесу побудови мереж зв'язку, систем обробки даних, інших систем та підсистем, наданих послуг та інших елементів ЦІУМБ за рахунок повного та точного опису цього процесу, а також застосування сучасних підходів їх побудови протягом всіх стадій життєвого циклу - від задуму до реалізації.

Специфіка розробленої науково обґрунтованої методики побудови типової ЦІУМБ полягає в її універсальності. Її головна ідея - це орієнтація на існуючі, обрані в результаті системного аналізу типові проектні рішення побудови його телекомунікаційної мережі, ІТ-послуг, використовуваних технологій забезпечення ІБ та систем захисту інформації (СЗІ) та допоміжних систем та комплексів, що відображають розвиток сучасних засобів обчислювальної

техніки (ЗОТ) та ІКТ. Саме уніфікація та стандартизація типового ЦІУМБ загалом та його типових проблемно-орієнтованих на процеси управління інцидентами ІБ (ПУІБ) компонентів, на базі яких здійснюється його побудова, має велике практичне значення в сучасних умовах. При широкому використанні імпортних ЗОТ, телекомунікаційного обладнання, апаратно-програмних СЗІ цей фактор стає об'єктивною необхідністю побудови типового ЦІУМБ. Крім цього, такий підхід надає єдині принципи та підходи до побудови окремих гомогенних (однорідних) систем та компонентів ЦІУМБ з орієнтацією на єдині базові технології їх функціонування, а також до забезпечення їх сумісності та уніфікації використовуваних для них програмних та технічних рішень та модулів.

Основна мета розробленої методики побудови типового ЦІУМБ як складного організаційно-технічного комплексу полягає в такій організації процесу побудови та забезпечення єдності управління ним, при якій гарантується виконання всіх сформульованих вимог, що пред'являються як до ЦІУМБ, так і до характеристик процесу розробки кожного його складового елемента.

Основним методологічним принципом побудови є системний підхід, згідно з яким при побудові типового ЦІУМБ забезпечується послідовне отримання надійних результатів забезпечення мережевої безпеки ІТКМ у рамках усієї СЗІБ різних організацій та розробляються і використовуються такі методики створення його інформаційного, аналітичного, технічного, програмного та організаційного забезпечення, які взаємопов'язані із загальною концепцією побудови та використання організаціями своїх ІТКМ.

Ключовими завданнями, вирішення яких має забезпечити методика побудови типового ЦІУМБ, є такі:

- забезпечення створення типового ЦІУМБ як відкритої інформаційної системи, що характеризується інтероперабельністю (здатністю до взаємодії при виконанні загальної роботи з використанням стандартних інтерфейсів), переносимістю (ПЗ, даних та користувачів) та функціонуванням відповідно до загальновизнаних стандартів з урахуванням усіх вимог до автоматизації ПУІБ для ІТКМ;

- гарантія створення типового ЦІУМБ із заданими якостями (власна захищеність, керованість, функціональна стійкість, масштабованість, еластичність, гнучкість, здатність до безперервного розвитку тощо) у задані терміни в рамках виділених засобів;

- підтримка централізовано керованих та контрольованих скоординованих дій при розробці кожної системи та комплексу типового ЦІУМБ відповідно до загальної концепції його побудови;

- забезпечення використання в створюваному типовому ЦІУМБ наявного обладнання в області ІКТ, ПЗ, БД тощо та створення умов для подальшої адаптації типового ЦІУМБ в середовище ІТКМ за рахунок його інтеграції до ЄІП організацій;

- підтримка зручності супроводу, модернізації та нарощування типового ЦІУМБ для адаптованості до динамічно змінного середовища ведення діяльності організацій та функціонування у цьому середовищі ІТКМ.

Основні завдання процесу побудови типового ЦІУМБ визначаються наступним чином, що відповідає послідовності дій, кожна з яких може бути додатково розбита на етапи та виконувані на них процеси:

- формулювання цілей і завдань створення типового ЦІУМБ в залежності від кола його користувачів та компонентів, що зумовлюють вибір принципів побудови;

— обстеження типової ІТКМ, збір, систематизація та аналіз первісної інформації, необхідної для побудови типового ЦІУМБ, вбудованого в ІТКМ;

- вибір методів і засобів розробки типового ЦІУМБ і організація робіт з його побудови відповідно до прийнятого плану робіт;

- розробка моделей діяльності, що автоматизується на основі типового ЦІУМБ;

- розробка архітектури типового ЦІУМБ;

- розробка вимог до функціональної та територіальної інтеграції всіх інформаційних та телекомунікаційних елементів у типовому ЦІУМБ та інтеграції типового ЦІУМБ у типову ІТКМ;

- розробка вимог до всіх елементів інформаційної та телекомунікаційної (як засобам підтримки локального та віддаленого інформаційного обміну між об'єктами та користувачами) складових типового ЦІУМБ;

- розробка інформаційної моделі (структури) типового ЦІУМБ (включаючи, наприклад, визначення множини наданих користувачам типових ІТ-послуг та інформаційних ресурсів із зазначенням пріоритетів щодо забезпечення основних властивостей ІБ для них);

- розробка вимог до цифрової інформації, представленої в різних форматах, для передачі від гетерогенних джерел по каналах зв'язку у вигляді єдиних інформаційних потоків як з типової ІТКМ в типовий ЦІУМБ і назад (наприклад, файли або команди зі зміни конфігураційних налаштувань СЗІ всередині типової ІТКМ), так і всередині типового ЦІУМБ;

- розробка відповідних технічних завдань на побудову та проект технічного завдання на впровадження типового ЦІУМБ, включаючи відповідні програми та методики випробувань;

- здійснення обґрунтованого вибору засоів для реалізації типового ЦІУМБ;

- розгортання типового ЦІУМБ на місці його експлуатації, включаючи проведення робіт з пілотування технічних рішень типового ЦІУМБ у типовій ІТКМ;

- апробація (проведення попередніх системних випробувань) та доопрацювання за її результатами технічних рішень, що забезпечують функціонування типового ЦІУМБ в типовій ІТКМ згідно з певними цілями та завданнями;

- розробка відповідної користувальницької та експлуатаційної документації для різної цільової аудиторії під час впровадження та використання типового ЦІУМБ;

- супровід типового ЦІУМБ, включаючи управління режимами функціонування, супровід технічних та програмних засобів, реєстрацію, діагностику та локалізацію помилок, внесення змін та тестування тощо.

Для кожного з перерахованих етапів далі необхідно визначити послідовність виконуваних у його межах робіт, вихідні дані та одержувані результати, необхідні для виконання робіт методи, засоби та ресурси, ролі та відповідальність учасників тощо. Такий формальний опис побудови типового ЦІУМБ дозволяє спланувати і організувати процес розробки типового ЦІУМБ та забезпечити його керованість.

Застосування розробленої методології побудови типової ЦІУМБ забезпечить виконання наступних загальносистемних вимог до ЦІУМБ:

— типовий ЦІУМБ проектується у відповідності з типовою організаційною інфраструктурою, а також розподіленим типовим ЄІП (з виділенням головного офісу та територіально розподілених підрозділів) сучасних установ;

- типовий ЦІУМБ забезпечення рішення динамічно змінного набору управлінських та інформаційно-аналітичних завдань у рамках управління мережевою безпекою типової ІТКМ;

- типовий ЦІУМБ є системоутворюючим технічним та організаційним компонентом ПУІБ для типового ЄІП установи в межах її СЗІБ;

- типовий ЦІУМБ як спеціалізований структурний елемент, вбудований у типову ІТКМ, максимально можливою мірою відповідає вимозі технічної незалежності від ІТКМ для забезпечення власної захищеності;

- типовий ЦІУМБ створюється та еволюційно розвивається поетапно протягом усього його життєвого циклу, який включає традиційні стадії аналізу, проектування, розробку, тестування та інтеграції, впровадження, супроводу та розвитку. Еволюційність розвитку типового ЦІУМБ та його компонентів тут означає можливість адаптації до розширених вимог щодо забезпечення ІБ для типової ІТКМ та її користувачів, а також впровадження більш досконалих ІКТ, сучасних відмовостійких обчислювальних платформ та мережевого обладнання, програмних засобів, ОС, СУБД та ін.

Вищеописані дії у відповідності до розробленої методології побудови типового ЦІУМБ добре узгоджуються щодо СУІБ із замкнутим циклом PDCA:

планування (розробка) - здійснення (впровадження та забезпечення функціонування) – перевірка (проведення моніторингу та аналізу) – дія (підтримка та покращення).

1.2 Цілі функціонування типового Центру інтелектуального управління мережевої безпеки

Основними типовими цілями функціонування типового ЦІУМБ в установі можуть бути, наприклад, такі:

- забезпечення функціональної стійкості та надійності телекомунікаційної складової ІТКМ за рахунок максимально можливої автоматизації ПУІБ;

- забезпечення виявлення аномалій, порушень (актів незаконного втручання), комп'ютерних атак та інцидентів ІБ на ранніх стадіях на основі застосування ІБ-аналітики до всіх даних, пов'язаних з ІБ та подіями ІБ в ІТКМ;

- забезпечення зменшення шкоди від порушень ІБ та інцидентів ІБ в ІТКМ за рахунок скорочення часу реагування на них та попередження їх появи у майбутньому;

- консолідація та захист пов'язаних з ІБ ІТКМ даних з гетерогенних джерел та оперативне надання уповноваженим особам інформації для розслідування порушень ІБ та інцидентів ІБ в ІТКМ;

- надання інформації про значні інциденти ІБ та порушення ІБ в ІТКМ з метою своєчасного інформування уповноважених органів та заінтересованих організацій відповідно до встановленої форми та у встановлений для цього час.

Для досягнення сформульованих цілей, розширення автономності управління інцидентами ІБ в рамках однієї установи та поглиблення знань про рівень ІБ її ІТКМ подальше викладення результатів проведеного дослідження спрямоване на об'єднання всіх переваг Центру ІБ та мережевого операційного центру (МОЦ) з їх унікальними та спільно застосовними інструментальними засобами управління мережею та її мережевою безпекою.

1.3 Мережевий операційний центр

Аналіз міжнародної та вітчизняної практики створення МОЦ показує, що вони, як правило, належать великим організаціям. Перші такі центри з'явився в США в 1960-х роках, наприклад, Центр управління мережею в AT&T, відомий з 1962 і змінив назву на МОЦ в 1977 р.

Головна мета МОЦ полягає у створенні та підтримці централізованого підрозділу установи, на основі якого персонал МОЦ може цілодобово вирішувати поточні питання управління функціонуванням ІТКМ для забезпечення безперебійної роботи мереж передачі даних, систем зберігання, обчислювальних ресурсів, послуг і т.п. Це передбачає можливість віддалено спостерігати, підтримувати та здійснювати контроль (моніторинг, діагностику) телекомунікаційної мережі ІТКМ за допомогою всього необхідного ПЗ та АТ для управління її оптимальним функціонуванням для різних платформ, середовищ та каналів зв'язку, а також візуалізувати докладну інформацію про детальний стан усіх пристроїв, за якими ведеться спостереження. Значно спрощуючи роль МОЦ, можна зробити висновок, що він досягає своєї мети, виконуючи ряд перевірок та процедур відновлення для критичних підмереж, пристроїв, додатків, даних і, зрештою, всієї ІТКМ. Ці центри можуть розглядатися як координаційні центри, що підтримують наступні типові види діяльності персоналу МОЦ:

— дослідження, проведення різних оцінок, управління та постійна підтримка високої доступності телекомунікаційних мереж та пристроїв за рахунок аналізу основних параметрів внутрішньомережевого трафіку, що називається «телеметрією» (від давньо-грецького τῆλε «далеко» + μέτρεω - «вимірюю»);

- цілодобовий контроль та моніторинг продуктивності мережевої інфраструктури та всіх компонентів мережі, включаючи телекомунікаційні пристрої, виділені лінії зв'язку, міжнародні канали, канали доступу в інтернет, обладнання маршрутизації, сервери, віртуальні машини тощо;

- планування виробничої потужності установи;

- постійне дослідження та контроль виникаючих проблем та аномалій (наприклад, виявлення відключень та збоїв у мережі електроживлення, виявлення помилок із втратою фреймів або бітів при передачі даних каналами зв'язку, виявлення помилок у рядках програмного коду, виявлення виходу з ладу каналів зв'язку та інші питання, які можуть вказувати на проблеми з працездатністю мереж), ізоляція проблем, визначення їх характеру та причин виникнення, вироблення рекомендації щодо усунення проблем, доставка попереджень правильному персоналу, виділення ресурсів, координація дії щодо їх вирішення, автоматична ескалація нагальних проблем, підготовка звітності, внесення інформації про проблеми в єдину БД тощо;

- управління доменними іменами;

- керування конфігураціями пристроїв та версіями (релізами) ПЗ;

- управління сховищами даних;

- керування електронною поштою та голосовим та відеотрафіком;

- управління підтримкою кінцевих користувачів та ін;

- адміністрування та резервне копіювання систем та даних;

- управління оптимізацією та якістю обслуговування, запобігання деградації послуг, підготовка відповідної звітності;

- встановлення, розповсюдження, усунення несправностей та оновлення прикладного ПЗ;

- координація доступу до/з афілійованих мереж (наприклад, бізнес-партнерів);

- застосування політик та вимог SLA;

- робота з основними (найпростішими) засобами управління ІБ, такими як автентифікації та авторизації, фільтрація IP- та MAC-адрес тощо.

Для досягнення найбільшої продуктивності персонал МОЦ зазвичай поділений на декілька груп – служба технічної підтримки (англ. Help Desk), перша лінія підтримки (англ. First Level Operations), друга лінія підтримки (англ. Second Level Operations) тощо. У кожній групі працюють профільні спеціалісти

необхідної кваліфікації, для яких чітко регламентовані дії та зони відповідальності.

Як видно з наведеного опису, за своєю суттю МОЦ працює з даними про стан мережі та її окремих елементів, що схоже на функціонування ЦІБ з тією відмінністю, що останній має справу лише з даними про події ІБ.

Для більшої наочності порівняльний аналіз характеристик ЦІБ та МОЦ, узагальнюючий результати, наведено в таблиці 1.1 [28], яка необхідна для розуміння і формулювання функціональних можливостей ЦІУМБ [29].

1.4 Функціональні можливості об'єднаного типового Центру інтелектуального управління мережевою безпекою

У даному дослідженні пропонується створити об'єднаний ЦІУМБ, який поєднує у собі всю специфіку та переваги Центру ІБ та МОЦ. Обидва ці центри призначені для виявлення, розслідування, встановлення пріоритетів, ескалації та вирішення проблем, але при цьому типи проблем та області їх дії значно різняться, що при об'єднанні дозволяє отримати якісно нову, більш функціональну структуру - ЦІУМБ. Його головна мета – надати установі керовану на основі інтелекту мережну безпеку ІТКМ, що дасть можливість випереджати проблеми в області ІБ за рахунок як можна тіснішої інтеграції з усіма бізнес-процесами в установі .

Створення ЦІУМБ об'єктивно можливе тому, що реалізація основних функцій Центру ІБ і МОЦ часто організована схожим чином - з багаторівневим підходом, аналогічними ролями на перших лініях підтримки та можливим спільним використанням деяких інструментальних засобів на технічному рівні. Об'єднання двох центрів в один єдиний вигідний і в довгостроковій перспективі, оскільки головним завданням МОЦ є обслуговування основної діяльності установи, тоді як Центру ІБ покликаний забезпечити її ІБ. Так, наприклад, при виявленні збою персонал МОЦ, швидше за все, пояснить його збоєм функціонування пристрою або системи та спробує усунути шляхом заміни

обладнання або зміни конфігураційних налаштувань. Персонал Центру ІБ може пов'язати проблему з вірусною активністю та швидше за все почне самостійне розслідування, перш ніж ініціює більш складні події у відповідь цю подію ІБ.

Таблиця 1.1 – Порівняльний аналіз характеристик МОЦ та Центру ІБ

Параметр	МОЦ	Центр ІБ
1	2	3
Область дії	Використовується для вирішення завдань, пов'язаних з управлінням, моніторингом та контролем ІТКМ.	Відстежує загрози ІБ для всіх елементів ІТКМ (в першу чергу її інформаційних активів), які намагаються використати вразливості та проникнути всередину ІТКМ.
Ключова роль	Протистояти загрозам для інфраструктури ІТКМ, постійно знаючи про її поточний стан, дотримуючись SLA і керуючи інцидентами для досягнення максимального часу безперебійної / безвідмовної роботи.	Протистояти загрозам ІБ для інформаційних активів ІТКМ, захищаючи комерційну таємницю, інтелектуальну власність, дані користувачів тощо.
Ціль	Відстежувати продуктивність ІТКМ, усувати несправності обладнання, сповіщати про порушення продуктивності та усувати проблеми з продуктивністю в першу чергу з точки зору забезпечення доступності та скорочення часу простою, а також покращення географічного покриття.	Відстежувати збереження всіх властивостей ІБ для інформаційних активів ІТКМ та якість надання послуг ІТКМ, а також швидке реагування при його погіршенні та інцидентах ІБ, які впливають на користувачів ІТКМ та її активи, з метою скорочення потенційних втрат від інцидентів ІБ та підвищення ступеня задоволеності споживачів.

1	2	3
Вплив на бізнес	Операційний рівень.	Стратегічний рівень, облік злиття технічних проблем з людським фактором.
Природа джерел вирішуваних проблем	Природні прогнозовані і передбачувані системні події, що відбуваються з пристроями.	В першу чергу «розумні», часто непередбачувані противники - порушники ІБ, а потім інші джерела загроз ІБ.
Технології, які використовуються при функціонуванні	Реактивний підхід, доступ до даних у режимі реального часу, інтерактивні інформаційні панелі, які відображають показники продуктивності, технологія автоматичного оповіщення про порушення продуктивності, аварійні сигнали.	Запобіжний підхід, доступ до даних, включаючи історичні, в режимі реального часу, складні інтерактивні інформаційні панелі, технологія прогнозування для раннього оповіщення про потенційні проблеми, які впливають на бізнес.
Засоби	Системи керування елементами, ПЗ для усунення несправностей, інструменти для реєстрації несправностей, ПЗ для моніторингу продуктивності.	МЕ, САЗ, СОВ/СПВ та інші СЗІ, SIEM- і SOAR-системи, ПЗ для визначення якості послуг тощо.
Приклади метрик	Моніторинг ключових показників ефективності мережі, таких як втрата відеопакетів та втрата викликів.	Кількість відбитих мережевих атак, кількість виявлених у режимі реального часу інцидентів ІБ, кількість виявлених на кінцевих пристроях комп'ютерних вірусів.
Супровід	Базується в одному або декількох місцях, розмір штату зазвичай від 80 до 500+ спеціалістів.	10-100 спеціалістів.
Навички, які вимагаються від персоналу	Мережева інфраструктура, обслуговування мереж, усунення несправностей, ІТ, системна інженерія, підтримка додатків та аналітика даних.	ІБ, мережна безпека, управління та інфраструктура ІБ, оцінка ризиків ІБ, моделювання сервісів, ІБ-аналітика та інтерпретація даних.

На додаток до ручного контролю ІТКМ, що все ще залишається, ЦІУМБ надає можливості автоматизованого моніторингу ПЗ та АО та дослідження першопричин подій ІБ для подальшого визначення характерних тенденцій, що виникають при обробці, зберіганні та передачі даних в ІТКМ, а також здатний виконувати завдання управління контролем доступу, відображення та запобігання вторгнень та розширеного аналізу загроз ІБ.

Переглядаючи всю ІТКМ у конкретному контексті діяльності установи, ЦІУМБ розуміє, як організована мережа та як по ній переміщуються інформаційні потоки. Отримуючи журнал реєстрації подій (ЖРП) від серверів, БД, ПЗ, веб-сайтів, СЗІ, кінцевих точок (комп'ютерів та інших) пристроїв, що використовуються користувачами), він керує доставкою зібраної інформації до SIEM-системи для аналізу та зіставлення з відомими загрозами ІБ та виявлення проблем. У такому ЦІУМБ більш результативно здійснюється пошук незвичайної та підозрілої поведінки користувачів, систем та кінцевих точок, збирання свідчень інцидентів ІБ та «полювання за погрозами».

Отже, ЦІУМБ отримує потужну синергію Центру ІБ та МОЦ за рахунок тісного співробітництва їх персоналу та спільного використання застосовуваних у них інструментальних засобів та технологій. У результаті одержуваними функціональними можливостями об'єднаного ЦІУМБ для їхніх організацій-власників є такі:

- централізоване управління ЦІУМБ як в частині функцій, виконуваних Центром ІБ, так і МОЦ, з відображенням у «єдиному вікні», призначеному для адміністрування та прийняття рішень;

- повна ситуаційна поінформованість із «безшовною» інтеграцією та комплексним відстеженням контрольованих об'єктів та процесів ІТКМ (зі створенням та веденням єдиної БД активів) та послуг ІБ-аналітики з підтримуючою інфраструктурою, включаючи моніторинг та СЗІ;

- моніторинг ІТКМ та її ІБ в режимі реального часу, інтегрований з вимогами по забезпеченню ІБ та включає автоматизований контроль за продуктивністю та доступністю ІТКМ та всіх її елементів, оповіщення та

повідомлення (на основі протоколів управління мережею), стандартні клієнт/серверні протоколи, звітність про виконання вимог SLA, інтегровану службу технічної підтримки (Help Desk) тощо;

- централізоване управління та аудит конфігураційних налаштувань мережевих пристроїв та СЗІ, БД, архівів тощо, включаючи їх зміни, що відображаються у прив'язці до зміни заходів забезпечення ІБ та порушення базових налаштувань, а також повну історію їх зміни тощо;

- керування змінами мережевих пристроїв разом із процесом автоматичного затвердження, вказівкою посилання на шаблон налаштування, перевіркою управління змінами, журналом історії;

- автоматизований збір даних, включаючи збір подій та потоків, агрегування та кореляцію за допомогою автоматизації та розширеної (як з погляду мережі, так і ІБ) аналітики з метою отримання максимальної користі з величезної кількості даних з ІБ, доступних ЦІУМБ;

- моніторинг всієї мережевої активності, що зв'язується з об'єктами, а не IP-адресами;

- пріоритизація попереджень про небезпеку від СЗІ відповідно до найбільш ймовірних подій, які можуть призвести до найбільш негативних наслідків;

- вилучення більшого інтелектуального контексту в масштабах всього ЄІП установи, що допомагає їй у прийнятті оперативних та стратегічних рішень у області ІБ та перевірки того, що в неї є правильна політика ІБ;

- можливість надавати, записувати та часто оновлювати метадані для кожної виявленої події/інциденту ІБ для його рекурсивного аналізу під час реагування на інцидент ІБ. Такі метадані важливі для ІБ-аналітики, щоб звести до мінімуму «шум» даних та диференціювати події ІБ та інциденти ІБ один від одного;

- швидше виявлення подій ІБ і скорочення часу реагування на інциденти ІБ за допомогою того, що автоматичне усунення помилок, оновлення та активізація заходів забезпечення ІБ працюють спільно для досягнення спільних

цілей, але при цьому Центр ІБ та МОЦ надають свої спеціалізовані функції, навички та досвід, доповнюючи один одного;

- розширене розслідування інцидентів ІБ в ІТКМ, що включає збереження всього трафіку, реконструкцію пакетів, відновлення сеансів користувачів, інтеграцію з реагуванням на інциденти ІБ тощо;

- поліпшене планування та реалізація заходів забезпечення ІБ при спільній відповідності за ідентифікацію та усунення причин виникнення інцидентів ІБ;

- дієве та раціональне управління інцидентами ІБ (включаючи аналітику поведінки при безперервному моніторингу, попередній та подальший аналіз) і розширену звітність із цінними результатами;

- централізована керуюча консоль з інформаційними панелями та звітами, що дозволяє керувати ризиками ІБ і дотримуватися вимог відповідності, яка також відображає топологію ІТКМ і візуалізує інформаційні потоки в ній;

- регулярний аудит ІБ ІТКМ і проведення різних оцінок, що піддаються вимірюванню характеристик з наданням звітів і узагальнюючих оглядів з заздалегідь визначеними метриками ІБ;

- поліпшений обмін інформацією (комунікації) з попередньо ескалацією та результативним спільним використанням синтезованих знань для підвищення обізнаності про ситуацію та координацію реагування;

- вимірювання ключових показників ефективності (англ. Key Performance Indicators, KPI) на основі контролю продуктивності і помилкових позитивних і негативних спрацювань, зниження співвідношення «сигнал/шум» для подій ІБ;

- облік та відстеження інтенсивності споживання користувачами ресурсів та послуг ЦІУМБ.

На основі цілей та отримуваних результатів функціонування можна зробити висновок, що для ЦІУМБ як об'єднання Центру ІБ та МОЦ існує чотири ключові бізнес-процеси:

1) моніторинг, аудит та оцінка мережевої безпеки;

2) класифікація та сортування подій у ІТКМ;

3) пріоритизація, аналіз та прогнозування подій в ІТКМ;

4) виправлення проблем, пов'язаних із цими подіями, та відновлення після них.

Іншими групами бізнес-процесів є процеси управління ЦІУМБ, процеси вимірювання, аналізу та вдосконалення функціонування ЦІУМБ, а також допоміжні процеси, які забезпечують здійснення ключових бізнес-процесів.

Чим більш інтегрованою та автоматизованою буде взаємодія Центру ІБ та МОЦ, тим більш результативним буде функціонування ЦІУМБ. Знову образно кажучи, ЦІУМБ – це «швидкий мозок забезпечення адаптивної попереджувальної мережевої безпеки з широко відкритими очима та вмілими руками». Однак операційні моделі та процеси тільки провідних організацій є досить зрілими для підтримки цієї розширеної сумісної моделі запобіжного управління інцидентами ІБ для ІТКМ, побудованого на архітектурі ІБ-аналітики великих даних, що стосуються ІБ.

1.5 Візуалізація інформації в типовому Центрі інтелектуального управління мережевою безпекою для прийняття рішень щодо управління інцидентами інформаційної безпеки в інформаційно-телекомунікаційній мережі

Візуалізація вже давно стала популярним і наочним засобом виявлення та вирішення проблем, що виникають в галузі управління ІБ. Візуалізація інформації про ІБ ІТКМ установи в ЦІУМБ має надавати якісь абстрактні дані про стан захищеності всіх об'єктів захисту ІТКМ, якщо порівнювати її з візуалізацією фізично існуючих явищ або даних (наприклад, людського тіла, географічних карт, землетрусу, урагану, цунамі тощо). В реальності найчастіше не існує тих об'єктів, які підлягають умовному відображенню на екрані монітора співробітника ЦІУМБ. Наприклад, досить складно уявити собі низькорівневу інформацію про мережу або інформацію, отриману від окремого мережевого пристрою, для виявлення подій ІБ у вигляді атак, що відбулися, або спроб атак на обладнання або окремий сервер ІТКМ, які тільки розвиваються на очах адміністратора або аналітика ІБ.

Інформація про ІБ ІТКМ, що підлягає візуалізації в ЦІУМБ, може бути використана для безпосереднього аналізу, виявлення подій ІБ в потоці всіх зібраних подій, прийняття рішень в галузі управління ІБ та ознайомлення з цією інформацією певного кола уповноважених осіб. Наприклад, при вирішенні наступних важливих завдань захисту ІТКМ від комп'ютерних атак із зовнішніх мереж типу інтернету або зловживання дітей з боку інсайдерів установи:

- трасування переміщення мережевих пакетів каналами зв'язку між хостами в ІТКМ;

- аналіз інформаційних потоків та виявлення несанкціонованих (шахрайських) операцій з інформацією;

- результати контролю доступу до всіх ресурсів ІТКМ (включаючи обладнання, приклади, БД, сервери, файли тощо);

- результати контролю системних конфігурацій та конфігураційних налаштувань АТ та СЗІ ІТКМ та їх відповідності встановленим вимогам (політикам);

- розпізнавання віддалених мережевих атак;

- знаходження шляхів поширення комп'ютерних вірусів і черв'яків або функціонування так званих заражених ботнетів (від англ. robot networks or botnets), які зазвичай використовуються для зловмисної діяльності - розсилки спаму та вірусів, розподіленого підбору паролів на віддалених комп'ютерах, запуску DoS-атак тощо;

- дослідження коду шкідливих програм або комп'ютерних вірусів;

- результати кореляції виявлених подій ІБ і «зріз» подій ІБ для виділеного каналу зв'язку, мережевого пристрою, мережевого протоколу, сервісу, додатку тощо;

- результати зіставлення подій ІБ з результатами аналізу вразливостей елементів ІТКМ;

- показ повідомлень/попереджень і рекомендацій щодо усунення проблем із забезпеченням ІБ окремих елементів ІТКМ, що автоматично генеруються СЗІ;

- встановлення деяких ознак (наприклад, сигнатур мережевих атак);

- побудова моделей і розробка правил забезпечення ІБ (наприклад, для налаштування в МЕ);

- відображення тенденцій у зміні рівня ІБ та ризиків ІБ ІТКМ;

- візуалізація свідчень інцидентів ІБ для подальшого їх розслідування;

- виявлення аномальної активності та контроль неблагонадійних співробітників;

- аналіз правильності налаштувань СЗІ;

- результати виявлення вразливостей в елементах ІТКМ;

- результати інвентаризації (контролю складу) АТ, ПЗ та СЗІ, що застосовуються в ІТКМ;

- вивчення взаємодії при одночасному використанні різних технологій забезпечення ІБ та окремих СЗІ;

- навчання питань ІБ та підвищення обізнаності в галузі забезпечення ІБ працівників установи тощо.

Проаналізувавши основні завдання управління мережевою безпекою ІТКМ, можна зробити висновок, що візуалізація інформації про ІБ ІТКМ можлива з двох основних точок зору - узагальнено по всій ІТКМ або за окремими подіями ІБ.

У першому випадку об'єктами візуалізації до ЦІУМБ для прийняття рішень його персоналом може бути наступна узагальнена інформація про ІБ ІТКМ:

- показники захищеності ІТКМ в цілому та її окремих частин, включаючи ризики ІБ (за типами, наслідками, ймовірностями реалізації) та місця локалізації вразливостей;

- показники результативності роботи СЗІ за типами та місцями їх використання;

- статистичні дані щодо кількості подій та інцидентів ІБ за типами, критичністю, місцями виникнення тощо;

- визначення пріоритетних напрямів, що вимагають негайного втручання;

- статуси та поточні стани подій ІБ та інцидентів ІБ тощо.

Щодо окремої події ІБ має візуалізуватися інформація, що відповідає на такі питання:

- хто: суб'єкт доступу;

- чому: наприклад, мимовільна або ненавмисна дія (помилка), необізнаність, недбалість або безвідповідальність, зловмисні дії (зовнішні або внутрішні), внаслідок аварії;

- що: НСД до системи та/або інформації, несанкціонований вплив на ІС та/або проти ІТКМ або всієї установи, несанкціонована установка програм (без згоди власника), дистанційне порушення роботи ІС, створення стресових ситуацій, фізичне вторгнення або незаконна дія, незаконна діяльність в інтернеті (що завдає шкоди установі), різні людські помилки (в адмініструванні, обробці, програмуванні, сумісному використанні), поломка або несправність АТ, проблеми в навколишньому середовищі (що викликають недоступність компонентів ІС через стихійне лихо);

- як: для кожного вищезгаданого «що» можливість, список використовуваних методів та засобів – особливо для комп'ютерних атак;

- статус події ІБ: спроба, в стадії реалізації, успіх чи невдача порушення ІБ;

- яка при цьому використовувалася вразливість: у поведінці, ПЗ, конфігурації обладнання або ПЗ, загальний захист, архітектурі або процесах систем, фізичному матеріалі;

- на який тип активів (основних і пов'язаних з ними): БД та додатки (які знаходяться на периметрі, всередині ІТКМ установи, у спільній хмарі, на аутсорсингу), системи (які знаходяться на периметрі, всередині ІТКМ установи, у спільній хмарі, на аутсорсингу), мережі та телекомунікації (низькорівневі пристрої, високорівневі комунікації, проміжне ПЗ, бездротові пристрої, СЗІ), пристрої автономного зберігання (папір, електронні пристрої, магнітні та оптичні пристрої), пристрої кінцевого користування (ПЗ локального застосування – що належать користувачеві або установі, багатоцільові робочі станції, люди (працівник, бізнес-партнер, постачальники послуг з власним

обладнанням або без), засоби та довкілля (нерухомість, фізичні засоби або системи захисту, будівлі та приміщення, офісні меблі);

- які наслідки для властивостей інформації (порушення конфіденційності, цілісності, доступності, невідмовності тощо);

- які наслідки для бізнесу загалом: прямі чи непрямі.

Отримуючи перераховану інформацію на екрані монітора, наприклад, оператор ЦІУМБ оперативно відреагує на виявлені відхилення від штатного функціонування систем або передає цю проблему на наступний рівень ескалації, а аналітик ІБ виділяє якісь тенденції і далі враховує їх у описі нової атаки і, зрештою, вибирає запобіжну стратегію захисту окремого елемента ІТКМ [30].

2 АРХІТЕКТУРА ЦЕНТРУ ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ МЕРЕЖЕВОЮ БЕЗПЕКОЮ

2.1 Функціональна архітектура типового Центру інтелектуального управління мережевою безпекою

Інфраструктура типового ЦІУМБ установи повинна будуватися по ієрархічному принципу і являє собою спеціалізований комплекс сучасних організаційних, технічних, апаратно-програмних, технологічних та інших заходів та засобів, який забезпечує ІБ ІТКМ та самого ЦІУМБ на всіх стадіях їх життєвого циклу. З одного боку, типовий ЦІУМБ інтегрований з ІТКМ для отримання всіх даних, які належать до ІБ для їх детального аналізу та створення захищеного ЄІП установи, а, з іншого боку, типовий ЦІУМБ розрахований на обслуговування своїх функціональних систем (підсистем) за допомогою створення своєї виділеної транспортної мережі з використанням ресурсів та послуг, що надаються лише всередині ЦІУМБ, які при цьому тим чи іншим способом інтегруються між собою.

Програмно-технічна взаємодія типового ЦІУМБ з типовою ІТКМ та іншими зовнішніми системами та джерелами інформації (наприклад, Threat Intelligence) повинно здійснюватися на основі стандартних або спеціальних уніфікованих протоколів і стандартів та підтримуватись на рівні додатків та інформаційного обміну з урахуванням прийнятих вимог. Створення індивідуальних протоколів взаємодії з кожною з таких систем недоцільно, бо це серйозно суперечитиме вимогам уніфікації.

Керуючись найкращими практиками побудови інфраструктур для складних мережевих систем з погляду виконуваних на їх основі бізнес-операцій та впорядкування процесів та заходів забезпечення ІБ, для типового ЦІУМБ можна виділити п'ять функціональних інфраструктурних рівнів – рівні платформ, ПЗ, надання послуг, доступу та управління (рисунок 2.1).

Рівень платформи надає множину базових «будівельних блоків» для наступного рівня ПЗ і включає мережну інфраструктуру, сховища даних, ЗОТ,

засоби резервного копіювання, засоби віртуалізації, обчислювальні засоби тощо. На цьому рівні перебувають і внутрішні послуги цих платформ, відповідальні за управління, наприклад, пам'яттю, процесами та зв’язками, міжпроцесною взаємодією, подіями, помилками і винятковими ситуаціями, часом, логічним ім'ям ресурсів, пристроями, файловими системами, конфігуруванням систем, послуги обробки транзакцій, обміну даними, друку та багато іншого.

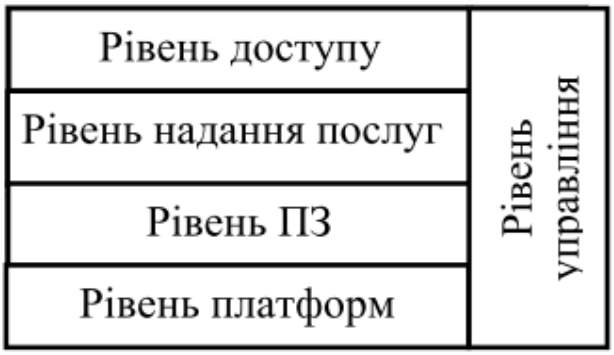

Рисунок 2.1 – Багаторівнева функціональна інфраструктура типового ЦІУМБ

Рівень ПЗ містить прикладне ПЗ, яке підтримує всю діяльність ЦІУМБ в рамках ПУІБ та використовує послуги додатків, що знаходяться на рівні платформ.

Рівень платформ спільно з рівнем ПЗ є системотворчою основою ЦІУМБ із погляду застосування ІКТ.

Рівень надання послуг забезпечує можливість здійснювати ті дії по управлінню послугами ЦІУМБ, які вимагають введення вхідних даних та взаємодії з власниками послуг та власниками установи. Елементи цього рівня також відповідають за перетворення вимог до управління ІБ у вигляд, придатний для подальшого використання при виконанні різних технологічних та операційних дій (такі як оптимізація обслуговування, життєвий цикл послуг, робота з каталогами, робота з автоматизованими бізнес-процесами ЦІУМБ тощо). Цей рівень відбиває специфіку діяльності ЦІУМБ, що здійснюється із застосуванням ІКТ.

Рівень доступу пов'язаний із рівнями надання послуг та управління. На рівні доступу послуги ЦІУМБ та її кінцеві користувачі підключаються до ЦІУМБ. Цей рівень дозволяє управляти та підтримувати доступ до ЦІУМБ з єдиної точки, використовуючи комбінацію декількох сервісів на основі каналів ІКТ і вирішує проблеми доступу великої ємності, високої продуктивності та надійності пристроїв, підтримки протоколів тощо (наприклад, шляхом виконання балансування навантаження). На цьому рівні також знаходяться послуги людино-машинної взаємодії, включаючи сервіси командного, текстового та графічного користувацького інтерфейсів.

Рівень управління необхідний для оперативного управління ЦІУМБ з допомогою ІКТ. Він забезпечує набір засобів для рівнів управління платформами та ПЗ, необхідних для підтримки рівня надання послуг та експлуатаційних процесів, що здійснюються з допомогою ІКТ, а також для підтримки персоналу при вирішенні завдань управління доступністю, продуктивністю, мережами, послугами, установкою, налаштуванням, змінами, організацією зберігання даних, диспетчеризацією завдань, адмініструванням користувачів, моніторингом, коректним запуском та зупиненням систем, сервісами резервного копіювання та відновлення інформації, знаннями, проблемами, позаштатними ситуаціями, інцидентами, звітністю, системою друку, захистом даних тощо.

Всі ці рівні та взаємозв'язки між ними мають бути захищені відповідними заходами забезпечення ІБ. Отже, інфраструктура захищеного типового ЦІУМБ повинна відповідати вимогам забезпечення його ІБ з різних точок зору - АТ, ПЗ, технічної, організаційної тощо.

2.2 Зональна архітектура забезпечення інформаційної безпеки в Центрі інтелектуального управління мережевою безпекою

Побудова типового ЦІУМБ у вигляді вбудованої та невід'ємної частини типової ІТКМ установи, а також централізованої, багаторівневої системи на основі сучасних архітектур і рішень, передбачає розподіл обробки даних, що

відносяться до ІБ, з виділенням зон їх збору в ІТКМ та власне обробки – початкової в місцях збору в ІТКМ та остаточної із застосуванням ІБ-аналітики у типовому ЦІУМБ. Для виконання такий різноманітної трудомісткої роботи потрібна належна інфраструктура забезпечення власної ІБ ЦІУМБ, яка дозволяє захищеним чином збирати, нормалізувати, проводити категорування (наприклад, створення профілів користувачів, щоденного запуску ПЗ тощо) і агрегування, корелювати, аналізувати та здійснювати передачу всіх зв'язаних з ІБ даних та підтримувати надання відповідних послуг санкціонованоним групам користувачів.

Забезпечення ІБ типового ЦІУМБ у загальній постановці проблеми може бути досягнуто при взаємопов'язаному вирішенні двох завдань: захисту інформаційних ресурсів, що знаходяться в ЦІУМБ, і наданих ІТ-послуг від зовнішніх та внутрішніх загроз ІБ, та захисту зовнішнього середовища – ЄІП установи – від загроз ІБ із боку самого ЦІУМБ. Таким чином, виникає проблема системної ув'язки задач забезпечення ІБ типового ЦІУМБ з рештою завдань забезпечення ІБ ЄІП установи. Ця проблема має як науково-методологічні, так і організаційні аспекти і у своєму рішенні може базуватися на уніфікації та типізації рішень для забезпечення ІБ ЦІУМБ.

Типовий ЦІУМБ установи можна розглядати як формальну систему, що представляється такою четвіркою:

$$Z=<R_0, R_n, \mathrm{K}, \mathrm{U}>, \qquad (2.1)$$

де R_0 - вихідний стан ЦІУМБ, що захищається, і визначається наявними вихідними даними;

R_n – прогнозований стан ЦІУМБ, що відповідає його потенційним можливостям протистояти загрозам ІБ;

K – знання про ЦІУМБ як деяких елементарних і складних моделей, взаємозв'язки між ними, обмеження на окремі параметри тощо;

U - функція ефективності ЦІУМБ при забезпеченні ІБ ІТКМ, що розміряє результативність функціонування та витрати на його забезпечення.

Принциповим елементом розробленої методології побудови типового ЦІУМБ установи є побудова його адекватних моделей і процесів, що відбуваються в ньому. Основою вирішення цієї проблеми може бути узагальнена модель процесів забезпечення ІБ в ЦІУМБ (рисунок 2.2).

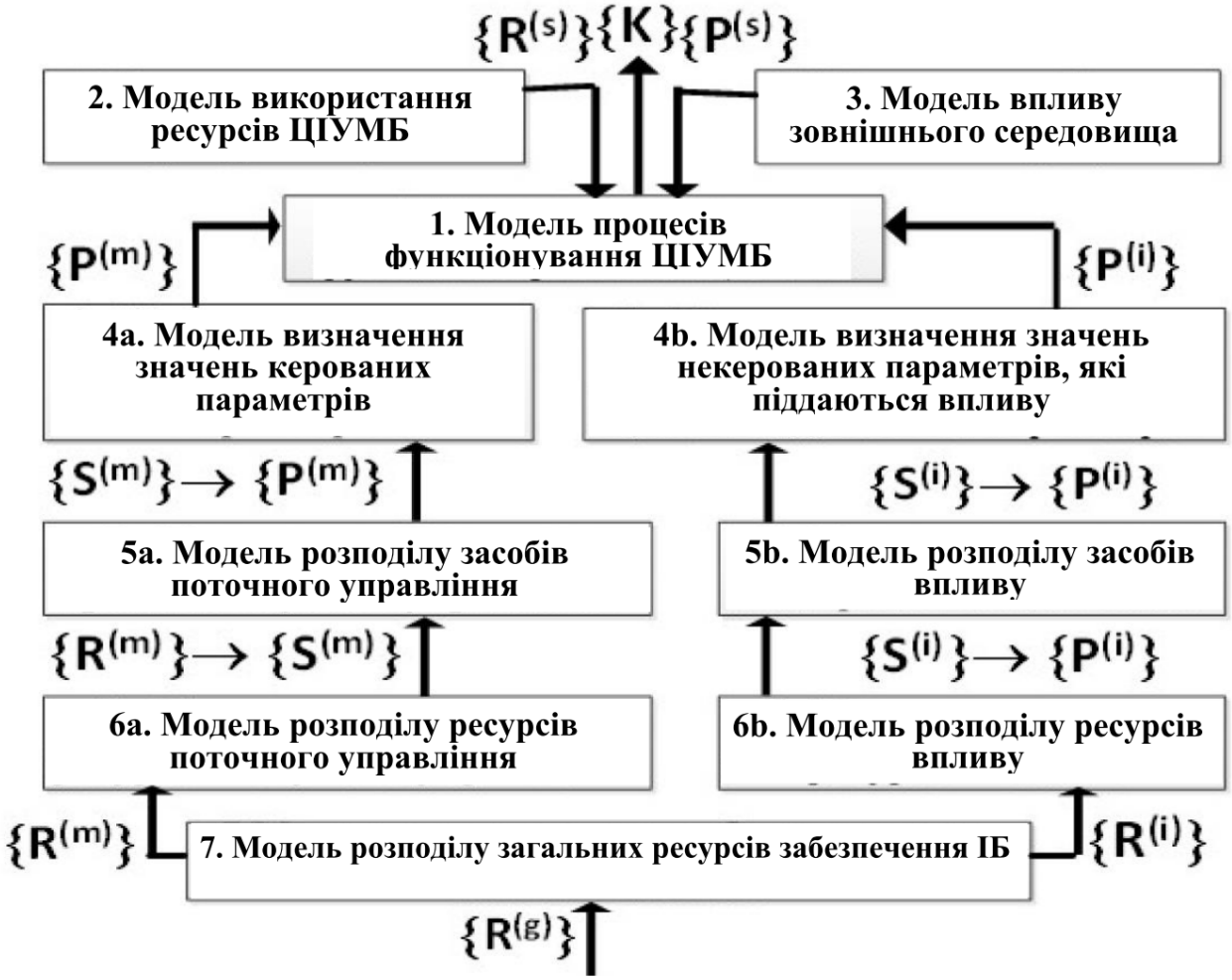

Рисунок 2.2 – Узагальнена модель процесів забезпечення ІБ в ЦІУМБ

Модель оперує такими параметрами:

- $\{K\}$ – множина показників інформаційної безпеки ЦІУМБ;

- $\{P^{(s)}\}$ - множина параметрів зовнішнього середовища, що впливають на функціонування ЦІУМБ;

- $\{R^{(s)}\}$ - множина ресурсів ЦІУМБ, що беруть участь в обробці інформації, що захищається;

- $\{P^{(m)}\}$ – множина внутрішніх параметрів ЦІУМБ, якими можна керувати безпосередньо у процесі обробки інформації, що захищається;

- $\{P^{(i)}\}$ – множина внутрішніх параметрів ЦІУМБ, які не піддаються безпосередньому управлінню, але піддаються впливу (наприклад, у процесі реорганізації або вдосконалення компонентів ЦІУМБ);

- $\{S^{(m)}\}$ і $\{R^{(m)}\}$ – множини засобів та ресурсів поточного управління;

- $\{S^{(i)}\}$ і $\{R^{(i)}\}$ - множини засобів та ресурсів впливу;

- $\{R^{(g)}\}$ - множина загальних ресурсів управління.

Для вирішення за допомогою цієї моделі задач аналізу, тобто визначення значень показників захищеності інформації у типовому ЦІУМБ, можна використовувати такий узагальнений вираз:

$$\{K\}=\mathrm{F}[\{P^{(m)}\}, \{P^{(i)}\}, \{R^{(s)}\}, \{P^{(s)}\}]. \qquad (2.2)$$

Завдання синтезу у загальному вигляді можуть бути наступні:

- знайти такі $\{R^{(m)}\}$ і $\{R^{(i)}\}$ при $(\{R^{(m)}\}+\{R^{(i)}\} \le \{\overline{R}^{(0)}\}$, де $\{\overline{R}^{(0)}\}$ – задані ресурси, щоб при заданих $\{R^{(s)}\}$ і $\{P^{(s)}\}$ виконувалася умова $\{K\}\to\max$;

— вибрати такі $\{R^{(m)}\}$ $\{R^{(i)}\}$, щоб при заданих величинах $\{R^{(s)}\}$ і $\{P^{(s)}\}$ умова $\{K\} \ge \{\overline{K}\}$, де $\{\overline{K}\}$ – заданий рівень захищеності, виконувалось при $\{R^{(0)}\}=\{R^{(m)}\}+\{R^{(i)}\}\to\min$.

Таким чином, завдання управління забезпеченням ІБ у типовому ЦІУМБ зводяться до оптимізації розподілу $\{R^{(m)}\}$, $\{S^{(m)}\}$, $\{R^{(i)}\}$, $\{S^{(i)}\}$.

Неважко бачити, що можливі такі модифікації узагальненої моделі:

- модель функціонування типового ЦІУМБ за відсутності управління забезпеченням ІБ (така модель дозволяє лише визначати значення показників захищеності інформації, тобто вирішувати завдання аналізу);

- модель поточного управління забезпеченням ІБ, основу якого становить оптимізація використання СЗІ, безпосередньо включених до складу типового ЦІУМБ;

- модель управління ресурсами, виділеними на забезпечення ІБ, яка додатково до попередніх завдань дозволяє оптимізувати процес формування засобів поточного управління забезпеченням ІБ;

- модель управління засобами впливу на параметри, що не допускають поточного управління, але які піддаються впливу;

- модель управління ресурсами, виділеними на розвиток типового ЦІУМБ;

- повна модель забезпечення ІБ типового ЦІУМБ, яка додатково до всіх можливостей, розглянутих вище, дозволяє оптимізувати використання всіх ресурсів, виділених на забезпечення його ІБ.

Результативність практичного використання даної моделі суттєво залежить від представницькості та адекватності вихідних даних, що дозволяють визначати функціональні залежності, які встановлюють взаємозв'язки показників захищеності інформації, параметрів СЗІ та розмірів ресурсів, що вкладаються у реалізацію процесів та заходів забезпечення ІБ. Тому ця модель може застосовуватися тільки в сукупності з неформальними методами аналізу та прогнозування.

Визначальними принципами розробки архітектури забезпечення ІБ типового ЦІУМБ є ізольованістю його внутрішніх систем і мереж від типової ІТКМ та жорстка регламентація доступу з постійним аналізом ресурсів та послуг ЦІУМБ, до яких було звернення. Такий підхід дозволяє працювати на випередження порушника ІБ та знижувати ризики ІБ до моменту реалізації.

Типовий ЦІУМБ як системоутворюючий елемент забезпечення ІБ може бути побудований відповідно до двох можливих варіантів: як вбудований в типову ІТКМ захищений ЦІУМБ або як окремо розміщений, що знаходиться на аутсорсингу, захищений ЦІУМБ. В обох випадках він повинен бути відкритим, гнучким, масштабованим тастійким з чітко визначеними, стандартизованими форматами вхідних та вихідних даних, високою продуктивністю та доступністю. І, щоб бути по-справжньому ефективним і захищеним, він повинен мати багаторівневий захист, постійно контролюватися і грамотно підтримуватися,

включаючи управління операціями, моніторинг продуктивності та доступності, керування відповідністю застосовуваним вимогам тощо.

2.3 Процес отримання знань Центром інтелектуального управління мережевою безпекою

Останні десятиліття дані організацій, що акумулюються у їх ІТКМ як основи ЄІП і які використовуються для більш якісного прийняття своєчасних та обґрунтованих вирішень для ефективної діяльності установи, ростуть надзвичайно швидко. Це великі обсяги даних про поточний стан їх мереж і, на перший погляд, незв'язані події, які відбуваються у них. Дані можуть надходити від різних серверів, контролерів доменів, СЗІ та характеризувати мережевий трафік, роботу засобів зв'язку, додатків та мережевих сервісів, дії кінцевих користувачів, веб-контент, передачу мультимедіа, геолокації, дані бізнес-процесів, внутрішні документи та аналітичні дані установи за багато років її існування. Всі дані, що стосуються ІБ ІТКМ установи, повинні належним чином збиратися, інтерпретуватися, зіставлятися та оцінюватися з погляду забезпечення ІБ. Таким чином, можна виділити чотири види різнорідних даних, з якими працюють системи ІБ-аналітики ЦІУМБ, типовими представниками яких є SIEM- та SOAR-системи:

1) дані, що знаходяться в окремих пристроях та СЗІ, додатках та БД;

2) дані, зібрані від окремих систем, додатків і т.д., що створюють інші дані, і поступаючі, наприклад, до інших БД, де вони зберігаються і обробляються без взаємодії із джерелом даних;

3) дані в потоках з такими унікальними характеристиками: величезний або, можливо, нескінченний об'єм, динамічно змінюються, входять і виходять у фіксованому порядку, вимагають швидкого (в режимі реального часу) відгуку тощо. Типові приклади включають різні види послідовних за часом даних і дані, отримані в динамічному мережевому середовищі, такі як мережевий трафік, дані

від телекомунікаційного обладнання, систем відеоспостереження, сенсорних мереж, потоки «кліків» на веб-сайтах, результати моніторингу ІБ тощо;

4) дані від різних бізнес-підрозділів установи, операційних груп, відділів тощо.

Основною особливістю цих даних є те, що вони представлені в різних форматах для різних цілей часто з різними політиками ІБ та вимогами відповідності та поступають у системи обробки ЦІУМБ у вигляді безперервних потоків великих даних, які вимагають негайної та швидкої обробки. При цьому дані можуть бути структурованими, слабоструктурованими і неструктурованими, що не дозволяє результативно управляти ними та обробляти традиційним чином. Крім цього, їх не слід розглядати як просте поєднання окремих елементів – навпаки, необхідно підтримувати фіксовані відношення кожного виконання та модифікації файлу, зміни реєстру, мережевого з'єднання, бінарного файлу, що виконується, в ІТКМ установи тощо.

Зазначені особливості притаманні для відомої проблеми великих даних (англ. Big data). Теоретичною основою ІТ великих даних став розділ інформатики, що отримав назву «наука про дані» (англ. data science), а критеріями, що визначають їхню відмінність від традиційних ІТ, є «три V»: volume – надвеликий обсяг даних, velocity – дуже висока швидкість передачі даних і variety – слабка структурованість даних, яка розуміється, перш за все, як нерегулярність структури даних та труднощі вилучення однорідних даних із потоку для подальшої кореляції. Пізніше до них додалися й інші критерії: veracity (достовірність), variability (мінливість), value (цінність), visibility (видимість). Може бути наступна інтерпретація поняття «великі дані»: масиви даних такого обсягу та структури, які перевищують можливості традиційних програмних інструментів (БД, ПЗ) зі збирання, зберігання та обробки даних за прийнятний час і тим більше перевищують можливості їхнього сприйняття людиною.

При управлінні мережевою безпекою чим більше в ЦІУМБ установи зібрано даних для аналізу, тим більш якісно можна встановити важливі

кореляції, зменшити кількість помилкових спрацьовувань і підвищити довіру до виявлених порушень ІБ та, зрештою, скоротити середній час реагування на інциденти ІБ. Тоді ІТ великих даних у типовому ЦІУМБ можуть застосовуватися переважно з двома цілями:

1) надання цих технологій як послуги при реалізації інших ІТ (зокрема, технології пошуку та аналізу даних для виявлення прихованих шаблонів) і як первинних джерел пошуку інформації та отримання основного змісту (семантики) в надвеликих масивах документів без їхнього безпосереднього читання людиною тощо;

2) власне ІБ-аналітика для ІТКМ з метою виявлення аномалій у функціонуванні систем, інцидентів ІБ, запобігання вторгнень тощо, яка включає три важливі дії:

- збирати: отримувати мільйони подій за секунду, частина з яких після обробки буде розглядатися як інциденти ІБ;

- приймати рішення, засноване на даних, по кожній події, яка потенційно впливає на ІБ ІТКМ;

- аналізувати в режимі реального часу: запускати автоматизований аналіз та забезпечувати видимість виявлених тенденцій щодо подій, уразливостей, загрозам ІБ тощо.

Відомо три типи обробки великих даних, всі з яких застосовні для використання у типовому ЦІУМБ:

1) пакетна обробка (англ. batch processing) в псевдореальному або «м'якому» реальному часі, коли обробці піддаються дані, вже збережені в енергонезалежній пам'яті, а імовірнісно-часові характеристики процесу перетворення даних в основному визначаються вимогами прикладних завдань;

2) потокова обробка (англ. stream processing) у «жорсткому» реальному часі, коли обробці піддаються дані, що знаходяться в оперативній пам'яті, без збереження на енергонозалежних носіях, а імовірнісно-часові характеристики процесу перетворення даних переважно визначаються темпом надходження даних, оскільки поява черг на обробних вузлах призводить до безповоротної

втрати даних. Прикладами є дані від смарт-камер відеоспостереження або мережевий трафік. Тут потрібна потокова система та сховище даних, здатні передавати та обробляти дані про події зі швидкістю їх надходження;

3) гібридна обробка, що використовує гібридну модель (відому як «Лямбда архітектура») з трьома архітектурними принципами: надійність (система має бути в стані управляти АТ, ПЗ та людськими помилками), незмінність даних («сирі» дані зберігаються завжди, і вони ніколи не змінюються) та повторюваність (результати завжди можна отримати обчисленням (повторним обчисленням) зі збережених вихідних даних), та чотирирівневою архітектурою: пакетний рівень (містить незмінний, постійно зростаючий майстер-набір даних, що зберігається в розподіленій файловій системі, і обробляє пакет, виходячи з цих вихідних даних), рівень сервісів (завантажує та надає нові пакети у сховище даних для подальшого виконання запитів), рівень швидкості (має справу тільки з новими даними і компенсує високу латентність рівня сервісу та опрацьовує нові пакети в режимі реального часу) і рівень комбінування (для синхронізації, об'єднання результатів та інших нетривіальних дій).

ІТ великих даних відносяться до «дата-центрованих» або «керованих даних» (англ. data-centric, data-driven). Якщо в традиційних ІТ в центр процесу обробки даних ставиться обробний пристрій або середовище (комп'ютер, кластер, хмарне середовище), які обробляли запити (заявки тощо), то великі дані розглядаються насамперед як безперервно «поточна» субстанція, методики обробки якої мають бути вбудовані в потоки. При цьому швидкість прийому даних, що знову надходять в обробку, і швидкість видачі результатів повинні бути не нижчі швидкості потоку, в іншому випадку це приводило б до нескінченного зростання черг або марного зберігання необроблених даних, обсяг яких нескінченно збільшується.

Сформулюємо важливі характеристики великих даних, які добре узгоджуються з вимогами до типового ЦІУМБ установи:

- бути своєчасними: дані повинні бути актуальними і відображати поточний рівень ІБ ІТКМ, загрози ІБ, уразливості, заходи забезпечення ІБ, а

також, у разі необхідності, до основних даних у встановленому порядку можуть бути додані історичні дані;

- бути всеосяжними: дані повинні бути зібрані воєдино, щоб відображати повну картину, гнучко інтегровані і легко перероблені в корисну та значиму інформацію – щоб негайно допомогти у забезпечення ІБ ІТКМ установи;

- бути адаптованими: дані повинні бути адаптовані до досягнення конкретної задачі в рамках загальної мети забезпечення ІБ ІТКМ;

- бути точними: дані мають бути коректними та отриманими від надійного (довіреного) джерела в ІТКМ;

- бути релевантними: дані повинні бути значущими і застосовними для подальшого використання.

В цілому, обробка великих даних, що стосуються ІБ, у типовому ЦІУМБ спрямована на «видобуток» нових даних (англ. data mining) – отримання (витяг) знань із великих обсягів даних. Це поняття є мультидисциплінарним, що поєднує бази і сховища даних, машинне навчання, високопродуктивні обчислення, розпізнавання образів, нейронні мережі, візуалізацію даних, пошук інформації, обробку зображень та сигналів, просторовий або часовий аналіз даних, статистичні методи тощо, що й інтегровано до ІБ-аналітики. Її завдання в даному контексті можуть бути класифіковані як описові, що характеризують загальні властивості великих даних, що стосуються ІБ, так і передбачувальні, що роблять висновок про поточні дані для складання прогнозів розвитку ситуації із забезпеченням ІБ ІТКМ установи.

Процес отримання знань про ІБ ІТКМ установи в типовому ЦІУМБ складається з послідовності кроків, поданих на рисунку 2.3, частина з яких може ітераційно повторюватися. Зокрема:

- крок 1: «Очищення» (англ. cleaning) даних, коли «шум» (що не стосується справи) і суперечливі дані видаляються із зібраних з гетерогенних джерел в ІТКМ для наступного аналізу. Дані для очищення надходять з реляційних, об'єктно-орієнтованих, ієрархічних, мультимедійних, мережевих та інших БД, сховищ даних та інформації (об'єднане фізичне або логічне сховище,

організоване в рамках єдиної схеми в одному місці), електронних таблиць, файлових систем, зовнішніх джерел типу Threat Intelligence тощо;

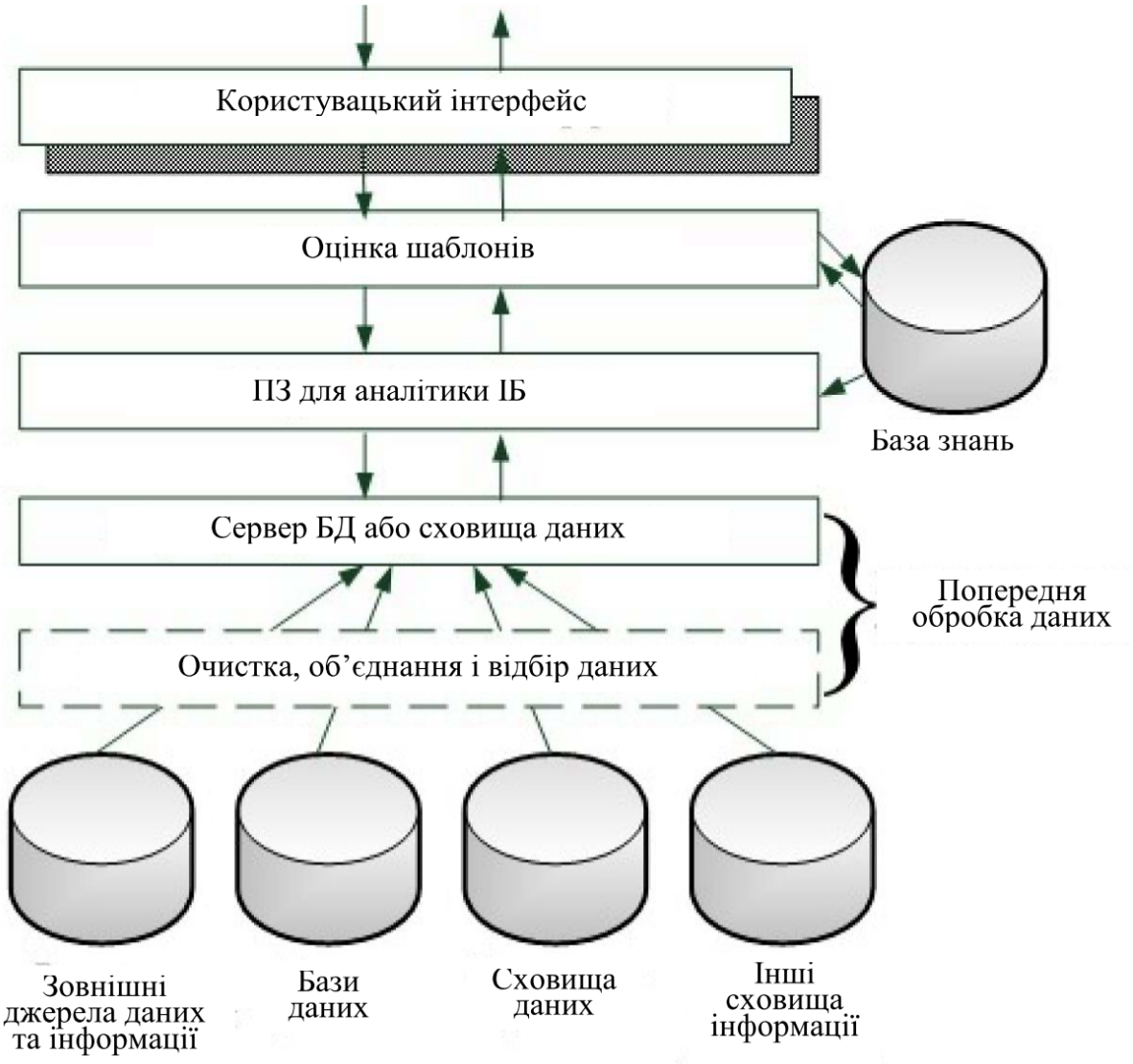

Рисунок 2.3 – Схема процесу отримання знань про ІБ ІТКМ для ЦІУМБ

- крок 2: об'єднання даних для подальшого інтелектуального аналізу на єдину БД;

- крок 3: відбір даних для вирішення конкретного завдання ІБ-аналітики, що дозволяє створити менший за розмірами обсяг аналізованих даних із збереженням цілісності вихідних даних;

- крок 4: перетворення на СУБД або сховище відібраних даних або їх об'єднання на основі певних форматів, що підходять для ІБ-аналітики. Так, наприклад, технологія сховищ даних включає аналітичну онлайн-обробку даних

(англ. Online Analytical Processing, OLAP), в тому числі можливості для реферування, консолідації, агрегування, складних аналітичних розрахунків, передбачень можливих сценаріїв «що, якщо» (наприклад, якщо при конкретному бюджеті потрібно скласти прогноз) та перегляду даних з різних точок зору. Хоча OLAP підтримує багатовимірний аналіз та прийняття рішень, ЦІУМБ для ІБ-аналітики додатково потрібні класифікація та кластеризація даних, визначення характеристик зміни даних із часом тощо;

- крок 5: ІБ-аналітика із застосуванням інтелектуальних методів і засобів для виявлення та вилучення потенційно корисних даних. Наприклад, у разі обробки потоків багаторівневий, багатовимірний оперативний інтелектуальний аналіз виконується на потокових даних у режимі реального часу при локальній потоковій передачі та колективній паралельній обробці, мережевих потоків тощо. Інший підхід полягає в асиметричній аналітиці з машинним навчанням, кластерним аналізом та розширеною візуалізацією для нелінійного аналізу від запиту до запиту у міру дослідження окремих подій та/або аномальної поведінки всієї ІТКМ, окремих ІС, активності користувачів тощо. Далі виявляються загальні закономірності та динамічні зміни на низькому і, що більш важливо, високому рівні абстракції для передбачення виникнення порушень ІБ та інцидентів ІБ. Закономірності описуються як шаблони (англ. patterns). ПЗ ІБ-аналітики являє собою набір функціональних модулів для визначення характеристик даних, аналізу зв'язків та кореляції, класифікації та кластерного аналізу, прогнозування та аналізу еволюції тощо;

- крок 6: оцінка отриманих закономірностей та виявлення серед них дійсно цікавих і корисних для конкретної ІТКМ з використанням спеціальних заходів перевірки. Модуль оцінки шаблонів, інтегрований у ПЗ ІБ-аналітики використовує, як правило, заходи та пороги «цікавості» для фільтрації виявлених шаблонів і взаємодіє з модулями їх знаходження таким чином, щоб сфокусувати пошук саме на «цікавих» з точки зору ІБ ІТКМ;

- крок 7: як заключний етап процесу ІБ-аналітики – представлення персоналу (зокрема, аналітикам) ЦІУМБ отриманих знань за допомогою різних

засобів візуалізації та підготовки звітності. Інтерфейс користувача є сполучною ланкою між системою ІБ-аналітики та користувачами, дозволяючи їм взаємодіяти з системою шляхом завдання запитів або запуску окремих завдань ІБ-аналітики, надаючи інформацію, що допомагає сфокусувати пошук, виконуючи «видобуток» даних на основі проміжних результатів аналізу, оцінки закономірностей, перегляду сховищ даних та візуалізації закономірностей у різних форматах. Прикладом можуть служити різні інформаційні панелі SIEM- та SOAR-систем.

3 РОЗРОБКА МОДЕЛІ ЦЕНТРА ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ МЕРЕЖЕВОЮ БЕЗПЕКОЮ

3.1 Метод застосуваня аналітики інформаційної безпеки у Центрі інтелектуального управління мережевою безпекою

Використання ІБ-аналітики у роботі типового ЦІУМБ саме з погляду ІТ великих даних може бути проілюстроване рисунком 3.1, де в овалах показані дані, включаючи додавання контексту розгляду «сирих» вихідних даних, а підписи курсивом відносяться до дій з обробки великих даних в ЦІУМБ.

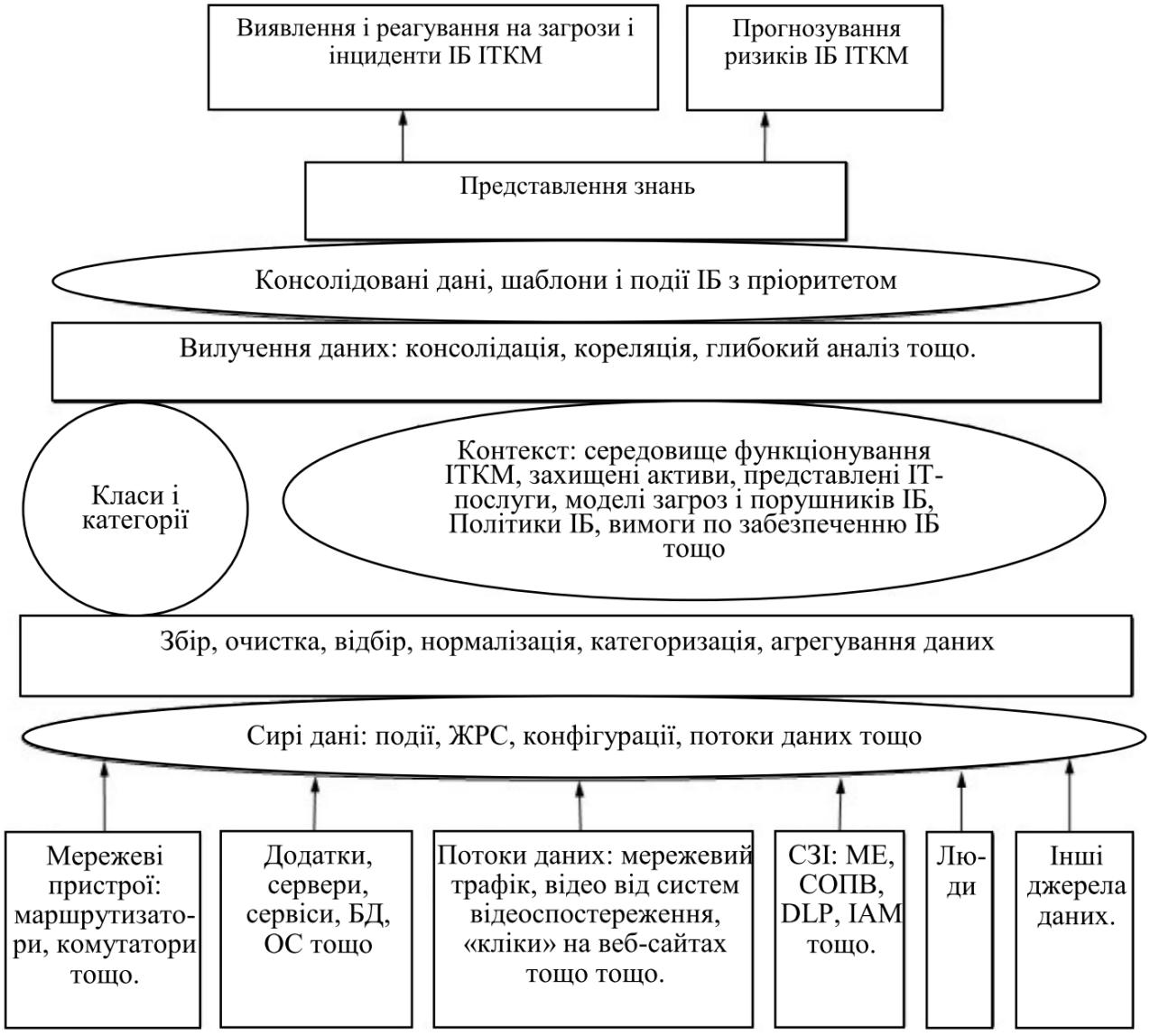

Рисунок 3.1 – Процес використання ІБ-аналітики в ЦІУМБ з точки зору ІТ великих даних

Найнижчий рівень на рисунку 3.1 – це рівень джерел даних. За ним йдуть рівні збору, обробки та зберігання даних. І зверху рисунка перебуває рівень подання інформації та знань безпосереднім споживачам.

Рисунки 2.3 та 3.1 повністю узгоджуються між собою. Отримані в результаті застосування ІБ-аналітики знання є основою не тільки для виявлення та реагування на інциденти ІБ, але і виявлення виникаючих загроз ІБ, а також для прогнозування ризиків ІБ ІТКМ установи.

Раніше неодноразово зазначалося, що ІБ-аналітика характеризується тим, що дані аналізуються не власними силами, а разом, у певному контексті. Для аналізу віднесених до ІБ ІТКМ даних визначаються такі типи контексту та приклади джерел отримання інформації про кожен тип контексту:

1) зовнішній:

- середовище (включаючи місце) здійснення діяльності установи - культурне, соціальне, політичне, правове, законодавче, фінансове, технологічне, економічне, природне та ринкове на міжнародному, регіональному, національному та локальному рівнях;

- установа у зовнішньому світі – основні фактори та тенденції, що впливають на цілі установи, стратегія та політика установи (особливо в області використання ІКТ та забезпечення ІБ ІКТ), інформація про установу із ЗМІ, репутаційні списки, списки бізнес-партнерів та постачальників обладнання та послуг, договори, інші зовнішні зв'язки тощо.

- світові тенденції в області ІБ - джерела Threat Intelligence (потоки з ненадійними IP-адресами, DNS-серверами, URL тощо);

- прохід в установу - системи контролю фізичного доступу (системи відеоспостереження, системи пропуску на територію установи тощо), місцезнаходження, погодні умови тощо;

2) внутрішній:

- організаційна структура - Статут, капітал, відомості про керівництво, відомості про управлінні ІТКМ, підрозділи, персонал, процеси прийняття рішень, комунікації всередині установи тощо;

- особливості ІТКМ – мережева карта ІТКМ, вся інформація про процеси, системи та використовувані технології, проектна документація, описи використовуваних протоколів, стандарти, керівні вказівки та моделі, прийняті організацією для ІТКМ, підсистеми ІТКМ, точки доступу, існуючі СЗІ тощо;

- дані, що обробляються в ІТКМ - категорування підлягаючої захисту інформації, списки зберігання даних (БД, сховища, носії інформації, у тому числі паперові), власники інформації, схема інформаційних потоків ІТКМ, інформація про системи управління даними (англ. Data Management Systems) і системи електронного документообігу (англ. Electronic Data Interchange), користувачі, правила контролю доступу тощо;

- інформаційні активи, ІС та ІТ-послуги ІТКМ - опис структури інформаційного забезпечення ІТКМ, реєстр активів із зазначенням розміщення, списки використовуваних додатків із зазначенням розробників, межі ІС, точки та канали взаємодії з іншими ІС, власники та користувачі ІС та ІТ-послуг, функціональні схеми ІС та ІТ-послуг, опис автоматизованих функцій, опис основних технічних рішень, структурна схема ІС, опис структури комплексу технічних засобів ІС, інша проектна та робоча документація на ІС та ІТ-послуги тощо;

- конфігурації АТ і ПЗ ІТКМ - опис структури ПЗ, опис структури АО,

організаційна структура підтримуючих підрозділів, організаційна структура користувачів, регламенти налаштування та внесення змін до налаштувань АО та ПЗ, даних з БД управління конфігураціями (англ. Configuration Management Database, CMDB) тощо;

- вразливості елементів ІТКМ – звіти з результатами використання САЗ та систем статичного (англ. Static Application Security Testing, SAST) та динамічного (англ. Dynamic Application Security Testing, DAST) тестування захищеності додатків, бази вразливостей, аудиторські звіти, реєстр ризиків ІБ, класифікація актуальних для установи вразливостей, модель загроз ІБ тощо;

- користувачі ІТКМ та їх бізнес-ролі - модель порушників ІБ, ІАМ-системи, сервіс директорій (англ. Active Directory), дані облікових записів, інформація відділу кадрів, список ролей і повноважень, регламенти та інструкції, політики ІБ, ЖРС DLP-систем, вивантаження за SIM-картами та корпоративними WiFi-мережами, інформація із соціальних мереж тощо.

Також слід зазначити, що при розгляді виникають в ІТКМ порушень ІБ та інцидентів, повинні бути використані в якості внутрішній контексту і всі раніше розроблені класифікації вразливостей, загроз ІБ, мережевих атак та інцидентів ІБ.

3.2 Архітектура обробки даних у Центрі інтелектуального управління мережевою безпекою за допомогою «Озера даних»

Для обробки даних, що відносяться до ІБ, у типовому ЦІУМБ пропонується використовувати не просто ІТ великих даних, але більш сучасні «озера даних» (англ. data lakes) або "Концентратори даних". Термін був введений у 2010 р. Дж.Діксоном (J.Dixon), але іноді він зневажливо розглядається як просто маркетинговий хід для розподілених систем, що підтримують проект з відкритим кодом Hadoop. Відомий і ще один підхід: «вчорашнє єдине сховище є сучасним озером даних організації». Озеро даних – це масштабоване сховище величезної кількості необроблених даних у вихідному форматі («як є»), поки вони не знадобляться, проміжних та кінцевих результатів їх обробки, а також система обробки, яка може приймати дані незалежно від їх структури.

Озера даних, як правило, будуються для обробки великих і швидко прибуваючих обсягів неструктурованих даних (на відміну від сховищ даних, що обробляють добре структуровані дані). Дані в озері стають доступними, як тільки вони будуть туди поміщені (на відміну від сховищ даних, призначених для даних, що змінюються повільно). Для зберігання даних озеро використовує «плоску» архітектуру, у якій кожен елемент даних має унікальний ідентифікатор та набір розширених тегів метаданих (на відміну ієрархічного сховища даних із

файлами і папками). Озеро не вимагає жорсткої схеми або маніпуляції даними всіх форм і розмірів, але вимагає підтримки порядок прибуття даних. Воно часто включає в себе семантичну БД - концептуальну модель, що використовує ті ж стандарти та технології, які застосовуються для створення інтернет-гіперспосилань, і додають рівень контексту для даних, що визначає їх значення і взаємозв'язок з іншими даними Для обробки даних в озері застосовуються динамічні (а не попередньо побудовані статичні, як у сховищах даних) аналітичні додатки. Його можна уявити як великий пул даних, що поєднує всі історичні та нові дані в режимі реального/близького до реального часу в одному місці, в якому схеми та вимоги до даних не визначені, поки дані не запитуються (використовується «схема-при-читанні»). Озера даних можуть комбінувати підходи SQL та NoSQL, а також можливості OLAP та оперативної обробки транзакцій (англ. Online Transaction Processing, OLTP).

При необхідності озеро даних двома способами можна поділити на три рівні:

1) вихідні дані; дані, що збираються щоденно; дані із зовнішніх джерел;

2) дані, яким менше, ніж 6 місяців, старі, але все ще активні дані, та архівні дані, які більше не використовуються, але обов'язково зберігаються через їх цінний зміст або за відповідними вимогами.

Усі перелічені характеристики озер даних повністю узгоджуються з вимогами до типового ЦІУМБ установи. Озеро даних є економічно ефективним місцем для проведення попереднього аналізу даних, у той час, як гнучке та цілеспрямоване структурування даних здійснюється лише тоді, коли це потрібно. «Відтік» даних з озера – це проаналізовані дані. Таким чином, озеро даних є ключовим компонентом ІБ-аналітики в типовому ЦІУМБ установи.

Для самого озера, оскільки воно є єдиним сховищем даних ЦІУМБ, дуже важливо забезпечити його експлуатаційну готовність, цілісність, контроль доступу, аутентифікацію та авторизацію, моніторинг та аудит, безперервність функціонування та відновлення після аварій. Управління таким озером включає середовище додатків для отримання та обробки даних у певному контексті за

допомогою каталогізації та індексування та для подальшого розширеного управління високоструктурованими даними – метаданими, синтезованими з вихідних, для відповіді на вторинні запити до них.

При зазначеному підході до побудови типового ЦІУМБ озера, що використовуються в ньому, володітимуть такими дуже важливими характеристиками для підтримки даних, що відносяться до ІБ:

- масштабована (зі зростанням даних) архітектура з високою доступністю;

- централізоване управління та дотримання політик збереження та видалення, ідентифікації застарілих даних тощо;

— централізована каталогізація та індексація всіх доступних даних та метаданих, включаючи їх джерела, керування версіями, забезпечення достовірності та точності;

- підтримка взаємозв'язків між даними;

- результативне керування даними, що враховує видалення та стиснення та усуває дублювання;

- можливість відстеження всіх перетворень, що виконуються з даними, включаючи тип перетворення, час і джерело надходження, хто і чому змінював їх, які версії існують, як довго вони будуть корисні чи актуальні тощо;

- єдине, просте в управлінні сховище даних, що спільно використовується, доступне для всіх додатків (замість створення контейнерів для нового файлу та копій даних);

- така модель даних, при якій кожен біт даних одночасно доступний в різних форматах, що не потребує повторного виконання процесів вилучення, перетвореня та завантаження і дозволяє швидко передавати дані аналітику та різнорідним додаткам і тим самим прискорює підтримку робочих процесів;

- доступ із будь-якого пристрою (блокнота, смартфона, ноутбука, робочого столу тощо) для підтримки мобільних працівників;

- гнучка аналітика при переміщенні даних в/з озера з використанням декількох аналітичних підходів і потоків обробки даних, а також єдина ІБ-аналітика, заснована на дуже конкретних випадках використання;

- заданий рівень якості обслуговування з надійно ізольованими (але за змістом консолідованими) виконуваними робочими процесами у своїх зонах у рамках типового ЦІУМБ для забезпечення їхнього захисту;

- самі дані нікуди не переміщуються - обробка "йде до них", а не навпаки;

- закладений у саму концепцію озер «принцип мінімальних привілеїв» при доступі до даних, що добре узгоджується з встановленими вимогами до типового ЦІУМБ.

В даний час обсяги пов'язаних з ІБ даних - це одна з проблем, але ще більша проблема – це швидкість, з якою події в області ІБ ІТКМ трапляються. Саме тому більшість пов'язаних з ІБ даних, що надходять до ЦІУМБ, можна розглядати і як швидкі дані (англ. fast data), оскільки вони вимагають негайної обробки для прийняття відповідних рішень та активації виконання певних дій у відповідь. Отже, концепція швидких (інтерактивних) даних доповнює ІТ великих даних щодо управління та обробки більшої кількості «летючих» даних, пов'язаних з ІБ ІТКМ.

Швидкі дані застосовуються в ІБ-аналітиці до даних у режимі жорсткого реального часу для вирішення того чи іншого завдання. Вони відіграють важливу роль у додатках, які вимагають низької латентності (очікування, затримки), і залежать від високої здатності вводу/виводу. Мета аналізу швидких даних - швидко зібрати (захопити) і проаналізувати із застосуванням інтелектуальних підходів структуровані та неструктуровані дані з різних джерел таким чином, щоб можна було швидко вжити відповідних заходів. Швидкі дані часто приходять у системи даних у потоках і тоді потрібна обробка великих потоків даних зі швидкістю їх надходження - "на льоту". Приклад – це дані смарт-ґрід додатків, що аналізує в режимі реального часу використання електроенергії в десятках тисяч локацій і автоматично ініціює відключення навантаження, щоб збалансувати подачу з потребою в певних географічних районах.

На основі вищевикладеного можна зробити висновок, що у типовому ЦІУМБ установи необхідно створити озеро (рисунок 3.2), розраховане

працювати з великими «сирими» даними, більша частина з яких є швидкими. «Сирі» дані зі своїми джерелами на рисунках 3.1 та 3.2 повністю збігаються.

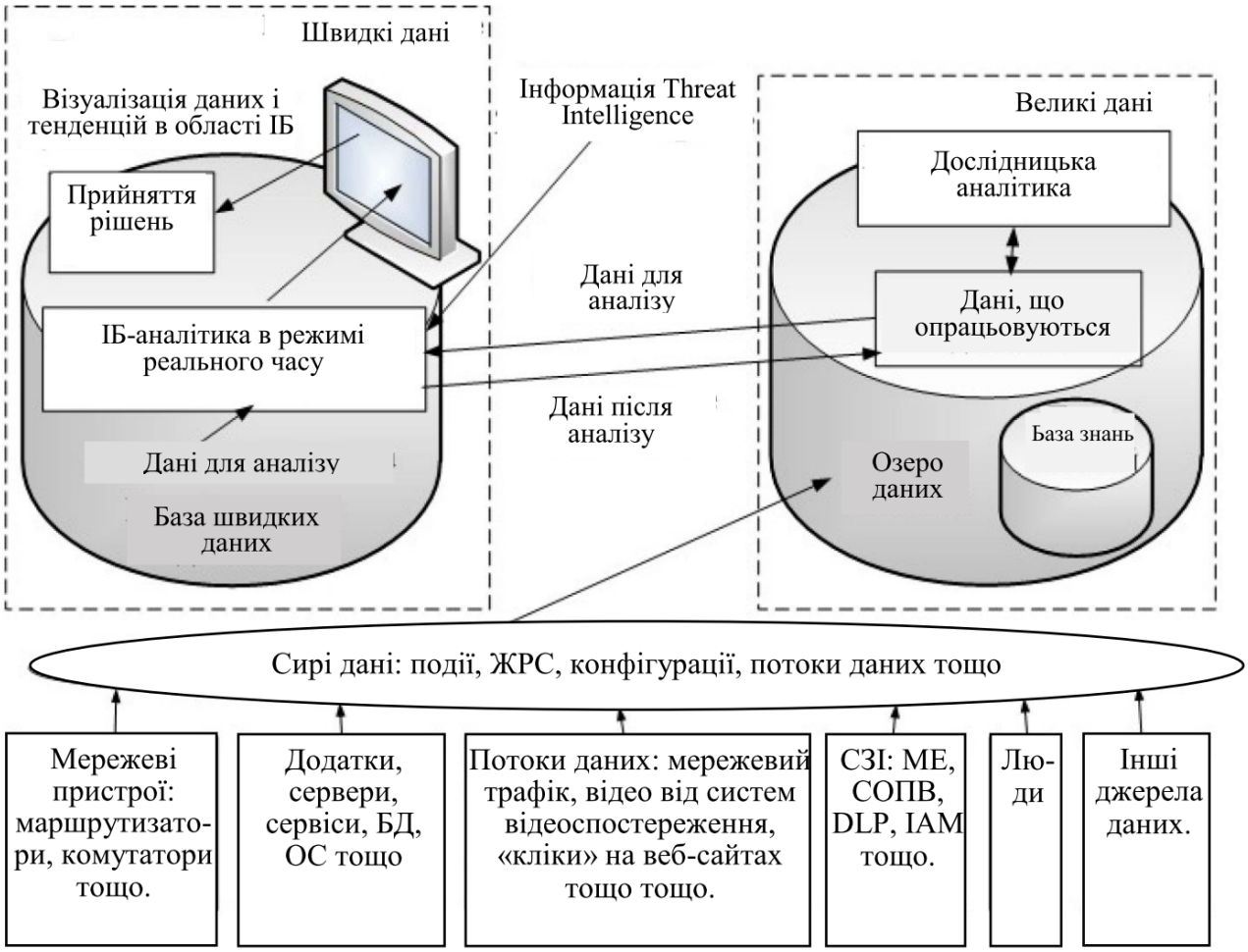

Рисунок 3.2 – Спрощена архітектура обробки даних у ЦІУМБ

Щоб процедури обробки не виконувати по кілька разів, в озері також будуть знаходитися і спочатку оброблені вихідні дані (C Boxes) і метадані (D Box), одержані на основі форматування та агрегування «сирих» даних, і власне результати обробки даних після застосування методів ІБ-аналітики (див. рисунок 3.2). Оброблені дані як підмножина необроблених менші за обсягом, ніж вихідні, але все ж таки вимагають спеціалізованих інструментів та експертних навичок для вилучення даних для аналізу. Останні представлені у готовому для подальшого аналізу форматі та мають керований доступ. Високопродуктивні аналітичні системи можуть забезпечити інтеграцію даних для аналізу з раніше обробленими даними з озера та необробленими швидкими даними, щоб ІБ-

аналітика могла здійснюватися в режимі жорсткого реального часу в контексті будь-якої транзакції в ІТКМ, що робить ці дані невід'ємною частиною аналітичного процесу.

Озеро даних також виконує функції K Box – у складі виділено базу знань.

Вироблення реагування у відповідь на інциденти ІБ та ведення звітності з ІБ (R Box) зображено на рисунку 3.2 як блок прийняття рішень на основі візуалізованих даних і тенденцій в області ІБ у попередньо налаштованих форматах.

Дослідницька аналітика призначена для проведення початкових досліджень необроблених даних з метою виявлення закономірностей і аномалій, а також перевірки гіпотез та припущень за допомогою зведеної статистики.

У таблиці 3.1 наведено результати порівняння базових можливостей традиційних підходів аналізу даних, що стосуються ІБ даних в ЦМБ та ІБ-аналітики в ЦІУМБ установи, які показують суттєві переваги ІБ-аналітики для реалізації попереджувального управління мережевою безпекою ІТКМ, що має у своєму складі ЦІУМБ.

Архітектура обробки даних у ЦІУМБ на рисунку 3.2 суттєво спрощена і просто показує, як великі дані можуть використовуватись у типовому ЦІУМБ установи. Організація взаємодії з швидкими даними відрізняється від такої для великих даних «у спокої» і вимагає систем, які побудовані трохи інакше, ніж традиційні БД.

3.3 Функціональна стійкість Центру інтелектуального управління мережевою безпекою в єдиному інформаційному просторі

Від типового ЦІУМБ потрібна не просто його стійкість як системи, а функціональна стійкість у штатному режимі та в умовах загроз ІБ (в умовах спрямованих на нього комп'ютерних атак, при збоях підвищеного ступеня серйозності та в умовах надзвичайних ситуацій) – здатність типового ЦІУМБ регулювати своє функціонування в ЄІП з метою підтримки виконання його

бізнес-процесів за очікуваних умов і в умовах посилення вимог, порушень та інцидентів, загроз ІБ та непередбачених обставин. Це активна форма стійкості для динамічної системи.

Таблиця 3.1 - Порівняння традиційних підходів аналізу даних в ЦМБ та ІБ-аналітики в ЦІУМБ установи

Традиційні підходи аналізу даних у ЦМБ	ІБ-аналітика в ЦІУМБ
1	2
- використання SIEM-системи 1.0 для виявлення поширених і добре формалізованих інцидентів ІБ правил «з коробки»; - слідування при аналізі логіки, яка застосовується порушником ІБ на перших стадіях мережевих атак - розвідка, зараження та початкове проникнення; - виявлення скомпрометованих облікових записів за допомогою кореляції подій; - пошук звернень на підозрілі зовнішні IP-адреси;	- аналіз структурованих, неструктурованих та напівструктурованих даних від гетерогенних джерел; - можливість обробки швидких даних; - кореляція мережевих потоків, даних про вразливості, події на кінцевих точках, даних, зібраних СЗІ тощо; - максимальне усунення «шумів» у даних, що підлягають аналізу; - створення метаданих та профілів (профілювання) дій користувачів та пошук аномалій у цих діях та даних, що вказують на інциденти ІБ; - використання контексту (так звана ситуативна аналітика - від англ. tradeoff analytics) при складанні правил кореляції та застосування інформації з потоків Threat Intelligence; - застосування «полювання за загрозами» щодо тих, що зберігаються в озері історичних даних за тривалі періоди часу;

1	2
- використання для виявлення інцидентів ІБ інформації, отриманої в результаті підписки на потоки Threat Intelligence; - вибудовування процесу реагування на виявлені інциденти ІБ усередині SIEM-системи на основі "сирих" подій.	- застосування інтелектуальних підходів для синтезу нових знань з метою виявлення раніше не виявлених інцидентів ІБ; - використання технологій штучного інтелекту та природних мов під час аналізу інцидентів ІБ; - широке використання різних можливостей візуалізації інформації на моніторі аналітика для виявлення прихованих інцидентів ІБ і тенденцій в області ІБ для розробки попереджувального управління мережевою безпекою ІТКМ.

Забезпечення функціональної стійкості типового ЦІУМБ має підтримуватись збереженням безперервності його бізнес-процесів та їх частини у вигляді окремих бізнес-процесів операцій та доступності ІТ-послуг та ресурсів користувачам, навіть в умовах передбачуваної заздалегідь деградації інфраструктури та функціональних процесів, у тому числі при впливі різних дестабілізуючих впливів та відмов усередині самого ЦІУМБ. Логічно продовжуючи цю думку, функціональну стійкість типового ЦІУМБ можна розглядати як таку його здатність, при якій рівень ризику порушення функціонування та доступності ІТ-послуг і ресурсів передбачувані і прийнятні як для їх користувача, так і для власника. Причому ця здатність має бути спочатку вбудована в проект типового ЦІУМБ, а не добавлена у вигляді окремих функцій, а всі порушення ІБ та інциденти ІБ мають бути контрольованими.

Функціональна стійкість типового ЦІУМБ в ЄІП після припинення дії збурення має проявлятися у двох режимах функціонування:

1) «у малому», коли з часом досить мале відхилення режиму роботи від вихідного (установленого) зменшується і функціонування ЦІУМБ повертається у вихідний стан;

2) «у великому», коли після припинення дії збурення при досить великому початковому відхиленні функціонування ЦІУМБ повертається у вихідний стан.

Управління функціональною стійкістю типового ЦІУМБ як невід'ємна частина всього процесу управління ЦІУМБ має враховувати, що для досягнення поставленої мети його функціонування під час та після впливу інциденту ІБ може знадобитися зміна значень параметрів, що стосуються всіх його бізнес-процесів (на відміну від окремого випадку управління – регулювання, яке полягає лише у підтримці певних параметрів системи у заданих межах).

В загальному випадку управління функціональною стійкістю типового ЦІУМБ базується на управлінні ІТ-операціями та наданням ІТ-послуг, управлінні безперервністю функціонування, управлінні власною ІБ ЦІУМБ та інших складових цього процесу, наприклад, управлінні фінансами, персоналом, комунікаціями та обізнаністю (рисунок 3.3).

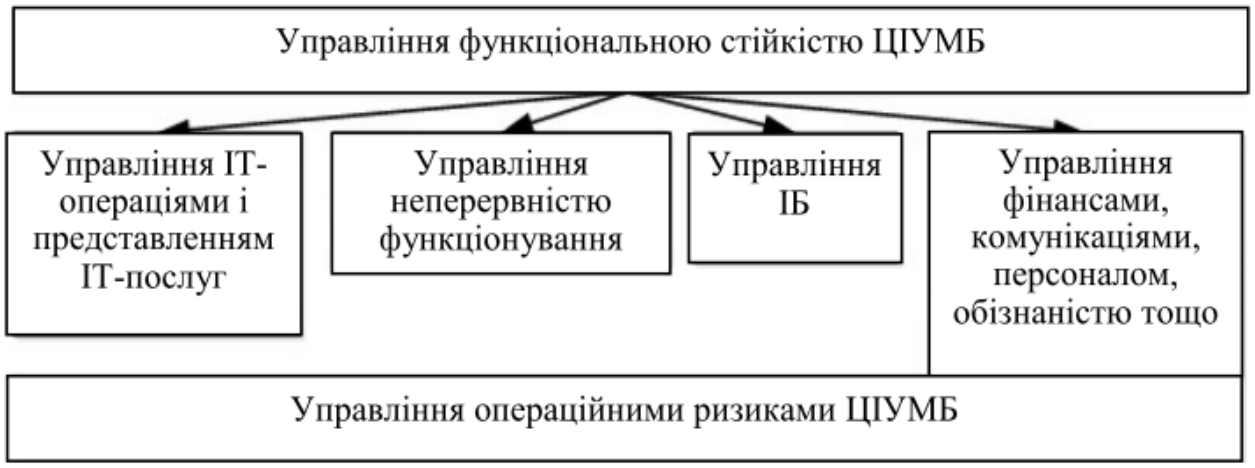

Рисунок 3.3 – Складові процесу управління функціональною стійкістю ЦІУМБ

Управління ІТ-операціями, безперервністю функціонування та ІБ – це доповнюючі і взаємодіючі між собою процеси, орієнтовані на управління операційними ризиками ЦІУМБ, які мають одну спільну мету – покращувати та підтримувати функціональну стійкість типового ЦІУМБ. При цьому ризик порушення функціонування ЦІУМБ або операційний ризик (англ. operational risk), це ризик збитку установи внаслідок неадекватних чи помилкових внутрішніх процесів ЦІУМБ, дій його робітників та систем або зовнішніх подій.

Однією з основних складових ІТКМ, а, отже, і ЦІУМБ, є інформаційна складова. Отже, значна частина операційних ризиків типового ЦІУМБ, включаючи ризик переривання його діяльності, пов'язана з інформацією, а рівень та умови прояву цих ризиків багато в чому визначаються якістю ІТ-послуг (з підготовки, обробки, передачі, зберігання та відображення інформації), які можуть бути надані з використанням ІКТ.

Безперервність функціонування ЦІУМБ в ЄІП – це стратегічна та тактична здатність типового ЦІУМБ планувати свою роботу у випадку інцидентів ІБ та порушень його функціонування, спрямована на забезпечення безперервності бізнес-процесів на встановленому прийнятному рівні Логічно продовжуючи наведене визначення, можна вважати, що забезпечення безперервності функціонування типового ЦІУМБ ЄІП буде забезпеченням такої стратегічної та тактичної здатності цієї системи, що передбачає довгострокове існування ЦІУМБ в ЄІП. У свою черга, управління безперервністю функціонування типового ЦІУМБ в ЄІП є цілісним системним процесом управління, що передбачає ідентифікацію потенціальних порушень та інцидентів ІБ та їх впливу на функціонування типового ЦІУМБ для прийняття обґрунтованих рішень щодо збереження його бізнес-процесів. Такий вид управління створює основу для підвищення функціональної стійкості типового ЦІУМБ і направлений на реалізацію таких типових заходів у відповідь проти інцидентів ІБ, які забезпечують захист функціонування ЦІУМБ. Тоді безперервність функціонування типового ЦІУМБ в ЄІП також можна визначити як здатність ЦІУМБ зберігати надійність його ресурсів, що забезпечують безперервність бізнес-процесів та доступність ІТ-послуг і самої інформації користувачам, навіть в умовах деградації інфраструктури та функціональних процесів ЦІУМБ, у тому числі при впливі різних порушень ІБ та інцідентів ІБ.

Користувач при зверненні до необхідних йому ресурсів та послуг ЦІУМБ у межах своїх повноважень має отримати доступ за прийнятний йому час. Для цього типовий ЦІУМБ для типової ІТКМ має бути системою високої доступності (англ. high availability), що має на увазі забезпечення для неї підвищеної

відмовостійкості (здатності зберігати працездатність при випадкових виходах з ладу або збоях окремих елементів ЦІУМБ), катастрофостійкості (здатності ЦІУМБ зберігати критично важливі ресурси і продовжувати виконання своїх функцій, можливо з певними обмеженнями, в умовах деградації його архітектури, викликаної знищенням елементів та зв'язків між ними в результаті стихійних лих, техногенних аварій і катастроф, цілеспрямованого впливу людей або груп людей) та достатньої інформаційної захищеності на задану перспективу. Висока доступність означає здатність ЦІУМБ працювати при існуючих навантаженнях та при їх збільшенні, а також протистояти відмовам, викликаних, у тому числі, знищенням його компонентів та зв'язків між ними, а рівень доступності зазвичай вимірюється "дев'ятками". Система високої доступності з максимальним рівнем доступності, рівним 99,999%, допускає п'ять хвилин простою на рік та призначена для практично безперебійного надання IT-послуг. Установа має самостійно визначити рівень доступності для свого ЦІУМБ.

З рисунка 3.3 ясно видно, що ефективність та результативність управління функціональною стійкістю типового ЦІУМБ безпосередньо залежить від процесів управління безперервністю функціонування ЦІУМБ в ЄІП та управління його ІБ на основі СОІБ. Причому на рис. 52 ці два процеси показані як незалежні, хоча насправді вони можуть перетинатися, оскільки деякі загрози та ризики управління неперервністю функціонування та управління ІБ можуть бути одними і тими ж. На основі проведеного аналізу однакових ризиків можуть бути вироблені схожі вимоги щодо забезпечення безперервності функціонування та ІБ, а надалі обрані однакові процеси та заходи забезпечення ІБ для подібних ризиків.

Загалом процес управління безперервністю функціонування типового ЦІУМБ в ЄІП можна розділити на два генеральні напрямки під час його реалізації:

1) забезпечення функціональної стійкості ЦІУМБ та його бізнес-процесів, в результаті чого відбувається зниження ймовірності настання ризикових подій

(інцидентів, порушень, відмов тощо) на основі розробки та впровадження превентивних антикризових заходів;

2) відновлення (або продовження) функціонування ЦІУМБ, включаючи при цьому бізнес-процеси, окремі операції та ресурси, після ризикових подій з наступною мінімізацією та коригуванням їх негативного впливу, якщо вони вже сталися.

Наочно процес відновлення функціональної стійкості ЦІУМБ після деякого інциденту ІБ можна представити так, як показано на рисунку 3.4. Важливо при цьому зауважити, що після закінчення інциденту ІБ не завжди відразу повинно відбуватися різке припинення виконання установлених бізнес-процесів (як на рисунку 3.4), оскільки він може породжувати як прямі, так і непрямі збитки.

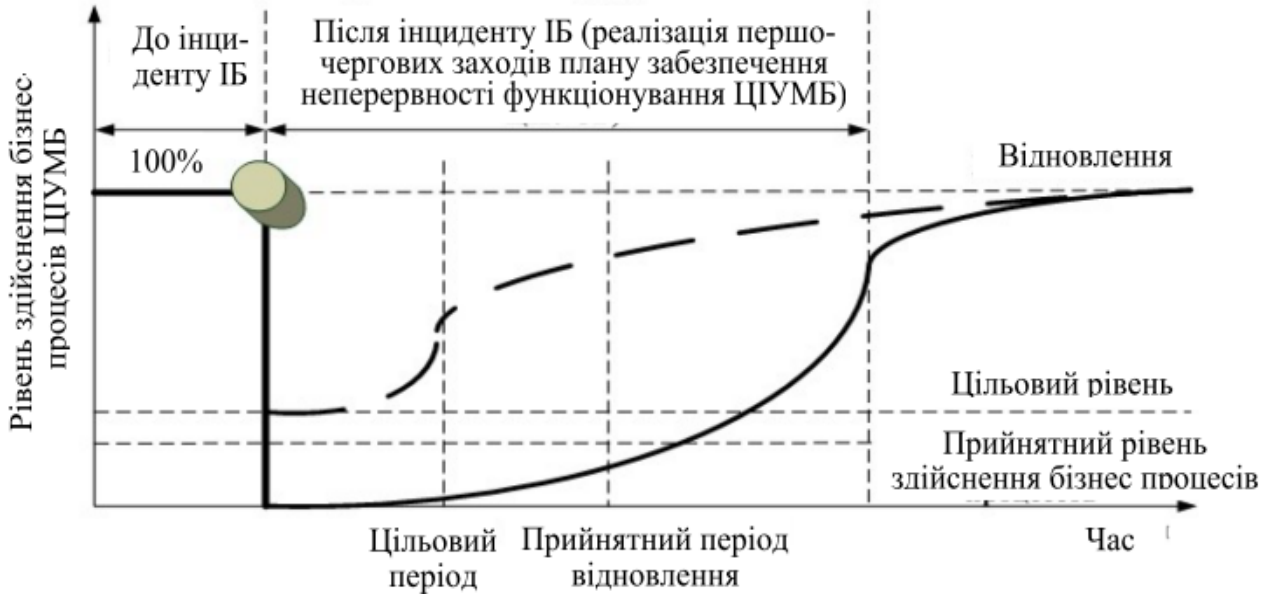

Рисунок 3.4 – Процес відновлення функціональної стійкості типового ЦІУМБ після інциденту ІБ

Найпростішими заходами забезпечення функціональної стійкості типового ЦІУМБ є розробка плану забезпечення безперервності функціонування, застосування генераторів для резервного живлення, використання більш довговічних будівельних матеріалів тощо.

Система управління функціональною стійкістю типового ЦІУМБ призначена для всебічної підтримки відповідного процесу управління та включає План і Програму управління, сам процес, процедури та практики управління, і навіть весь задіяний у процесі персонал (рисунок 3.5).

Рисунок 3.5 – Основні елементи системи управління функціональною стійкістю ЦІУМБ

При ефективній реалізації цієї системи вона сприяє наступному:

- постійне вдосконалення стійкого функціонування ЦІУМБ і забезпечення стабільності у досягненні його основних бізнес-цілей;

- надання відпрацьованого методу відновлення здатності ЦІУМБ представляти ресурси та IT-послуги на встановленому рівні в межах узгодженого часу після порушення функціонування;

— забезпечення верифікуючої здатності ЦІУМБ керувати порушеннями функціонування та захищати свої бізнес-процеси.

У таблиці 3.2 представлений початковий набір показників для функціональної стійкості типового ЦІУМБ за прийнятий звітний період (зокрема, день, тиждень, місяць, квартал або рік) із зазначенням вибраного одного із трьох класів – управлінські (У), організаційні (О) та технічні (Т), до яких вони можуть бути віднесені. У міру вдосконалення діяльності щодо проведення оцінок рівня функціональної стійкості ЦІУМБ цей набір буде розширятися.

Таблиця 3.2 - Початковий набір показників функціональної стійкості типового ЦІУМБ за ухвалений звітний період

Функція ЦІУМБ	Очікуваний узагальнений результат оцінки	Показники функціональної стійкості ЦІУМБ за прийнятий звітний період
1	2	3
Управління інцидентами ІБ	Наскільки добре виявляються, правильно ідентифікуються, обробляються і усуваються наслідки інцидентів ІБ	Вартість інциденту ІБ (У). Середня вартість інциденту ІБ (У). Середня вартість відновлення після інциденту ІБ (О). Середній час до виявлення інциденту ІБ(О). Кількість інцидентів ІБ(Т). Середній час між інцидентами ІБ(О). Середній час відновлення після інциденту ІБ(О).
Управління уразливостями	Наскільки добре виявляються вразливості засобами ідентифікації та усунення відомих вразливостей.	Зона дії сканерів аналізу захищеності (Т). Відсоток систем, в яких немає відомих серйозних вразливостей (У). Середній час усунення уразливостей (О). Кількість відомих уразливостей (Т). Середня вартість усунення уразливості (О).
Управління оновленнями	Наскільки добре вдається підтримувати постійне оновлення систем.	Дотримання політики встановлення оновлень (У). Зона дії встановлення оновлень (Т). Середній час до оновлення (О). Середня вартість поновлення (О).

1	2	3
Управління конфігураціями	Який стан конфігурацій систем організації.	Відсоток правильних конфігурацій (У). Зона дії управління конфігураціями (Т). Поточні налаштування відображення шкідливих кодів (Т).
Управління змінами	Як зміни в конфігураціях систем впливають на ІБ установи.	Середній час внесення змін (О). Відсоток змін із аналізом ІБ (У). Відсоток змін із винятками ІБ(О).
Захист додатків	Чи можна покластися на захищеність додатків, які використовуються для здійснення діяльності установи.	Кількість додатків (Т). Відсоток критичних додатків (Т). Зона дії оцінки ризиків ІБ (Т). Зона дії тестів із забезпечення ІБ (Т).
Фінанси	Який рівень та цілі витрат на забезпечення ІБ.	Витрати на ІБ у відсотковому відношенні до витрат на ІТ (У). Бюджетні асигнування на ІБ (О).

На прикладі управління інцидентами ІБ у самому ЦІУМБ покажемо, як можна розрахувати вказані в таблиці показники:

- вартість інциденту ІБ, що складається з прямих втрат (вартість знищених активів тощо) – ПП; вартості простою ЦІУМБ (вартість відшкодування витрат для бізнес-операцій та вартість втрат для установи, безпосередньо пов'язаних з інцидентами ІБ у ЦІУМБ) - СП; вартості утримання (зусилля та вартість; консультаційні послуги) - СУ; вартості відновлення (вартість дослідження та аналізу інциденту ІБ; зусилля, необхідні для відновлення і заміни АТ, ІВ, ПО ЦІУМБ; вартість заміни перерахованого обладнання, консультаційні послуги із

заміни або дослідження) – СЗ; вартість відшкодування збитків (штрафи та інші кошти, що виплачуються через порушення контрактів, що виникли внаслідок інциденту ІБ до ЦІУМБ; вартість ненадання клієнтам ІТКМ послуг внаслідок інциденту ІБ до ЦІУМБ; вартість зв'язків із громадськістю; вартість розкриття та повідомлення; судові витрати, штрафи та виплати) – СВУ: ССІ = ∑ (ПП + СП + +СУ + СЗ + СВП) / (загальна кількість інцидентів ІБ);

- середня вартість відновлення функціональної стійкості ЦІУМБ після інцидента ІБ, яка дорівнює усередненій за всіма інцидентами ІБ сумарної вартості: ССВПІ = ∑ (Вартість_відновлення) / (загальна кількість інцидентів ІБ);

- середній час до виявлення інциденту ІБ за ухвалений звітний період, який має з часом знижуватися: СВВІ = ∑ (Дата_виявлення – Дата_події) / (загальна кількість інцидентів ІБ);

- середній час між інцидентами ІБ за прийнятий звітний період, який повинен з часом збільшуватися і залежить від усередненого за кількістю інцидентів ІБ сумарного часу між двома інцидентами ІБ, що відбулися один за одним: ЗВМІ = ∑ (Дата_пригоди_n – Дата_події_n-1) / (загальна кількість інцидентів ІБ);

- середній час відновлення після інциденту ІБ за ухвалений звітний період, який має з часом зменшуватися і залежить від усередненого по всіх інцидентах ІБ сумарного часового інтервалу між датами всіх подій та відновлень після них:

СВВПІ = ∑ (Дата_відновлення – Дата_події) / (загальна кількість інцидентів ІБ).

Аналогічні формули можна вивести для інших показників і скласти перелік їх атрибутів.

ВИСНОВКИ

1. Здійснено аналіз сучасних методик побудови типових Центрів інтелектуального управління мережевою безпекою, що дозволило виявити їх недоліки та обгрунтувати необхідність використання нових підходів до комплексного управління інформаційною безпекою.

2. Розроблено функціональну та зональну архітектуру забезпечення інформаційної безпеки в Центрі інтелектуального управління мережевою безпекою, що дозволило побудувати схему отримання знань Центром управління.

3. Розроблено модель обробки даних у Центрі інтелектуального управління мережевою безпекою за допомогою «Озера даних», що дозволило продемонструвати функціональну стійкість Центру в єдиному інформаційному просторі.

4. Розроблено метод застосуваня аналітики інформаційної безпеки у Центрі інтелектуального управління мережевою безпекою, що дозволило розробити моель обробки даних за допомогою «Озера даних».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Заїка В.Ф., Варфоломеєва О.Г., Домрачева К.О., Гринкевич Г.О. Телекомунікаційні системи та мережі наступного покоління, 2019. 315с.

2. Яцишин О.В. Дослідження технологій безпроводових сенсорних мереж з інфокомунікаційними наземними вузлами у зоні надзвичайної ситуації. https://ela.kpi.ua/bitstream/123456789/28112/1/Yatsishin_bakalavr.pdf

3. Піневич Т.О. Стандартизація інфокомунікаційних мереж та систем. Інформаційно-керуючі системи на залізничному транспорті 2018 №6. С. 41-58.

4. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики: Вибр. наук. праці. К. : НІСД, 2016. 528 с.

5. 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.

6. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. К.: ДУТ, 2015. 449 с.

7. Cisco AVVID Network Infrastructure Overview Електронний ресурс] – Режим доступу: https://www.cisco.com/web/offer/CAT4500/toolkit/comin_ov.pdf

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

9. Tanenbaum A.S., Wetherall D.J. Computer Networks, 5th Ed. Prentice Hall, Cloth, 2011. 960 pp.

10. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. - Pearson Education, Inc., Old Tappan, New Jersey, 2016. 538 pp.;

11. 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.

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

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

14. 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.

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

16. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. Житомир: ЖНАЕУ, 2016. 636 с.

17. 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

18. 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.

19. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: монографія; за загальною редакцією д-ра юрид. наук, проф. Бандурки О. М.. Харків: Вид-во Ун-ту внутр. Справ, 2015. 368 с.

20. Азаров Д.С. Злочини у сфері комп’ютерної інформації (кримінально-правове дослідження): моногр. К.: Атіка, 2007. 304 с.

21. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства. Сучас. спец. техніка. 2011. № 3 (26). С. 104–114.

22. 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.

23. 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.

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

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

26. Підлиський П., Лисик М. Модель функціональної стійкості Центру інтелектуального управління мережевою безпекою. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2024), Тернопіль, 2024. С.153-155.

27. Підлиський П., Залужна Н. Функціональна інфраструктура типового Центру інтелектуального управління мережевою безпекою. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2024. С.80-81.

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

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

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