Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи
магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

напрям підготовки 125 Кібербезпека
(код і назва напряму підготовки)

освітній рівень ***магістр***
(назва освітнього рівня)

кваліфікація _____
(назва кваліфікаційного рівня)

на тему: Розробка рекомендацій щодо управління станом захищеності інформаційних ресурсів в умовах впливу кібератак

Виконавець: студент II **курсу**, **групи** КБМ-21

_____ Кулько Андрій Аркадійович
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	Толюпа С.В.		
Рецензент			
Нормоконтроль	Фесенко А.О.		

Київ 2021

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації
_____ Лукова-Чуйко Н.В.
«_____»_____2021 року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту КБм-21 (група) Кулько Андрію Аркадійовичу (прізвище ім'я по-батькові)

Тема дипломної роботи Розробка рекомендацій щодо управління станом захищеності інформаційних ресурсів в умовах впливу кібератак.

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ
Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол №2 від 08.10.2020р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень процес функціонування ІТС обробки ІР в умовах впливу кібератак.

Предмет досліджень методи управління станом захищеності ІР на основі даних про кібератаки.

Мета роботи розробка рекомендацій щодо покращення існуючих підходів до управління станом захищеності ІР від зовнішніх та внутрішніх кібератак на ІТС.

Вихідні дані для проведення роботи	результати обстеження середовищ функціонування інформаційної системи

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна	Вперше отримано рекомендації щодо процесу управління станом захищеності шляхом удосконалення методу управління станом захищеності використовуючи розмежування даних для зовнішніх і внутрішніх кібератак.

Практична цінність	Отримані результати можуть бути використані для підвищення ефективності функціонування ІТС, при розробці комплексної системи захисту для інформаційних ресурсів та проектуванні систем управління інформаційними ресурсами в умовах впливу кібератак.

4. ВИМОГИ ДО РЕАЛІЗАЦІЇ РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота повинна виконуватися згідно діючої законодавчої та нормативної бази у сфері технічного захисту інформації та забезпечення національної безпеки України в кібернетичному просторі.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	08.10.2020 – 17.10.2020
Аналіз інформаційних джерел	18.10.2020 – 01.11.2020
Збір даних для вибору рішення	02.11.2020 – 24.11.2020
Обгрунтування вибраних цілей та завдань	25.12.2020 – 15.12.2020
Способи та шляхи досягнення цілей і завдань	16.12.2020 – 31.01.2021
Методи інтелектуального аналізу даних	01.02.2021 – 26.02.2021
Розробка рекомендацій	27.02.2021 – 02.03.2021
Збір результатів та їх аналіз	03.03.2021 – 13.03.2021
Робота над висновками	14.03.2021 – 25.04.2021
Оформлення роботи	02.04.2021 – 22.04.2021
Оформлення презентації	23.04.2021 – 23.05.2021
Оформлення пояснювальної записки	23.05.2021 – 24.05.2021

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект	мінімальні витрати на впровадження запропонованих рекомендацій щодо покращення управління станом захищеності
Соціальний ефект	застосування рекомендацій дозволить більш прокащити процес управління станом захищеності.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ С.В. Толюпа
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ А.А. Кулько
(підпис) (ініціали, прізвище)

Дата видачі завдання: 08 жовтня 2020 року

Термін подання дипломної роботи до ЕК: 24 травня 2021 року

УДК 004.056 (045)

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Розробка рекомендацій щодо управління станом захищеності інформаційних ресурсів в умовах впливу кібератак.» складається зі списку скорочень, вступу, основної частини, що містить 3 розділи, висновків і списку літератури та джерел, а також додатку А і Б. Загальний обсяг роботи – 93 сторінки. Робота містить 16 рисунків, 4 таблиці та 2 додатки. Список використаних джерел включає 68 джерел.

Мета і завдання дослідження. *Метою досліджень* є розробка рекомендацій щодо покращення існуючих підходів до управління станом захищеності ІР від зовнішніх та внутрішніх кібератак на ІТС.

Завдання магістерської роботи полягає в розробці рекомендацій щодо управління станом захищеності ІР від зовнішніх та внутрішніх кібератак на ІТС з використанням методів ідентифікації, динамічного програмування та опорних векторів.

Об’єкт дослідження – процес функціонування ІТС обробки ІР в умовах впливу кібератак.

Предмет дослідження – методи управління станом захищеності ІР на основі даних про кібератаки.

Методи дослідження. Для вирішення сформульованого завдання в магістерській роботі використано такі наукові методи: аналіз – для вивчення методів роботи існуючих підходів до управління станом захищеності ІР в ІТС; теорія ймовірностей та математична статистика – для вивчення закономірностей випадкових явищ, подій, їхніх функцій, властивостей та операції над ними; метод опорних векторів – для розпізнавання образів, пошуку закономірностей даних та класифікації за ознаками; динамічне програмування – для розбиття складних задач на більш прості, встановлення структурних зв’язків між елементами досліджуваної системи; моделювання –

для побудови моделі ІТС, що використовувалася для дослідження процесу управління станом захищеності ІР з використанням розроблених методів.

Наукова новизна отриманих результатів. У результаті проведених досліджень отримано такі результати:

У даній дипломній роботі вперше одержано рекомендації щодо процесу управління станом захищеності шляхом удосконалення методу управління станом захищеності використовуючи розмежування даних для зовнішніх і внутрішніх кібератак.

Практичне значення отриманих результатів. Отримані результати можуть бути використані для підвищення ефективності функціонування ІТС, при розробці комплексної системи захисту для інформаційних ресурсів та проектуванні систем управління інформаційними ресурсами в умовах впливу кібератак.

Апробація матеріалів магістерської. Основні результати наукових досліджень, викладені в магістерській роботі, були опубліковані та обговорені в ході проведення:

1. А.А. Кулько, С.В. Толюпа Виявлення атак за допомогою методу опорних векторів. ІІІ міжнародна науково-практична конференція. Проблеми кібербезпеки інформаційно-телекомунікаційних систем. Збірник матеріалів доповідей та тез. м. Київ, 2020 р. КНУ імені Тараса Шевченка. с. 105-109.
2. Толюпа С.В., Шестак Я.В., Кулько А.А., Чечуга А.М. Автоматизація процесу управління інцидентами інформаційної безпеки. Збірник тез IV Міжнародної науково-практичної конференції «Прикладні системи та технології в інформаційному суспільстві». К.: Київський нац. ун-т імені Тараса Шевченка, 2020. – 215-222с.
3. Сергій Толюпа, Олександр Успенський, Андрій Кулько, Олег Кулініч. Вплив кібернетичних атак на інформаційну систему. Збірник матеріалів доповідей та тез. IV Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS). – К.: ВПЦ"Київський університет", 2021. – 149-151 с.

Ключові слова: інформаційна безпека, кібербезпека, інформаційні ресурси, інформаційно-телекомунікаційні системи, стан захищенності, внутрішні кібератаки, зовнішні кібератаки.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІР	- інформаційні ресурси
ЗЗ	- засоби захисту
ІТС	- інформаційно-телекомунікаційна система
НСД	- несанкціонований доступ
АС	- автоматизована система
ПЗ	- програмне забезпечення
ПЗБ	- підсистема забезпечення безпеки
СЗІ	- служба захисту інформації
СУ	- система управління
ДССЗЗІ	- Державної служби спеціального зв’язку та захисту інформації
НД ТЗІ	- нормативні документи сфери технічного захисту інформації
SIEM	- Security information and event management, технологія управління інформаційною безпекою та подіями безпеки.
ДП	- динамічне програмування.

ВСТУП

Останні тенденції проведення кібернетичних атак, свідчать про розвиток форм, способів та методів, які застосовуються для проведення кібератак на систему управління інформаційними ресурсами та інформаційно-телекомунікаційні системи. Для ефективного функціонування ІТС доцільно використовувати у складі системи управління ІР відповідну підсистему забезпечення безпеки з можливістю проведення оцінювання та управління станом захищеності ІТС в режимі реального часу та в умовах постійно змінюючій природі кібератак.

Одним з найважливіших питань, що необхідно вирішити в процесі експлуатації ІТС є гарантування інформаційної безпеки, а для управління станом захищеності ІР необхідно застосувати спеціальне обладнання, алгоритми та методи, що гарантують безпечну роботу вузлів, компонентів, та ІТС в цілому.

У зв’язку з цим, до складу підсистеми забезпечення безпеки ІТС повинна входити система управління подіями інформаційної безпеки, яка на основі відповідних методів управління станом захищеності, буде оцінювати поточний стан ІТС та приймати управлінські рішення для підтримання належного рівня безпеки в ІТС .

Однак, запропоновані на сьогодні методи управління станом захищеності ІТС не враховують особливостей проведення кібератак внутрішнім і зовнішнім зловмисниками, а також мають низьку достовірність прийняття управлінського рішення щодо оцінювання стану захищеності ІТС та застосування засобів захисту. Водночас, основними вимогами, які пред’являються до методів управління станом захищеності ІР в ІТС є: робота в режимі реального часу; врахування загроз характерних інформаційно-телекомунікаційним системам; адаптивне функціонування системи захисту інформації з самоорганізацією; децентралізація управління та ієрархічно-розподільча структура; збільшення достовірності та повноти прийняття

управлінського рішення; зменшення математичної складності та ресурсної обтяжливості методів; застосування спеціальних вибірок про стан захищеності ІТС; можливість застосовування в системах з високою динамікою зміни топології; децентралізація управління та наявність ієрархічно-розподільної структури; мінімальне завантаження мережі службовою інформацією.

Таким чином, сьогодні спостерігається невідповідність між вказаними можливостями існуючих методів управління станом захищеності ІТС та вимогами до методів управління станом захищеності ІР в ІТС, для усунення якого поставлене наукове завдання, а саме: розроблення методів управління станом захищеності ІР від зовнішніх та внутрішніх кібератак на ІТС з використанням методів ідентифікації, динамічного програмування та опорних векторів. В ході досліджень було визначено наступні напрямки вирішення наукового завдання: розподіл системи управління станом захищеності ІТС на основі зовнішніх та внутрішніх кібератак, а також розроблення нових та удосконалення існуючих методів управління станом захищеності при проведенні зовнішніх та внутрішніх кібератак на ІТС на основі динамічного програмування, розподільчої ідентифікації та опорних векторів.

РОЗДІЛ 1
ХАРАКТЕРИСТИКА УПРАВЛІННЯ СТАНОМ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ, ЩО ОБРОБЛЯЮТЬСЯ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

1.1 Аналіз роботи систем управління інформаційними ресурсами

Вдосконалення та розвиток системи забезпечення безпеки, залишається на сьогодні одними з ключових питань. Система забезпечення національної безпеки грунтується на національних інтересах та формується з урахуванням реальних загроз, небезпек та викликів безпеці.

Підрозділи спеціального зв'язку та захисту інформації є суб'єктами забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, ІР та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, а також інших завдань відповідно до закону [1]. Служба Держспецв'язку забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі ІР та інформації, вимога щодо захисту якої встановлена законом [2]. Необхідність інформатизації СУ, створення баз даних ІР обумовлена стрімким ростом кількості виникнення військових конфліктів, як гібридних так і кібернетичних або інформаційних, що виконують ішні держави з метою дескридитування.

Слід приділяти вагому роль захисту ІР в умовах зростання загроз інформаційних та кібернетичних війн шляхом комплексного підходу до побудови та впровадження систем захисту інформації а також формування політики щодо інформації.

Інформаційні ресурси формуються і використовуються відповідно до соціальних процесів та різноманітних підходів до організації суспільної діяльності. Реалізація знань через втілення ІР виходить розвиток через використання сучасних інформаційних технологій, а для отримання і збереження переваг в умовах конкуренції кожна дія в інформаційному середовищі має значний вплив у світі фізичних ресурсів: предметних, фінансових або інших. Це систематизується в мережевих банках даних, з якими взаємодіють користувачі ІТС. Ці ресурси визначають споживчу цінність ІТС, через це потрібно: з частою періодичністю створювати і поповнювати ресурси; виконувати архівувацію та оновлювлення у встановлені проміжки часу; вичасне надання інформації за допомогою використання мереж.

До програмних ресурсів відносять мережеве ПЗ, а саме:

– мережеві операційні системи, серверне ПЗ, ПЗ робочих станцій;

– прикладне ПЗ;

– інструментальні засоби: утиліти, аналізатори проходження трафіку, засоби мережевого контролю, програми додаткових функцій, навігація (забезпечення пошуку інформації в мережі), обслуговування мережевих електронних поштових скриньок, криптозахист інформації, автентифікація.

Ресурси ІТС надають змогу обробляти дані, надавати якісний пошук у будь-якому місці інформаційно-телекомунікаційних систем, а також збір інформації та її зберігання. Набір мережевих ресурсів надає можливість переходу в стан інформаційних повідомлень, зв’язок між інформаційними системами та виробництва нових послуг та інформації.

ІР представляє упорядокввану інформацію, яка доступна при виокристанні інформаційних технологій, тобто забезпечення високої швидкісті обробки даних і застосування обчислювальної техніки, пришвидшений пошук інформації, розподіл даних, можливість доступу до інформації незважаючи на її місце розташування. ІР включають в себе відкриту інформацію (статистичну, соціологічну, інформацію державних

органів, правову, науково-технічну та довідкову), конфіденційну інформацію (в тому числі персональні дані) та таємну інформацію.

До найпопулярніших технологій в сфері ІТ відносять інформаційно-телекомунікаційну систему, а саме множину інформаційних та телекомунікаційних систем, що в співпрацюють, як одне ціле. Вагому роль у ході впровадження ІР у галузі життедіяльності суспільства країни відіграє ІТС з її інформаційними ресурсами і послугами.

Телекомунікаційна система становить системоутворюючу сукупність засобів телекомунікацій, що надає територіальновіддаленим об'єктам можливість інформаційної взаємодії шляхом обміну сигналами [5]. В такому випадку об'єктами є: системи мереж або кінцеві мережі та робочі пристрої абонентів в середині системи.

Мережевий інтерфейс робочого пристрою абонента безпосереднє мережеве обладнання у вигляді комутаторів та хабів (рис. 1.1).

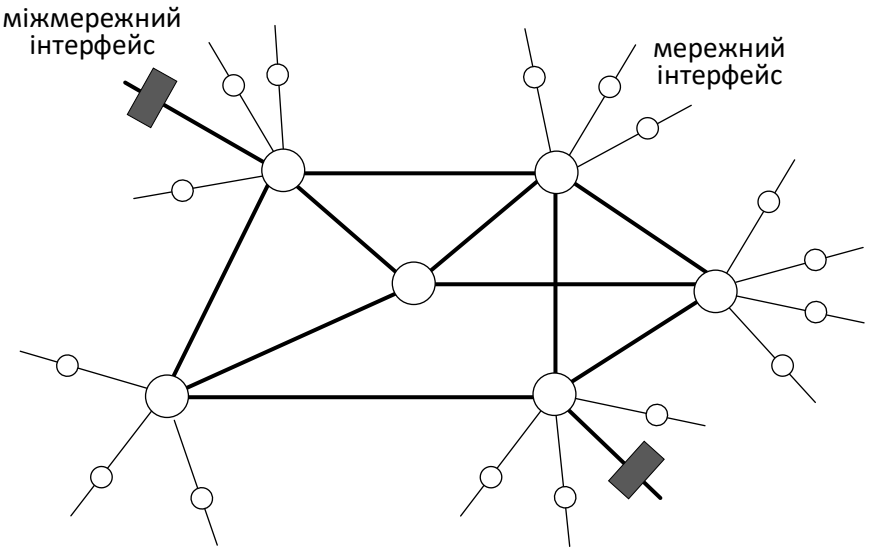

Рисунок 1.1 – Структура телекомунікаційної мережі

Телекомунікаційні системи класифікують за :

– типом режиму перенесення інформації (синхронні, асинхронні);

– технологічними характеристиками (середовищем передавання, заданою шириною смуги пропускання, якістю передавання сигналів, швидкістю передавання та ін.).

ІТС передбачає розгляд телекомунікаційної мережі в сукупності зі взаємодіючими за допомогою неї об’єктами [6]. В данному випадку ІС представляється, як телекомунікаційна система.

Усі процеси щодо роботи в ІС виконується реалізується в кінцевих системах мережі, а роль транспортної системи бере на себе телекомунікаційна мережа (рис. 1.2).

Параметри оцінки ефективності інформаційної системи встановлено, як міра ефективності мережі, що є системою розподільчих ресурсів і мають наступний перелік характеристик:

– часу обробки в мережі;
– затримки при передачі;
– варіанти затримок при передачі;
– зрозумілості роботи.

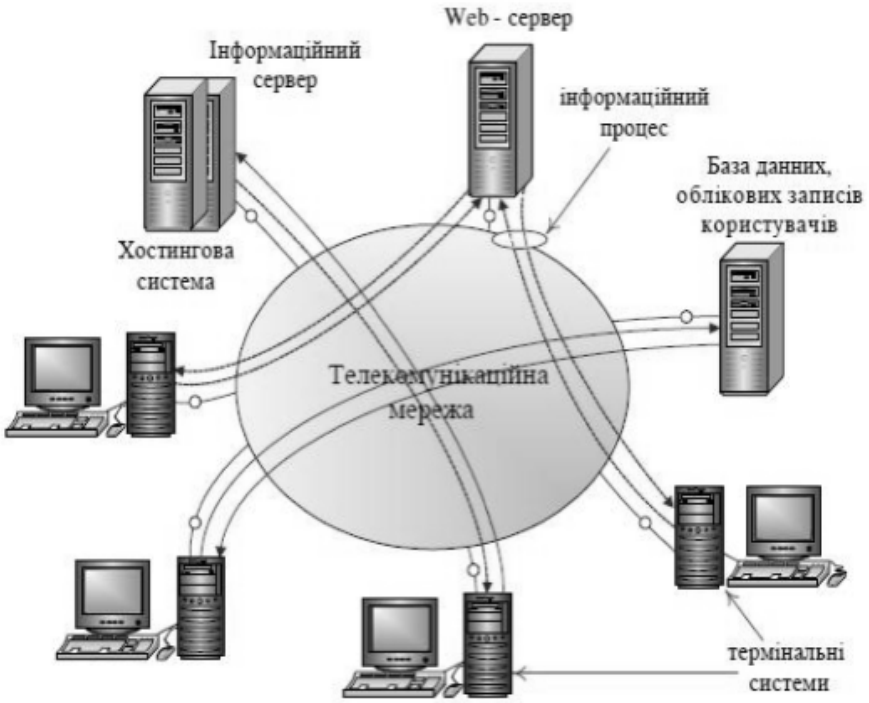

Рисунок 1.2 – Структура інформаційної системи

Інформаційно-телекомунікаційна система є набором робочих пристроїв абонентів (термінальних систем), комутаторів та хабів (кінцеві компоненти мережі) та сервіси надання послуг, що відповідають вимогам роботи користувачів та якості таких послуг. (рис. 1.3).

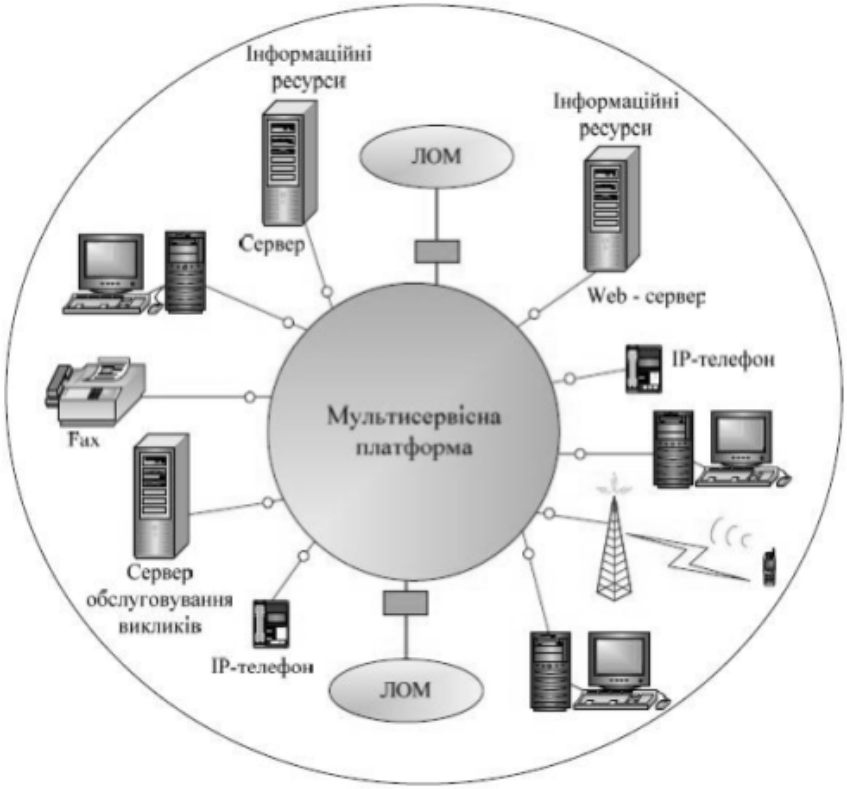

Рисунок 1.3 – Структура ІТС

Таким чином, ІТС надає змогу вирішити наступні завдачі, а саме:

– можливість обміну інформаційними повідомленнями різного типу (мультимедійні данні або звичайний текст);

– швидкість отримання запитуваної інформації з будь-якої частини мережі;

– автоматизація дій, що можуть виконуватись над інформацією, а саме обробка, накопичення, зберігання значних обсягів інформації в середині мережі.

Компоненти ІТС скаладють наступні елементи, а саме: обчислювальна техніка, програмне забезпечення, канали зв'язку, комутаційне обладнання,

бази даних та системи управління базами даних , системи захисту. Узагальнена структура ІТС представлена на рис. 1.4.

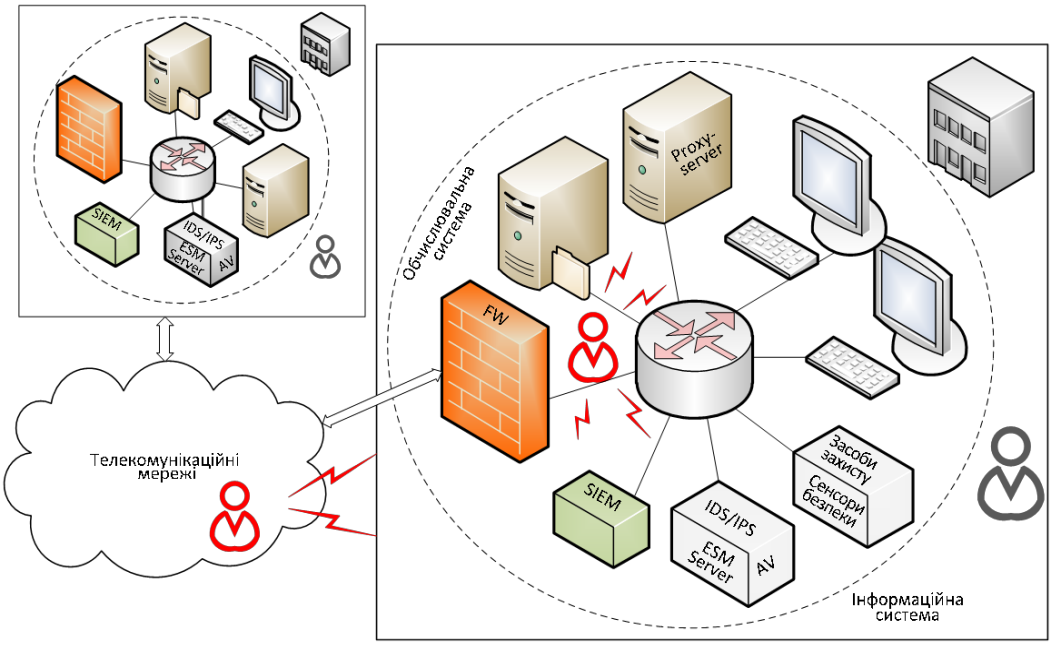

Рисунок 1.4 – Узагальнена структура ІТС

Інформаційно-телекомунікаційні системи, інформаційні ресурси ІТС, інформаційні продукти, проміжна і технологічна інформація, інформаційні сервіси ІТС та користувачі загалом функціонують та підлягають захисту в кіберпросторі, тобто у віртуальному просторі, що надає можливості для здійснення комунікацій, утворене в результаті функціонування сумісних (з'єднаних) інформаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [5, 7]. Для забезпечення безпеки кіберпростору необхідне впровадження комплексу систем і механізмів захисту, а саме систем [8]: автентифікації, авторизації, міжмережного екранування, розмежування доступу користувачів, криптографічних методів захисту інформації, антивірусного захисту елементів ІТС, віртуальні приватні мережі, виявлення та запобігання вторгнень, попередження втрати даних, управління захищеності, управління безпекою та подіями, аудиту.

При побудові ІТС важливо враховувати можливі вразливості, що виникають на кожному із рівнів моделі OSI, в таблиці 1.1 наведено відповідність вразливостей рівням моделі OSI.

Таблиця 1.1 Відповідність вразливостей рівням моделі OSI

Рівень OSI	Вразливості
Фізичний рівень	– втрата потужності; – фізичні крадіжки даних і устаткування; – фізичне пошкодження або знищення даних і устаткування; – несанкціоновані зміни у функціональному середовищі; – вимкнення фізичних каналів передачі даних; – приховане перехоплення за рахунок побічних електромагнітних випромінювань та наводок.
Канальний рівень	– підміна mac-адреси; – обхід технологій vlan; – переповнення cam-таблиць; – spanning tree для передачі пакетів у нескінченний цикл; – затоплення комутаторами всіх портів vlan.
Мережевий рівень	– підміна маршруту; – підміна ip-адреси; – проблеми одноразової ідентифікації.
Транспорт-ний рівень	– неправильна передача пакетів; – перевантаження за рахунок великої кількості звернень до номерів портів обмежує фільтрацію трафіку; – механізми передачі пакетів можуть бути предметом підміни і призводити захоплення контролю над мережею.
Сеансовий рівень	– слабкі механізми автентифікації; – передача під час сеансу інформації, такої як ім’я користувача і пароль у відкритому вигляді; – ідентифікація сеансу може бути предметом підміни і викрадення; – витік інформації на основі невдалих спроб автентифікації; – здійснення атаки на облікові дані для доступу в разі необмеженої кількості спроб на встановлення сеансу.
Рівень представ-лень	– погана обробка даних може призвести до збою програми; – ненавмисне використання зовнішніх даних, що вводяться в контексті управління може призвести до віддаленої маніпуляції або витоку інформації; – криптографічні недоліки можуть бути використані для обходу захисту конфіденційності.

продовження табл.1.1

Прикладний рівень	– використання безкоштовних ресурсів та програм невідомого походження; – недоліки програмного забезпечення, наявність backdoors; – недостатній контроль ЗЗ за принципом «все або нічого»; – надмірно ускладнений механізм контролю безпеки;

Зазначені основні вразливості впливають і на безпеку інформаційних ресурсів [9]. В цілому сучасні системи обробки ІР здебільшого функціонують в кіберпросторі та мають враховувати особливості функціонування ІТС. Тому доцільно висунути до ІТС множину вимог:

– робота в режимі реального часу;

– врахування загроз характерних ІТС;

– адаптивне функціонування СЗІ з самоорганізацією;

– децентралізація управління та ієрархічно-розподільча структура;

– збільшення достовірності та повноти прийняття управлінського рішення;

– врахування особливостей функціонування ІР;

– зменшення математичної складності та ресурсної обтяжливості методів.

В результаті аналізу можна винести наступні твердження: у сучасноу світі ІТС піддаються вразливостям, що перелічені вище. Якщо узагальнити вищезазначене, то стає зрозуміло, що продуктивність захисту ІТС визначає її змогу роботи в умовах впливу зашкоджуючих факторів та стійкість до атак.

Зважаючи на вищезазначене, доцільно провести аналіз вразливостей ІТС в умовах поставлених задач та викликів і загроз безпеки, а також загроз інформаційним, а також атак, які можуть бути реалізовані.

Взявши до уваги особливості процесу обробки інформаційних ресурсів засобами передачі та персоналом, пропонується під ІР розуміти взаємопов’язану сукупність інформації, носіїв інформації, обчислювальних ресурсів, засобів передачі та персоналу, що захищається системою захисту в ІТС.

Зазначимо, що існуючі сучасні ІТС становлять складову кіберпростору та в цілому призначені для функціонування ІР. Вразливості і загрози, які виникають на кожному рівні моделі OSI характерні і ІТС загалом. Тому для забезпечення безпеки ІР необхідно враховувати сучасні вразливості та їх властивості, а також механізми захисту та відповідні індикатори.

Розглянемо порядок забезпекчення відкрита інформація, що належить до ІР, а також інша відкрита інформація, вимога щодо захисту якої встановлена законом на прикладі АС підрозділів Держспецзв'язку.

Відповідно до [10], захисту в АС підрозділів Держспецзв'язку інформація з обмеженим доступом (включаючи персональні дані) та відкрита інформація, що належить до ІР, а також інша відкрита інформація, вимога щодо захисту якої встановлена законом. Захист інформації в АС має здійснюватися на етапах розробки, впровадження, експлуатації та виведення з експлуатації АС в усіх режимах її функціонування, на всіх технологічних етапах обробки інформації.

Вимоги щодо захисту інформації в АС визначаються нормативно-правовими актами та НД ТЗІ та встановлюються згідно із [10] відповідно до вищого ступеня обмеження доступу до інформації, що оброблятиметься в АС, умов і особливостей функціонування АС, класу АС.

Вищий ступінь обмеження доступу до інформації, що оброблятиметься в АС підрозділу Держспецзв'язку, встановлюється керівником підрозділу Держспецзв'язку, виходячи із завдань, покладених на цей підрозділ, виконання яких потребує обробки інформації з відповідним обмеженням доступу.

Для захисту інформації в АС створюється КСЗІ за порядком, визначеним в [11], з урахуванням специфіки та особливостей, встановлених в [10], та здійснюється підтвердження її відповідності вимогам технічного завдання на створення КСЗІ в АС, а також вимогам нормативно-правових актів та НД ТЗІ. Відповідність підтверджується за результатами державної експертизи КСЗІ.

У разі обробки в АС інформації, що підлягає захисту (крім інформації що становить державну таємницю), КСЗІ складається з комплексу ЗЗ від несанкціонованих дій з інформацією та з організаційних заходів захисту інформації.

КСЗІ в АС підрозділів Держспецзв'язку створюються виконавцями робіт за дозволом власника. Державна експертиза КСЗІ проводиться виконавцями шляхом експертних випробувань (за принципом неупередженості експертні випробування мають проводити фахівці виконавця робіт, які не брали участь у створенні КСЗІ, або підрозділ, який не брав участь у створенні КСЗІ). Проектні, експлуатаційні й інші технічні документи АС, КСЗІ в АС та документи щодо державної експертизи КСЗІ розробляються виконавцями робіт. Технічне завдання на створення КСЗІ в АС, програми і методики проведення державної експертизи КСЗІ погоджуються Департаментом захисту інформації Адміністрації Держспецзв'язку. Матеріали державної експертизи КСЗІ надсилаються до Департаменту захисту інформації Адміністрації Держспецзв'язку для їх аналізу, оформлення та реєстрації. Атестати відповідності КСЗІ набирають чинності з моменту їх реєстрації в Департаменті захисту інформації Адміністрації Держспецзв'язку.

У разі обробки в АС класу «2» із фізично-логічним об'єднанням або в АС класу «3» інформації, що становить державну таємницю, створення комплексів ТЗІ у складі КСЗІ та їх атестація, включаючи інструментальний контроль захищеності інформації від витоку технічними каналами, проводяться виконавцями робіт за дозволом згідно з їх секторальним розподілом. Проектні, експлуатаційні й інші технічні документи та документи щодо атестації комплексів ТЗІ розробляються виконавцями робіт за дозволом, затверджуються (погоджуються) відповідно до вимог цього Порядку. При цьому ТЗ на створення комплексів ТЗІ (якщо такі розробляються), програми та методики атестації комплексів ТЗІ погоджуються Департаментом захисту інформації Адміністрації Держспецзв'язку. Матеріали атестації комплексів ТЗІ (протоколи інструментального контролю захищеності інформації, акти

атестації комплексів ТЗІ) надсилаються до Департаменту захисту інформації Адміністрації Держспецзв'язку для їх аналізу та реєстрації актів атестації комплексів ТЗІ. Акти реєструються за Порядком реєстрації Адміністрацією Держспецзв'язку актів атестації комплексів технічного захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, затвердженим наказом Адміністрації Держспецзв'язку. За умов відповідності матеріалів атестації вимогам ТЗ на створення КСЗІ (або вимогам Технічного завдання на створення КСЗІ), Положення-023 та НД ТЗІ 3.6-003-2016 «Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації» акти атестації комплексів технічного захисту інформації реєструються Департаментом захисту інформації Адміністрації Держспецзв'язку та заносяться до реєстру.

Для організації, координації та виконання робіт із захисту інформації в АС у кожному підрозділі Держспецзв'язку створюється Служба захисту інформації.

Адміністратор безпеки зі складу СЗІ зобов'язаний:

– встановлювати та налаштовувати ПЗ, необхідне для функціонування підрозділу Держспецзв'язку;

– брати участь у проведені категоріювання та обстеження об'єктів електронно-обчислювальної техніки;

– брати участь у розробці проектів технічних та організаційно-розпорядчих документів, а також забезпечувати їх виконання;

– брати участь у впровадженні заходів захисту інформації в АС та здійснювати контроль умов використання АС відповідно до експлуатаційної документації;

– здійснювати поточне адміністрування та оновлення інформації комплекс (облікових записів користувачів, їх атрибутів доступу, прав доступу користувачів до об'єктів захисту в АС, журналів реєстрації подій, тощо);

– здійснювати/забезпечувати оновлення та здійснювати контроль за своєчасним оновленням антивірусних програмних засобів;

– здійснювати регулярний перегляд журналів реєстрації подій АС;

– надавати та змінювати права користувачів АС щодо доступу до інформації в АС;

– проводити технічне обслуговування здійснювати контроль за функціонуванням ЗЗ інформації;

– здійснювати опечатування вузлів та блоків ПЕОМ;

– вживати заходів щодо відновлення інформації після аварійних ушкоджень або уражень комп'ютерними вірусами;

– здійснювати поточний контроль стану захисту інформації в АС;

– оформлювати та вести технічну (експлуатаційну) документацію на АС.

Під час поточного контролю проводиться перевірка:

– виконання умов використання АС;

– виконання вимог приписів на експлуатацію об'єкта ЕОТ;

– працездатності технічних та криптографічних засобів захисту інформації, що входять до складу КСЗІ (тобто функціонування засобів захисту інформації відповідно до технічної документації на них), шляхом огляду та аналізу зовнішніх індикаторів працездатності;

– відповідності використання (експлуатації) технічних та криптографічних засобів захисту інформації, що входять до складу КСЗІ, вимогам, що визначені в експлуатаційній документації на ці засоби та на КСЗІ;

– виконання вимог (відповідності та своєчасності) оновлення антивірусних програмних засобів;

– журналів реєстрації подій АС.

Для захисту відкритої інформації, що належить до ІР, в АС Держспецзв'язку створюються КСЗІ, які мають забезпечувати захист інформації від модифікації та/або від блокування доступу до інформації, у тому числі з використанням комп'ютерних вірусів. Комплексна система

захисту в АС у такому випадку складається з комплексу засобів захисту від НСД та організаційних заходів.

До відкритої інформації належить інформація, яка не має законодавчо встановлених обмежень щодо доступу до неї. Рішення щодо віднесення відкритої інформації до ІР і створення КСЗІ в АС, де оброблятиметься відкрита інформація, що належить до ІР, приймає керівник підрозділу Держспецзв'язку, де експлуатуватиметься АС. Рішення має прийматися з огляду на те, що до ІР належить така систематизована (тобто окремі документи, файли, масиви документів, бази даних, реєстри, тощо) інформація, яка є доступною за допомогою інформаційних технологій і яка:

– створена співробітниками Держспецзв'язку в процесі виконання ними своїх основних функціональних обов'язків за сферою діяльності Держспецзв'язку або створення якої передбачено законодавством (у тому числі відкрита інформація про діяльність Держспецзв'язку, яка оприлюднюється в мережі Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними системами, власником або розпорядником яких є Держспецзв'язку, відкрита інформація, яка знаходиться у володінні Держспецзв'язку та накопичена в базах даних або в системах довідково-енциклопедичного характеру, спотворення, модифікація або знищення якої може завдати шкоди діяльності Держспецзв'язку);

– створена суб'єктами владних повноважень (органами державної влади, іншими державними органами, органами місцевого самоврядування, іншими суб'єктами, що здійснюють владні управлінські функції відповідно до законодавства) та військовими формуваннями в процесі виконання ними своїх функцій, визначених законодавством;

– створена з використанням бюджетних коштів юридичними особами, що фінансуються з державного та/або місцевих бюджетів.

При побудові комплексної системи захисту відкритої інформації, що належить до ІР, в АС Держспецзв'язку рішенням керівника підрозділу Держспецзв'язку визначається об'єкт, де технічними засобами АС

оброблятиметься відкрита інформація, що належить до ІР. Виконавець робіт з побудови КСЗІ проводить обстеження середовищ функціонування АС, розробляє модель загроз для інформації від несанкціонованих дій та модель порушника (вихідними даними для розробки моделі загроз для інформації від НСД є результати обстеження середовищ функціонування АС: ІТС, інформаційного середовища і технології обробки інформації та середовища користувачів АС), розробляє політику безпеки інформації в АС та технічне завдання на створення КСЗІ в АС, впроваджує ЗЗ інформації (проводить встановлення, інсталяцію, ініціалізацію, конфігурування, адміністрування і налагодження комплексу засобів захисту інформації від НСД) та здійснює інші види робіт відповідно до [10].

1.2 Огляд та аналіз атак на інформаційні ресурси.

З огляду на ключову роль системи забезпечення кібербезпеки значною постає вимога забезпечення ІР в кіберпросторі та, як наслідок, спроможності СУ та ПЗБ або кібербезпеки виконувати точне та доречне визначення впливу загроз на стан безпеки ІР на основі оцінки зміни значень множини окремих показників. Основним питанням при прийнятті рішень в підсистемі, що забезпечує кібербезпеку є найбільш точна дефініція впливу загроз на стан безпеки ІР в цілому.

Одним з важливих факторів розвитку інформаційних технологій є глобальне об’єднання програмних продуктів, технічних засобів та мереж передачі інформації. Таке поєднання надає сучасним технічним засобам нові можливості, зручності у користуванні та керуванні. Проте зворотною стороною таких переваг є додаткові вразливості програмно-керованих технічних засобів. Крім відомих технічних каналів витоку інформації слід враховувати загрози несанкціонованого віддаленого доступу до технічних засобів, наявні в них уразливості та незадекларовані функції, а також можливості впровадження шкідливого програмного забезпечення та

програмних закладок. Зазначені вразливості можуть «експлуатуватись» з метою порушення конфіденційності, цілісності, достовірності та доступності інформації, яка обробляється технічними засобами, а також порушення конфіденційності інформації, яка циркулює в місцях їх встановлення.

Сучасне робоче місце в загальному випадку обладнане рядом технічних засобів, які у процесі інформаційно-технологічного розвитку перейшли від «звичайних» технічних засобів до програмно-керованих технічних засобів. До таких засобів можна віднести системи зв'язку, телебачення, відеонагляду, ІТС, мультимедійні системи тощо. Технічні засоби зазначених систем мають у своєму складі модулі або інтерфейси передачі даних, які за певних умов можуть бути використані в якості каналів несанкціонованого керування технічними засобами. Використання програмно-керованих технічних засобів, які мають у своєму складі модулі та інтерфейси передачі даних, потребує вжиття додаткових заходів із захисту інформації, враховуючи сучасні загрози [12].

З позиції теорії систем, підсистеми забезпечення кібербезпеки відносяться до класу складних систем, математично строге моделювання яких, як правило, становить актуальне завдання [13].

Порушення захищеності у сфері використання ІТС розподіляються на такі види:

– НСД до роботи АС, баз даних та мереж;

– створення за для поширення або збуту шкідливих ПЗ або технічних засобів, а також їх розповсюдження або збут;

– несанкціонований розповсюдження інформації з обмеженим доступом, яка зберігається в АС, мережах або на носіях такої інформації;

– злочини, як метод отримання неправомірної вигоди, що отримана шляхом використання інформаційної зброї.

Інформаційні технології дозволяють отримати важливий ефект тонкого регулювання інформаційного впливу залежно від одержувача. Можна виготовити багато варіантів віртуальної реальності, більш того, її (реальність)

можна набудовувати на конкретного споживача у момент запиту на одержання [14].

На цей час в усьому світі постає питання щодо захисту національних інформаційних ресурсів у зв’язку з розширенням доступу до них через відкриті інформаційні мережі. Враховуючи, що постійно збільшується кількість комп’ютерних злочинів, реальною стала загроза інформаційних атак на більш високому рівні для досягнення політичної і економічної мети.

ІТС та ІС мають широкі можливості надання впливу на формування суспільної думки, поширення дезінформації, тиску на прийняття політичних, економічних або військових рішень, маніпуляція інформаційними ресурсами противника.

Поняття інформаційна зброя об’єднує електронний і людський аспекти. З одного боку, суспільство все більше підпадає у залежність від інформаційних технологій, тому повсякденна робота багатьох АС і ІТС має життєво важливе значення. З іншого боку, головним стратегічним об’єктом впливу інформаційної зброї залишаються люди. Основними завданнями застосування інформаційної зброї у мережі є:

– порушення конфіденційності, цілісності та доступності інформації;

– подолання систем захисту;

– обмеження доступу законних користувачів, дезорганізація роботи технічних засобів, комп'ютерних систем.

Види інформаційної зброї у глобальних мережах [14]:

– деструктивні програми типу “комп’ютерні віруси” – програми, що мають здатність до самовідтворення, і, як правило, здатні здійснювати дії, які можуть порушити функціонування системи і/або зумовити порушення політики безпеки. Мають властивість впроваджуватися у програми, передаватися лініями зв'язку, мережами передачі даних, виводити з ладу системи керування і т.д.;

– деструктивні програми типу “троянський кінь” – програми, які є авторизованим процесом, окрім виконання документованих функцій, здатні

здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми;

– деструктивні програми типу “логічна бомба” – програмні закладні пристрої, що заздалегідь впроваджують в інформаційно-керуючі центри військової або цивільної інфраструктури, які уводяться в дію за сигналом або у встановлений час;

– “люк” – це залишені розробником не документовані функції, використання яких дозволяє обминути механізми захисту;

– засоби подавлення інформаційного обміну та фальсифікації в ІТС, передусім, державного і військового призначення;

– засоби нейтралізації тестових програм;

– різноманітні помилки, які свідомо вводяться супротивником до ПЗ;

– електромагнітний вплив на електронно-обчислювальну техніку з метою знищення інформації, виведення з ладу обладнання, модифікації системних настроювань та створення умов для НСД до ІР.

Ці засоби надають можливості супротивнику завдавати інформаційних ударів. Наприклад, порушити комунікації, паралізувати телефонну мережу, заплутати фінанси, порушити функціонування космічних апаратів.

Інформаційну зброя стає небезпечною при реалізації наступних факторів: універсальність, економічність, прихованість, множинна реалізація програмно-апаратних форм, радикалььний вплив, вибір відповідного часу і місця застосування. Її легко замаскувати під засоби захисту, це дозволяє проводити наступальні дії анонімно, без детекції зловмисника.

Активне використання глобальних мереж для ведення інформаційної війни обумовлено наявністю ряду переваг: оперативність, економічність (залучення невеликої кількості персоналу і матеріальних засобів для вирішення поставлених завдань: наприклад, застосування комп’ютерних технологій для виведення з ладу систем керування конфронтуючої сторони у визначених умовах може призвести до більш значного ефекту за умови менших витрат порівняно із використанням традиційних засобів (вогневого

ураження, радіоелектронної боротьби), прихованість джерела впливу, дистанційний характер впливу, масштабність можливих наслідків, комплексність подачі інформації та її прийнятність, доступність інформації.

Для запобігання або нейтралізації наслідків застосування інформаційної зброї необхідно вжити наступних заходів [14]:

– захист матеріально-технічних об'єктів, що складають фізичну основу інформаційних ресурсів;

– забезпечення нормального і безперебійного функціонування баз і банків даних;

– захист інформації від НСД, перекручування або знищення;

– збереження якості інформації (своєчасності, точності, повноти і необхідної приступності).

Атаки реалізуються зловмисниками для порушення конфіденційності, цілісності або доступності ІР, що зберігається, обробляється та циркулює в ІТС. З цією метою, як правило, використовують вразливості ІТС, тобто нездатність системи протистояти реалізації певної загрози або сукупності загроз [15].

Для одержання інформації про можливі атаки на інформаційні ресурси, вимога щодо захисту якої встановлена законодавством, інформаційні наслідки їхнього прояву, а також виявлення найбільш небезпечних кібератак використовують модель поводження інформаційних систем та ІТС при впливі на них кібератак (рис. 1.5), де КБА – комбінації кібератак, S – підмножина станів ІС, ВФ – виконання функцій ІР, ІНПІС – інтенсивності переходів ІС, МСЗІР – модель системи захисту інформаційних ресурів [16].

Проведемо аналіз таких характеристик безпеки ІР, як: загрози ІР, вразливостей ІТС та атак на ІР. Також розглянемо сучасні бази даних, які містять детальний опис вразливстей атак та загроз, які взаємодіють між собою на рівнях моделі OSI.

У моделі OSI, взаємодія між системами проходить у вигляді двох моделей – ієрархічної та розподільної&

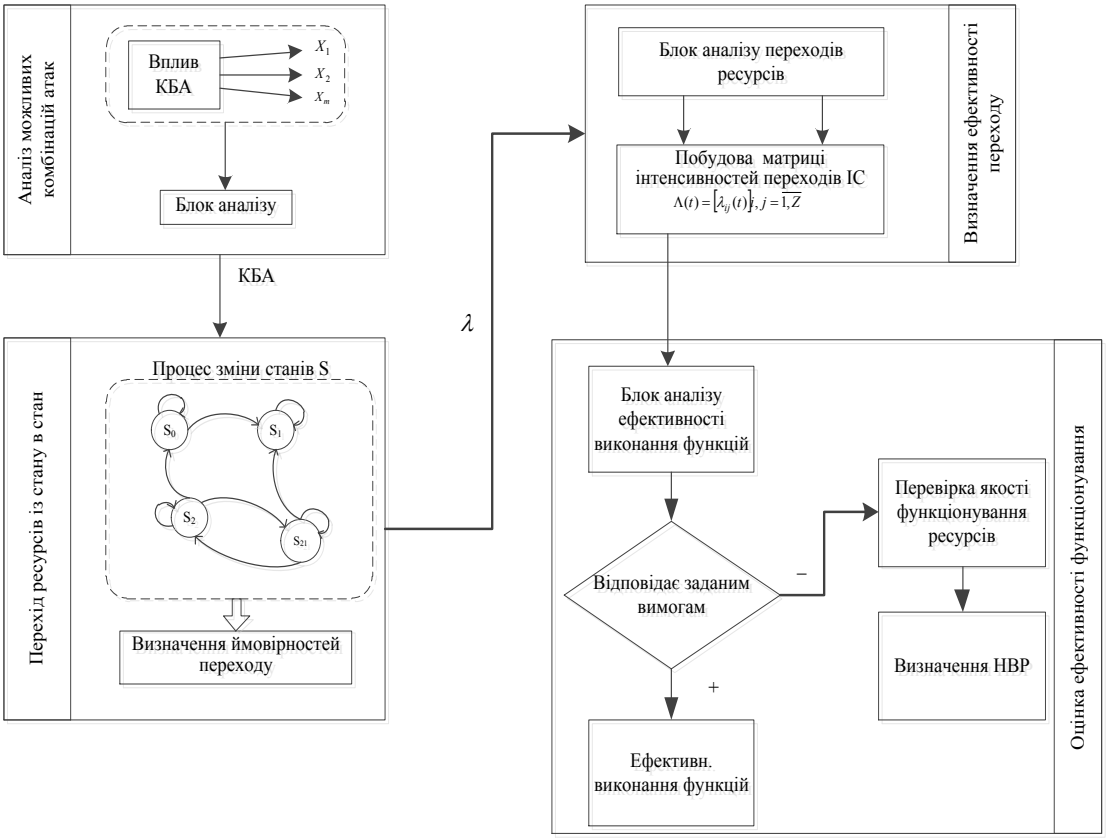

Рисунок 1.5 – Модель поводження системи при впливі атак

Розглянемо бази даних вразливостей:

– CVE - Довідка щодо файлів щодо вразливості та зворотного зв'язку. Важливою складовою системи є маркування CVE - унікальні ідентифікатори, присвоєні кожній відомій вразливості безпеки. CVE має понад 98 000 записів про окремі вразливості [17]. Основною відмінністю є найбільш повне і систематиче, тому цю систему беруть за основу при відповідності записів вразливості при обробці інших даних бази даних, що забезпечує ефективний пошук в будь-якому місці ІТС збір та зберігання даних Група мережевих ресурсів надає можливість переходу до стану інформаційних повідомлень, взаємодії між інформаційними системами та виробництва нових послуг та інформації.

Основними елементами структури вихначення та запису виявлених вразливостей є:

1) статус – в цьому полі може міститися або значення Entry (перевірена запис), або значення Candidate (ще не перевірена вразливість);

2) фаза – в цьому полі міститься значення етапу розвитку вразливості, а також дата присвоєння зазначеного етапу. Можуть бути наступні фази:

– пропозиції вразливості (Proposed);

– проміжна фаза вразливості (Interim);

– модифікації вразливості (Modified);

– встановлення вразливості (Assigned);

3) опис – поле містить опис вразливості;

4) посилання – в даному полі містяться посилання на інші джерела із зазначенням конкретної адреси інтернет-ресурсу опису вразливості і ідентифікатора джерела;

5) голоси – поле містить імена членів голосування, які прийняли рішення про занесення вразливості в базу;

6) коментарі – вноситься ім'я автора коментаря та його текстовий зміст.

Також в елементах записів вразливостей міститься тип вразливості, ім'я та ідентифікатор. Ім'я вразливості має формат «CVE-YYYYNNNN»,
де YYYY – це рік виявлення вразливості, а NNNN – її порядковий номер.

Національна база даних вразливостей США (NVD) – NVD це сховище даних управління вразливістю стандартів уряду США, представлених за допомогою протоколу автоматизації вмісту безпеки (SCAP). Ці дані дозволяють автоматизувати управління уразливістю, вимірювання рівню безпеки та відповідність вимогам. NVD включає бази даних посилань на контрольний список безпеки, недоліки програмного забезпечення, пов'язані з безпекою, неправильні конфігурації, назви продуктів та показники впливу. На 2021 рік база даних вразливостей NVD має більш ніж 150000 записів вразливостей [18].

Вказані вразливості зловмисник може використати для вторгнення в ІТС що призведе до порушення цілісності, доступності та конфіденційності інформації, що протікає в ІТС, або для шкідливого впливу на функціонування ІТС [26].

Взявши до уваги вищезазначене, можна зробити висновок, що у ІТС повинна бути передбачено можливість виявлення та запобігання вторгнень, що можуть бути реалізовані значною кількісьтю різного роду кібератак. Щоб забезпеччити дану можливость СЗІ містить у своєму складі систему управління пдіями інформаційної безпеки, функціонування якої повинно здійснюватися на основі відповідних методів [27].

Під порушенням безпеки слід розуміти дії, що порушують безпеку та призводять до несанкціонований доступу до ІТС. Значення атаки слід інтерпретувати, як зусилля, що можуть призвести до виконання існуючої загрози. Однак, загроза визначається, як деякі події, обставини які стають або потенційно можуть стати причиною порушення функціонування складових ІТС, та нанесення збитків[28, 29].

Розглянемо нині існуючі типи атак на ІТС обробки IP (таблиця 1.2), та їх параметри [30, 31]. Особливу увагу слід приділити останньому типу атак. З точки зору віддаленої атаки вкрай важливим є взаємне розташування суб’єкта й об’єкта атаки, тобто знаходяться вони в різних або в однакових сегментах. Під час атаки в сердині сегменту мережі, суб’єкт і об’єкт атаки є частиною одного сегменту системи. У випадку атаки із зовні суб'єкт і об’єкт атаки знаходиться у різних сегментах системи мережі. Цей класифікаційний ознака дає можливість судити про “ступінь віддаленості” атаки.

Таблиця 1.2 – Класифікація атак

Ознака атаки	Тип атаки	Характеристика атаки
За характером впливу	пасивні	Атаки, що не мають безпосереднього впливу на роботу системи, але можуть порушувати її політику безпеки. Важко виявити. Після атаки не залишається ніяких слідів. Приклад: прослуховування каналу зв'язку в мережі.

продовження табл.1.2

За характером впливу	активні	Атаки, що безпосередньо впливають на роботу системи (зміна конфігурації ІТС, порушення працездатності і т. д.) і порушують прийняту в ній політику безпеки. Практично всі типи віддалених атак є активними. Існує можливість виявлення, так як в результаті здійснення атаки в системі відбуваються певні зміни.
За метою впливу	порушення кон-фіденційност	Перехоплення інформації. Приклад: прослуховування каналу в мережі.
	порушення цілісності	Спотворення інформації. Прикл.: впровадження помилкового об'єкта в ІТС.
	порушення доступності	Не відбувається НСД (зберігається цілісність і конфіденційність), проте доступ до інформації легальних користувачів неможливий.
За умовою початку здійснення впливу	атака на запит від об'єкта, що атакується	У разі запиту атакуючий очікує передачі від потенційної мети атаки запиту певного типу, який і буде умовою початку здійснення впливу. Ініціатором здійснення початку атаки є об'єкт, що атакується. Приклад: DNS- і ARP-запити в стеці TCP / IP.
	атака по настанню події, що очікується на об'єкті	У разі настання події, атакуючий здійснює постійне спостереження за станом операційної системи віддаленої цілі атаки і при виникненні певної події в цій системі починається вплив. Ініціатором здійснення початку атаки є об'єкт, що атакується. Приклад: переривання сеансу роботи користувача з сервером в мережевих операційних системах без видачі команди LOGOUT.
	безумовна атака	У разі безумовної атаки початок її здійснення безумовно по відношенню до мети атаки, тобто атака здійснюється негайно і безвідносно до стану системи і атакується об'єкта. Ініціатором здійснення початку атаки є атакуючий.
За наявністю зворотного зв'язку з об'єктом, який атакується	зі зворотнім зв'язком	Атака зі зворотним зв'язком – атака, під час якої атакуючий отримує відповідь від об'єкта на частину своїх дій. Ці відповіді потрібні, щоб мати можливість продовжити атаку і/або здійснювати її більш ефективно, реагуючи на зміни, що відбуваються в системі.

продовження табл.1.2

За наявністю зворотного зв'язку з об'єктом, який атакується	без зворотного зв'язку (односпрямована атака)	Атака без зворотного зв'язку – атака, яка відбувається без реакції на поведінку системи, що атакується. Приклад: відмова в обслуговуванні.
За кількістю атакуючих	розподілена	Атака, вироблена двома або більше атакуючими на одну і ту ІТС, об'єднаними єдиним задумом і в часі.
По розташуванню атакуючого щодо атакуємого об'єкту	нерозподілена	Нерозподілена атака проводиться одним атакуючим.
	внутрисегментна	Атака, при якій суб'єкт і об'єкт атаки знаходяться всередині одного сегменту мережі (сегмент – фізичне об'єднання станцій за допомогою комунікаційних пристроїв не вище канального рівня).
	міжсегментна	Міжсегментна атака – атака, при якій суб'єкт і об'єкт атаки знаходяться в різних сегментах мережі.

Практично внутрисегментну атаку (внутрішню) здійснити набагато простіше, ніж міжсегментну (зовнішню). Також зовнішня віддалена атака представляє більшу небезпеку, ніж внутрішня. Це пов’язано з тим, що в разі внутрішньої атаки її об’єкт і атакуючий можуть перебувати на відстані багатьох тисяч кілометрів один від одного, що може істотно перешкодити заходам по протидії атакам.

Опис стратегій здійснення атак, що використовуються при проведенні атак на ІТС представлено в проекті корпорації The MITRE Adversarial Tactics, Techniques and Common Knowledge [24]. В свою чергу база даних атак та модель для оцінки поведінки зловмисників (при здійсненні вторгнень) являє собою матрицю ATT@CK, яка описує найбільш небезпечні фази атаки на ІТС.

Матриця ATT@CK - це база знань з протиборчих тактик та методів, заснованих на спостереженнях у реальному світі. База знань ATT@CK її

беруть за основу під час розробки визначених моделей та методологій загроз, як в урядових так і в приватних установах.

Використвуючи зазначену базу знань та співставляючи параметри трафіку, що поступають на мережеві пристрої можна виокремити параметри, які характеризують тактики та реалізації внутрисегментних атак від внутрішнього зловмисника та між сегментних атак від зовнішнього зловмисника.

Таким чином, MITRE ATT@CK, дозволяє класифікувати кібератаки та описати як починається атака, де проявляється, які програми або дії запускає і так далі. А також виявивти та ідентифікувати зловминиска в залежності від етапу реалізації атаки та від місця його розташування.

Існуючі на сьогодні атаки, що застосовують для вторгнення в ІТС діляться на 5 категорій. Кожна з цих категорій має декілька типів атак, що реалізують вторгнення. Однак, кожен тип такої атаки має в собі загрозу мережі відповідно до рівнів мережевої моделі OSI та виконує функцію здійснення деструктивного впливу на мережу [25].

До наведених категорій атак відносяться:

– атаки реалізовані побічними каналами, що спрямовані на практичні вразливості в криптографічних систем. Такі атаки використовуть інформацію про фізичні процеси в пристрої, що не мають розгляду в теоретичній частині алгоритму криптографії. Далі наведено список найпопулярніших Side-channel атак: probing attack, fault–induction attack, electromagnetic analysis attacks, power analysis attack, timing attack;

– DoS атаки – це атаки в мережі, що створюють ситуації в системі, що піддається вторгненню, шляхом відмови в обслуговуванні. Зазначені атаки характеризуються генерацією великого об`єму трафіка, що призводить до перенавантаження та блокування сервера.

– U2R атаки – реалізуються шляхом отримання користувачами привілеїв адміністратора. Типи атак, що відносять до U2R: buffer overflow, load module, perl, root kit;

– R2L атаки – такі атаки визначаються, як отримання доступу стороннього користувача до мережі з віддаленої станції. R2L атаки поділяються на наступні види атак: guess passwd, multihop, phf, warezclient, imap, warezmaster, ftp write, spy;

– Probe-атаки – атаки із застосування сканування мережевих портів для отримання конфіденційної інформації. Такі атаки поділяють на види, наприклад: nmap, portsweep, satan, ipsweep та інші.

Наявність множинних параметрів під час визначення яких можна пов'язати з окремим типом атак, що характеризує кожну атаку окремо [25]. Данне значення несе в собі послідовність параметрів з'єднання, а саме: тип використовунваного протоколу, тривалість з'єднання, послуги в мережі, кількість інформації повідомлення, поточний стан з'єднання, кількість термінових пакетів, кількість невдалих спроб з'єднання та інше.

Як правило атака потрапляє до IP під виглядом текстового повідомлення відео матеріалу, аудію матеріалів або інших типів даних. Таке повідомлення має наступні компоненти: передзаголовок, заголовок, контрольна сума, текст повідомлення і найголовніше це завершення повідомлення, що і ідентифікуються системою виявлення вторгень, як встановлена атака. Наведені типи атак використовуючи свій функціонал можуть завдавати вплив на: управління інформаційно-телекомунікаційними ресурсами, поділ доступу до IP, обмін пакетами, доступ до шифрування та кодування, управління IP.

Враховуючи особливості роботи ІТС що виконують обробку IP доцільно висунути ряд вимог до методів управління станом захищеності IP в ІТС:

– робота в режимі реального часу;

– врахування загроз характерних ІТС;

– адаптивне функціонування системи захисту інформації з самоорганізацією;

– децентралізація управління та ієрархічно-розподільча структура;

– збільшення достовірності та повноти прийняття управлінського рішення;

– зменшення математичної складності та ресурсної обтяжливості методів.

Проведений аналіз вразливостей та атак на ІР, що обробляються в ІТС показав різноманіття побудов інсуючих баз вразливостей, кожна з яких має переваги та недоліки. Орієнтація існуючих на сьогодняшній день баз вразливистей, що використовуються в експертних системах є найбільш значущим підходом до побудови баз вразливостей. Існуючі ІТС обробки ІР містять великий перелік зовнішніх і внутрішніх вразливостей, а реалізація даних вразливостей виконується множиною використання різнопланових атак. Збільшення популяції вразливостей у окремій частині або модулі ІТС може нести в собі появу нових або додаткових, вже існуючих, загроз щодо безпеки ІР, що в ній оброблюються. Зважаючи на вказані фактори, для того щоб визначити множину параметрів під час оцінюванки захищеності ІР та виявлення нових вразливостей, слід гарантувати функціонування системи управління подіми ІБ використовуючи перелічені вимоги, параметрів та характерних особливостей сучасних системи управління ІР.

1.3 Аналіз методів управління станом захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах

Аналіз подій безпеки, що отримані від мережевих пристроїв в реальному часі, забезпечує технологія Security information and event management (SIEM). SIEM представлено додатками, приладами або послугами, і використовується також для журналювання даних і генерації звітів. Сегмент систем управління безпекою, що пов'язаний з моніторингом в реальному часі, кореляцією подій, оголошеннями і відображенням на кінцевих пристроях зазвичай називають управлінням подіями. Друга область забезпечує довготривале зберігання, аналіз і звітність за накопиченими даними відома як управління інформаційною безпекою. У міру зростання потреб у додаткових можливостях

безперервно розширюється і доповнюється функціональність даної категорії продуктів.

Рішення SIEM були введені на початку 2000-х у формі або SIM-рішення, або рішення SEM. Системи на цьому початковому етапі з 2000 по 2005 рік забезпечували базову агрегацію журналів між різними типами систем, а також основні методи кореляції подій. Для виявлення нападу ці системи покладалися лише на відомі атаки загроз. Отже, вони були абсолютно не в змозі мати справу з атаками нульових днів на системи організації.

Основний акцент зроблено на управління привілеями користувачів, служб каталогів та іншим змінам конфігурації, а також забезпеченню аудиту та огляду журналів, реакцій на інциденти. Система має змогу до збору інформації, аналізу, групує їх у бази даних, проводить аналіз поведінки підставою яких є попередні спостереження. На практиці використовується реалізація за допомогою визначених компонентів: агенти (збір даних з різних джерел); сервери-колектори (акумуляція інформації, що надійшла від агентів); сервер баз даних (зберігання інформації); сервер кореляції (аналіз інформації). Вхідною інформацією для SIEM-систем може служити практично будь-яка інформація.

SIEM є центральним елементом центру управління кібербезпекою, і взагалі будь-якої розвиненої системи захисту державної установи. Вони збирають дані про інциденти від розрізнених СЗІ, таких як міжмережеві екрани, IPS і антивіруси, дозволяють виявляти підозрілі і потенційно небезпечні ситуації [33].

Перші SIEM рішення виникли близько десяти років тому, еволюціонувавши з систем управління журналами подій. Потреба в таких рішеннях обумовлена лавиноподібним зростанням кількості загроз, їх ускладненням і появою цілеспрямованих атак, в тому числі з використанням різних векторів проникнення. SIEM може бути реалізована або апаратно, або у вигляді програмного забезпечення (віртуальне пристрій), а розміщуватися –

як на території замовника, так і в хмарі. Схема роботи SIEM представлена на рис. 1.7.

SIEM збирає дані від всіх вузлів мережі і розрізнених пристроїв захисту (міжмережеві екрани, системи виявлення та запобігання вторгнень, антивіруси на робочих станціях і т.д.), в реальному часі проводить їх кореляцію і оповіщає співробітників в разі виявлення невідповідності встановленим правилам. Ці правила можна налаштувати в залежності від потреб організації по пріоритетності загроз і скорочення помилкових спрацьовувань. Чим більш витонченими стають атаки, тим більша потреба в удосконаленні механізмів їх розпізнавання.

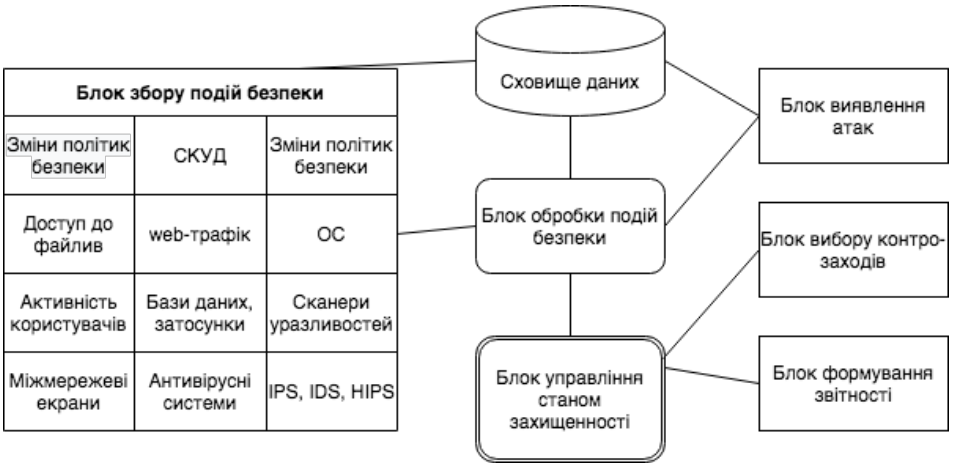

Рисунок 1.7 – Структурна схема існуючої системи управління подіями інформаційної безпеки

Існує безліч міжнародних рейтингів виробників SIEM. Найвідоміший з них - «магічний квадрант» Gartner, який відносить до лідерів чотири компанії: IBM, Splunk, LogRythm і McAfee.

Кібератака являє собою навмисні дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (в тому числі інформаційні, програмні, апаратні засоби, інші технічні або технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності ІР, що обробляються в ІТС; отримання НСД до зазначених ресурсів; порушення безпеки, сталого, надійного режиму функціонування ІТС; використання ІТС, її ресурсів та

засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту [34].

Забезпечення безпеки ІТС оброки ІР пов’язано з вразливостями ІТС, які зумовлені передачею інформації в кіберпросторі, масштабованістю, необхідністю збору достнього об’єму інформації про стан системи для роботи протоколів та застованих методів на різних рівнях мережевої моделі OSI [9, 26]. Визначені вразливості потенційно може використати зловмисник для вторгненення або проведення атак на ІТС з метою шкідливого впливу на її функціонування.

Управління станом захищеності ІТС є актуальною задачею при визначенні рівня безпеки ІР та оцінці достатності засобів безпеки, що було впроваджено.

Захищеність ІР являє собою сукупність станів, в яких забезпечується безпека ІР, тобто їх конфіденційність, цілісність і доступність. Процес управління станом захищеності ІТС передбачає перевірку можливості порушення таких станів доступними зловмиснику способами. Виконання цієї процедури вимагає вирішення наступних завдань: збір інформації про компоненти ІТС; обробка цієї інформації і побудова прийнятної моделі ІТС на основі отриманих результатів для подальшого використання при оцінці ризиків ІТС. В свою чергу забезпечення безпечного функціонування ІТС представляє собою безперервний процес прийняття рішення з оцінювання стану захищеності ІТС, ефективності реалізованих засобів захисту, дестабілізуючих факторів та визначення оптимального набору засобів захисту.

Існуючі методи управління станом захищеності [34-37], в основі яких покладено імовірнісний підхід або перевірка відповідності вимогам, заданих на етапі технічного завдання, не враховують реальний стан захищеності ІТС, а лише дають наближену оцінку, засновану на даних, отриманих експертним шляхом.

Першим етапом при управлінні станом захищеності ІТС є проведення оцінювання поточного стану ІТС, що реалізується відповідними методами. Класифікацію методів оцінювання захищеності [30] представлено на рис. 1.8.

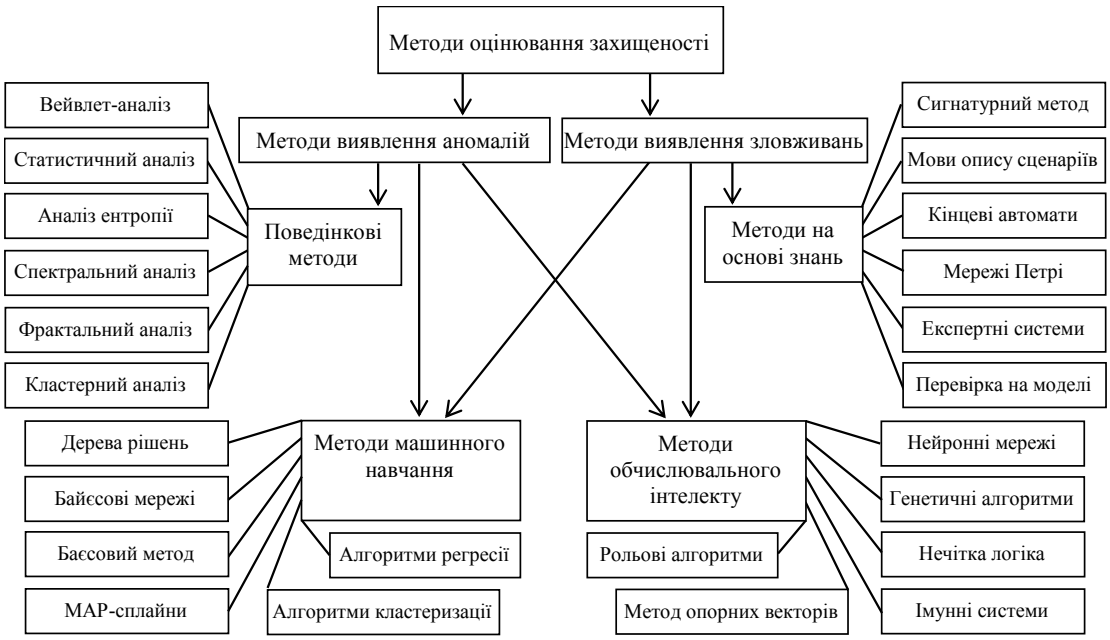

Рисунок 1.8 – Класифікація методів оцінювання захищеності

Зазначені вище методи як правило використовуються в системах, які визначають наступними параметрами, а саме: необмеженістю ресурсів, великим часом під час прийняття управлінських рішень, низькою точністю прийняття управлінських рішень, неврахування можливості застосування в нечіткому середовищі, наявність чіткої структури не пристосованої до перерозподілу функціональних можливостей, та інше [38,39]. Тому доцільно висунути множину вимог для методів управління станом захищеності ІТС а саме: робота в режимі реального часу; врахування загроз характерних ІТС; адаптивне функціонування СЗІ з самоорганізацією; децентралізація управління та ієрархічно-розподільча структура; збільшення достовірності та повноти прийняття управлінського рішення; зменшення математичної складності та ресурсної обтяжливості методів.

Як видно з вищезазначеного аналізу при врахування великої кількості вимог, що були висунуті, слід модернізувати вже існуючі методів управління

станом захищеності які функціонують в СЗІ [40-44] для вищезазначених характеристичних особливостей.

Таким чином проведено аналіз методів управління станом захищеності та прийняття рішень з застосування ЗЗ в ІТС та визначено, що використання проаналізованих методів недостатньо відповідає визначеним вимогам для забезпечення захищеності ІР в ІТС. Для забезпечення безпеки ІР, що циркулюють в ІТС, а також оцінка реалізованих методів і механізмів безпеки в СЗІ, слід комбінувати та удосконалювати розглянуті методів відповідно до вимог СЗІ та роботи ІТС.

Висновки до розділу 1

У даному розділу магістерської роботи було розглянуто сучасний стан функціонування ІР в ІТС. Досліджено роботу систем управління станом захищеності в ІТС та визначено основні завдання щодо роботи підсистеми оцінювання, як складової СЗІ. Проаналізовано основні типи атак на ІР, вразливості ІТС які використовуються при проведені кібератак, а також методи управління станом захищеності ІР в ІТС. Під час аналізу виявлено, що існуючі методи здатні оцінювати рівень захищеності на основі повної вибірки параметрів кібератак, та не враховують характеристичні особливості функціонування ІТС, що в свою чергу не враховує можливості пошуку нових типів кібератак, підбору управлінських рішень направлених на підтримання стану захищеності системи, та призводить до зменшення рівня достовірності і збільшення часу прийняття рішень.

РОЗДІЛ 2
РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИБОРУ МЕТОДІВ УПРАВЛІННЯ СТАНОМ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ

2.1 Модель порушення захищеності інформаційних ресурсів, що обробляються в інформаційно-телекомунікаційних системах

У зв'язку з тим, що СЗІ ІТС обробки ІР має забезпечувати реалізацію прийнятої політики безпеки, керувати розмежуванням доступу, сигналізувати про небезпечні події, виявляти атаки на ІР, проводити оцінку захищеності системи та вживати заходи щодо управління станом захищеності ІР в ІТС [6, 15], то СЗІ має відслідковувати весь трафік, що циркулює в ІТС. Для цього СЗІ функціонує на всіх рівнях моделі OSI, виконуючи: контроль з'єднань, трафіку, аналіз мережевих пакетів, оцінку станів функціонування елементів системи.

При використанні ІТС, метою порушення захищеності ІР може бути приховане управління мережевими та кінцевими ресурсами або вплив на програмні або апаратні засоби ІТС [44-47]. Реалізація зазначеної мети досягається використанням методів, що направлені на вразливості ІТС. В свою чергу це може призвести до втрати ІР внаслідок віддаленого керування кінцевим або мережевим обладнанням. Відомі підходи до моделювання забезпечення захисту і порушення захищеності ІР використовують різні математичні підходи, що беруть до уваги завдання доступу до об'єктів, організації процедури захисту ІР та її вартості але не розглядають вплив різних типів атак на імовірність реалізації порушення зовнішнім або внутрішнім зловмисником.

Під вразливістю розуміємо властивості інформаційно-телекомунікаційної системи (архітектурний, програмний, організаційний або

інший недолік), які можуть бути використані для здійснення деструктивних впливів. В свою чергу вразливість являє собою характеристику захищеності ІТС, а будь-яка вразливість ІТС несе в собі загрозу впливу на ресурси системи за допомогою атаки [26]. Класифікацію загроз безпеці інформаційним ресурсам при вторгненні в ІТС представлено в таблиці 2.1.

Таблиця 2.1 – Класифікація загроз безпеці ІР в ІТС

Загрози безпеки інформаційних ресурсів																									
За ступенем наміру дії		За характером дії		За джерелом загрози		За впливом на властивості інформації			За технічною реалізацією			За способом дії на об'єкт			За розміром нанесеного збитку				За способом реалізації		За досягнутою метою		За кінцевим результатом		
навмисні	ненавмисні	активні	пасивні	внутрішні	зовнішні	конфіденційність	цілісність	доступність	сканування	відмова від обслуговування	вторгнення	безпосередні	на ІТС управління	опосередковані	загальні	локальні	часткові	імітаційні	вплив однієї загрози	вплив множин загроз	проміжні	кінцеві	віддалений контроль	блокування	захоплення

З таблиці видно, що ІТС складається з множини взаємопов’язаних функціональних систем, серед яких є СЗІ. В свою чергу СЗІ містить ряд підсистем. Важливе місце в СЗІ займає підсистема управління станом захищеності, яка функціонує в тісній взаємодії з іншими підсистемами. В основу роботи підсистеми управління станом захищеності ІТС покладені відповідні методи оцінювання поточного стану захищеності ІТС та методи прийняття управлінських рішень про застосування механізмів і засобів захисту. Підсистема управління станом захищеності ІТС отримує дані з суміжних підсистем СЗІ, аналізує поточний стан ІТС та ефективність реалізованих ЗЗ та приймає управлінське рішення щодо достатності вжитих захисних засобів або необхідність підвищення стану захищеності.

Вказані загрози впливають на ІТС та її компоненти, які забезпечують передачу інформації у відповідності до функціональних особливостей кожного об’єкта системи.

Узагальнена архітектура підсистеми управління станом захищеності ІТС та взаємодія її елементів представлені на рис. 2.1.

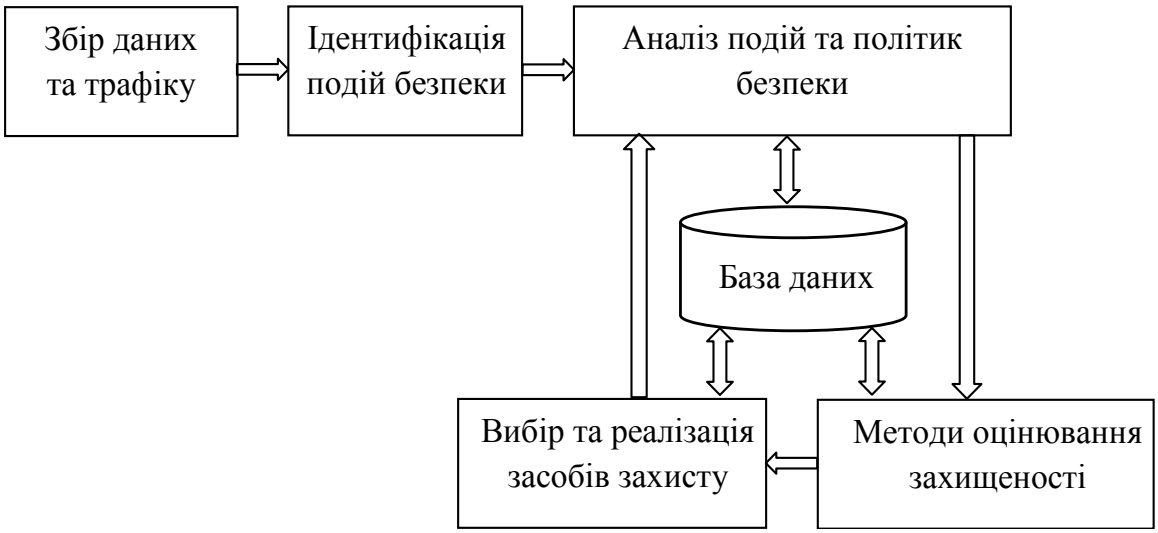

Рисунок 2.1 – Узагальнена схема підсистеми управління станом захищеності.

Важливо зазначити, що для ефективного функціонування СЗІ, підсистема управління станом захищеності повинна проводити власну оцінку базуючись на даних про реалізацію основних типів атак, що здійснюються із зовні (зовнішні) або на частини в середині системи (внутрішні) та зважаючи на стратегії щодо порушення захищеності системи.

Атаки реалізуються множиною способів (вплив загрози на один чи декілька об’єктів; вплив множини загроз на один об`єкт чи декілька об`єктів, тощо). Такі підходи спрямовані на досягнення проміжної або кінцевої мети наслідком якої є віддалений контоль системи, відмова в обслуговуванні системи, блокування системи або заволодіння частини ІТС або в цілому.

Слід зазначити, що проаналізувавши здійснення порушень на практиці або атак на засоби ІТС, можна зробити висновок, що об’єктом атаки є правила і процедури, що виконують обробку та передачу інформації в ІТС.

Показники реалізації порушення захищеності ІР та здійснення атак на ІТС залежать від: кваліфікації того хто реалізує порушення, обладнання яке застосовується для реалізації, покладених задач, стратегії здійснення порушення та інше. Зловмисник, в свою чергу, розраховує на вразливості об'єкту порушення та низький рівень забезпечення безпеки ІТС. Також зловмисник має множину інструментів для реалізації порушень/атак, які в свою чергу впливатимуть на імовірність успішного їх здійснення [65].

Необхідно розробити модель порушення захищеності ІТС для оцінки ймовірності реалізації порушень безпеки ІР від зовнішніх і внутрішніх загроз.

Ймовірності виявлення порушення на кожному етапі проведення атаки в загальному вигляді матиме вигляд:

$$R = P_z \times P_v \times \bar{\omega} \tag{2.1}$$

де P_z – ймовірність виявлення порушення на окремій фазі проведення атаки; P_v – імовірність використання вразливостей на окремій фазі проведення атаки; ϖ – коефіцієнт здійснення атаки.

Як наслідок, імовірність того, що ІТС на окремій фазі проведення атаки при використанні СЗІ може бути застосована для виявлення j_z типів атак, у разі реалізації варіантів проведення атак Z, де $Z = 1,...,Z$, буде визначатися: $P_a = 1 - \prod_{z=1}^{Z}(1 - P_{j_z})$

$$P_a = 1 - \prod\nolimits_{z=1}^{Z}(1 - P_{j_z}) \tag{2.2}$$

Так як варіанти проведення порушень Z можуть реалізовуватись j_z типами атак, то існування джерела проведення порушення Z визначається апріорною імовірністю $P(Z)$. Водночас, реалізація варіантів проведення порушення Z типами атак j_z визначатиметься імовірністю $P(j_z / Z)$.

Тоді імовірність реалізації варіантів проведення порушень на окремій фазі проведення атаки типами атак j_z від джерела атак матиме вигляд:

$$P_Z = P(Z)P(j_z/Z) \tag{2.3}$$

Імовірність порушення на окремій фазі проведення атаки за деякий час t, може здійснитися j_z типами атак з деякою частотою λ. З цього виходить, що час t доцільно розподілити на x рівних частин. Тоді імовірність того, що на відрізку часу відбудеться порушення визначатиметься:

$$P_t = \lambda t/x \tag{2.4}$$

В свою чергу на окремій фазі проведення атаки імовірність того, що серед x рівних частин часу відбудеться j_z типів порушень буде визначатися:

$$p_{j_z}(t) = \left(\frac{\lambda t}{x}\right)^{j_z}\left(1-\frac{\lambda t}{x}\right)^{x-j_z} \tag{2.5}$$

Під час моделювання процесу оцінювання стану захищеності ІТС мають бути враховані стратегії проведення кібератак на ІТС. Реалізація варіантів проведення порушень Z на окремі об'єкти ІТС l можна описати законом ймовірності. До об'єктів на які може поширитись дана імовірність можливо віднести:

$P(Z/l)$ – імовірність впливу варіантів проведення кібератак Z на окремий об'єкт ІТС l;

$P(Z/\sum l)$ – імовірність впливу варіантів проведення кібератак Z на множину об'єктів ІТС l;

$P(\sum Z/l)$ – імовірність впливу множини варіантів проведення кібератак Z на окремий об'єкт ІТС l;

$P(\sum Z/\sum l)$ – імовірність впливу множини варіантів проведення кібератак Z на множину об'єктів ІТС l .

Розглядаючи ймовірність порушень у ІТС в цілому необхідно врахувати мінімальний час, протягом якого відбувається порушення на кожній фазі проведення атаки [48].

Методи впливу множини кібератак R на інформаційні ресурси визначають множину потенційних атак R та з кожним інформаційним ресурсом X_m, де $m=\overline{1,M}$, зв'язують підмножину R_n, де $n=\overline{1,N}$, відносно повної множини R, що можуть впливати на цей ресурс та складають таблицю інтенсивностей β_{nm}.

Для ІР X_m інтенсивність сумарного потоку кібератак з множини R дорівнює [16]

$$\beta_m(t)=\sum_{n=1}^{N}\sum_{m=1}^{M}\beta_{nm}(t) \qquad (2.6)$$

Розглянуті вирази, свідчать про те, що виявлення атак в ІТС залежить від швидкості адаптації існуючих СЗІ до нових загроз. А рівень безпеки ІР буде залежить від вибору стратегії порушення захищеності ІТС.

2.2 Модель протидії порушенням захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах

Модель захисту інформації повинна відображати основні процеси, які протікають в ІТС для покращення процесів ЗІ. Дані процеси представлено, як процеси розподілу і використання ресурсів, що використовують на захист інформації. В даний час існує значна кількість засобів та способів забезпечення захисту ІР, що обробляються в ІТС [55-60]. Удосконалення СЗІ потребує побудови моделі протидії порушенням захищеності ІР в ІТС, враховуючи системний характер впливу на ІТС різних за характером, місцем застосування та фізичною природою загроз.

Використання методів моделювання при забезпеченні належного рівня захищеності ІР призвело до розробки деякої кількості формальних моделей

безпеки [4], що спомогає підтриманню відповідного рівня захищеності де за основу взято об’єктивні тведження математичних теорій.

Побудова моделі, що враховує найбільш значний перелік причин впливу і надає змогу визначати ймовірність виникнення вразливості та реалізації загрози, обчислити час її реалізації і збитки, що може заподіяти ця загроза, визначати ефективність упровадження засобів захисту та стан захищеності системи [50-52].

Основою побудови моделі є опис об’єктів у вигляді сукупності елементів, пов’язаних між собою певними відносинами. Моделі опису атак:

– етапна модель – розглядає атаку як послідовність декількох ізольованих етапів, не надає можливості оцінювання успішності кожного етапу;

– дерева атаки – надає велику ступінь деталізації і можливість введення оцінок за деякими критеріями, але, не може бути використана для моделювання атак, оскільки не забезпечує засобів динамічного моделювання, включення в модель умов зовнішнього впливу та не забезпечує вибору наступного етапу на підставі результатів попереднього.

– графова модель – призначена для оцінювання складності порушення безпеки ІТС, враховує поточні значення параметрів ІТС та передбачає аналіз умов, необхідних для реалізації атаки [51, 52].

Ступінь адекватності механізмів захисту інформації, які реалізовані в ІТС, ризиків, що існують в середовищі та загрози безпеці характерезуються ступінь захищенності ІТС. Взаємодію загроз, ресурсів ІТС та СЗІ описує узагальнена типова модель процесу захисту з повним перекриттям загроз [49], яку представлено на рис. 2.2.

В даній моделі вважається, що кожній загрозі СЗІ існує визначений механізм захисту. Реалізована за наведеним принципом СЗІ не дозволяє впливати загрозам на області, які захищаються. Основним положенням захисту з повним перекриттям є теза про те, що ІТС повинна мати хоча б один ЗЗ на кожному можливому шляху впливу загроз на ресурси ІТС. Наведену

модель варто поєднувати з іншими типами моделей СЗІ. При синтезі систем забезпечення безпеки в ІТС такий підхід дозволяє мінімізувати витрати ресурсів ІТС для забезпечення заданого рівня захищеності ІР.

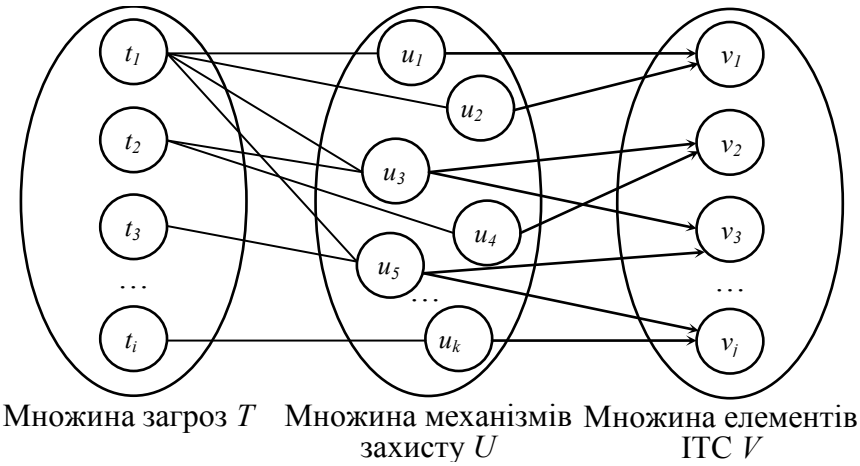

Рисунок 2.2 – Типова модель процесу захисту інформації з повним перекриттям

Уразливість СЗІ представляє собою можливість здійснення певної загрози у відповідності до визначеного об’єкту. Під уразливістю на практиці визначають не можливість здійснення атаки, а властивості СЗІ, які сприяють здійсненню атаки, або потенційно можуть бути використані.

В механізмах захисту (m_k) СЗІ визначено такі області:

1. Області уразливості механізмів захисту U, на які впливають загрози, де $U = \{u_r\}$ – набір уразливих місць СЗІ, $r = \overline{1,R}$ – кількість уразливих місць;

2. Бар’єри захисту B, що використовуються в СЗІ для блокування загроз, які несуть вплив на області уразливості СЗІ, де $B = \{b_g\}$ – набір бар’єрів захисту, які є в СЗІ, $g = \overline{1,G}$ – кількість бар’єрів захисту.

Також існують бар’єри, які перешкоджають здійсненню таких загроз в СЗІ з повним перекриттям загроз. Дана модель потребує проходу всіх визначених загроз виключно через механізми захисту для використання користі запропонованої моделі. [49].

Вплив загроз аналітично описують у вигляді функціональних залежностей, які зв'язують характеристики різних типів загроз $t_i \in T$ та об'єкти захисту $v_j \in V$.

Кожна з величин $v_j \in V$ залежить від координат уразливостей r та координат бар'єрів g. Ступінь залежності величин v_j залежить від уразливостей $u_r \in U$ та бар'єрів $b_g \in B$ і визначається відповідно до передатних функцій $a_{ik}(p), c_{ik}(p), d_{ik}(p)$, де p – оператор Лапласа.

Використовуючи матричні визначення, можна записати дану систему рівнянь у вигляді векторів:

$$V(p) = T(p) \times A(p) + U(p) \times C(p) + B(p) \times D(p) \qquad (2.7)$$

де $V(p), T(p), U(p), B(p)$ – матриці-стовпці розмірності $j \times 1$; $A(p), C(p), D(p)$ – матриці-стовпці розмірності $1 \times j$.

На практиці значно складніше отримати точні значеня A та C через важку формалізацію поняття загрози, уразливості та бар'єра. Такий варіант не дозволяє визначити зв'язки у СЗІ, не та ускладнює пристосування СЗІ в реальному часі, що залежить від реалізованих атак та не враховує впливів загроз, про які ще відсутні будь-які відомості.

Дані моделі необхідно використовувати коли ще не сформовано загальну архітектуру системи, і необхідно визначити проміжну оцінку ефективності СЗІ, тобто під час проектування СЗІ.

З метою усунення зазначених недоліків та урахування особливостей обробки ІР засобами ІТС висунемо множину вимог:

– робота в режимі реального часу;

– врахування загроз характерних ІТС;

– адаптивне функціонування системи захисту інформації з самоорганізацією;

– децентралізація управління та ієрархічно-розподільча структура;

– збільшення достовірності та повноти прийняття управлінського рішення;

– зменшення математичної складності та ресурсної обтяжливості методів.

– простота побудови математичної моделі оцінки впливу загроз на стан захищеності.

На основі проаналізованих уразливостей ІТС обробки ІР та з метою оцінки ефективності СЗІ і оцінювання стану захищеності ІР, що в них циркулює, доцільно побудувати модель протидії порушенням захищеності ІР в ІТС.

Суть моделі протидії порушенням захищеності ІР в ІТС полягає у зміні структури функціонування елементів моделі у порівнянні з вищезазначеним прикладом. На стан захищеності елементів ІТС та ІР в цілому впливає в певний момент часу множина зовнішніх і внутрішніх загроз, які направлені на порушення цілісності, доступності, конфіденційності елементів СЗІ та ІТС або проведення деструктивного впливу на програмну, апаратну, інформаційні складові самої системи. Також на стан захищеності ІТС впливає множина механізмів захисту, які реалізовані в ІТС та направлені на забезпечення безпеки. У ІТС механізми захисту реалізуються на основі алгоритмів навчання з учителем на етапі розробки самої ІТС, та алгоритму навчання без учителя, який реалізується у процесі функціонування ІТС. Саме перетин зазначених множин та наявність інструментів захищеності ІТС в цілому визначає поточний стан захищеності самої ІТС. Що в свою чергу дозволяє запропонувати для рекомендації управлінське рішення для підтримки належного стану безпеки та визначити механізми протидії на кожну окрему загрозу виходячи із цільової функції або мети управління безпекою.

Відомі підходи до оцінювання захищеності ІТС та її складових використовують схожі методики багатовимірного порівняльного аналізу, які в основному ґрунтуються на методах таксономії з елементами факторного аналізу. При цьому результати застосування методик залежать від кваліфікації

виконавця внаслідок помітної частки суб'єктивізму та функціональних особливостей моделей [49–51].

Для зменшення обсягу вхідних даних під час оцінювання стану захищеності ІТС і підвищення об'єктивності і оперативності пропонується здійснити визначення порядку математичного аналізу вхідних даних, якими виступають оцінки захищеності ІТС, з метою визначення стану захищеності ІР в цілому. Математичний апарат оцінки має бути гнучким до переліку загроз безпеці ІР та параметрів атак за умови забезпечення оперативного оцінювання поточного стану захищеності ІТС. За таких умов важливою є вимога забезпечення працездатності формальних методів за короткими обмеженими вибірками про стан захищеності.

Розпізнавання станів захищеності ІТС здійснюється наступним чином. Необхідно, використовуючи інформацію про стани ІТС та їх класифікацію, знайти таке правило, за допомогою якого можна було б з мінімальним числом помилок класифікувати нові стани за даними про отримані параметри атак.

Узагальнену типову модель, що описує взаємодію загроз, засобів захисту ІТС та множину станів захищеності ІТС представлено на рис. 2.3.

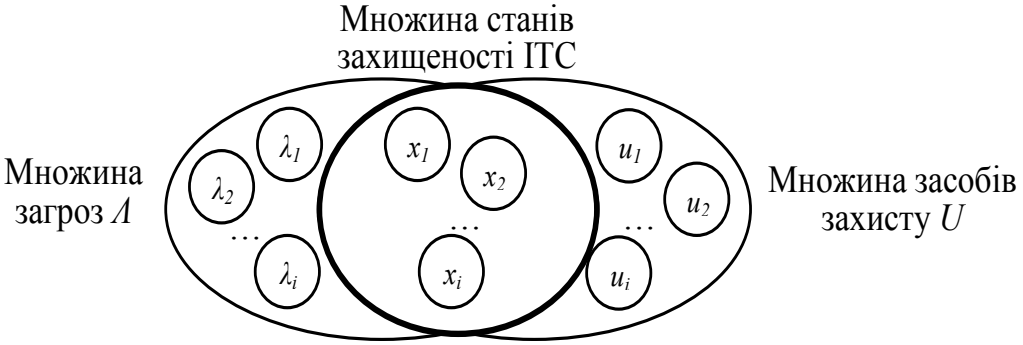

Рисунок 2.3 – Типова модель протидії порушенням захищеності ІР.

Класами можуть бути стани захищеності ІТС. Приклад для двох класів: стан захищеності ІТС погіршується; стан захищеності ІТС покращується. Приклад для трьох класів: стан захищеності ІТС погіршується; стан захищеності ІТС залишається без змін; стан захищеності ІТС покращується. Очевидно, що кількість класів може бути довільною та визначатися умовою однозначної класифікації поточної ситуації.

Отже, зміна стану захищеності інформаційних ресурсів, як процес протікає в певній фізичній системі, яка не може бути представлена детермінованою системою.

Математична модель протидії порушенням захищеності інформаційних ресурсів в ІТС визначається в результаті послідовного розв'язання наступних завдань:

– визначення початкової множини загроз, об'єднаної в конкретний момент часу в вектор загроз, та зміни координат вектора за певний період спостереження;

– оцінка чисельних значень рівнів загроз на обраних часових зрізах фазового простору моделі;

– пошук оптимального направляючого вектора розділяючої гіперплощини для множини векторів зміни рівнів загроз.

Виходячи з вищезазначеного, можна зробити висновок, що оцінювання стану захищеності ІТС залежатиме від швидкості адаптації існуючих СЗІ до нових загроз, коректної ідентифікації вхідного трафіку та виявлення параметрів атак за внутрішнім або зовнішнім ознакам.

Запропонована модель протидії порушенням захищеності ІР в ІТС на відміну від подібних існуючих на сьогодні моделей, які призначені для оцінювання впливів можливих атак і загроз різного рівня та прийняття обґрунтованого рішення щодо реалізації СЗІ ІТС, надає можливість оперативно оцінювати поточний стан захищеності ІТС за умов забезпечення працездатності формальних методів за короткими обмеженими вибірками про параметри засобів захисту ІТС та параметри загроз, що впливають на елементи ІТС. Рекомендації щодо застосування даної моделі дозволить отримувати поточні оцінки стану захищеності ІР, надати додатковий час на підготовку та проведення заходів реагування на загрози з метою посилення безпеки ІР.

2.3 Вибір математичного підходу використання методів управління станом захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах

Забезпечення ефективного функціонування ІР в ІТС можливе лише за наявності системи управління, здатної приймати управляючі рішення в умовах впливу кібератак. Функціонування ПЗБ не можливе без системи управління станом захищеності, основним завданням якої є оцінюваня поточного стану системи та приймання управлінських рішень для підтримання належного рівня безпеки ІР в ІТС на основі аналізу трафіка ІТС.

На сьогоднішній день системи управління подіями інформаційної безпеки інтенсивно розвиваються в напрямку інтелектуалізації, при цьому істотно змінюється технологія прийняття управлінських рішень.

Одним із шляхів підвищення ефективності заходів захисту ІР в ІТС є забезпечення умови своєчасної оцінки їх стану. Значущою виявляється умова своєчасного виявлення змін у стані захищеності ІР та безпеки ІТС і здатності враховувати вплив зовнішніх і внутрішн іх кібератак. Ця задача вирішується через оцінювання стану безпеки ІТС та рівня захищеності ІР на основі алгоритмів ідентифікації та розподілу параметрів тафіку, динамічного програмування та методу опорних векторів.

Відомі методичні підходи до управління станом захищеності ІР в ІТС та безпеки її складових [53-58] використовують методики порівняльного аналізу за умов великої кількості вимірів, що в більшості випадків базуються на методах таксономії з елементами факторного аналізу.

Для зменшення обсягу вхідних даних при управлінні станом захищеності ІР і підвищення достовірності та оперативності оцінювання пропонується наступний апарат. Визначимо порядок проведення математичного аналізу для оцінки рівнів загроз безпеці ІТС, що в данному випадку є вхдними данними для обчислення, з метою встановлення стану захищеності ІР. За данних умов математичний підхід до оцінки повинен бути

адаптивним до набору загроз безпеки ІР за умови, забезпечення оперативного оцінювання поточного стану рівня захищеності ІР. В такому випадку постає необхідність здатності роботи формальних методів за обмеженими вибірками даних спостереженняза короткий період часу.

Є деяка множина спостережень, які відносяться до p різних класів. Компонентами вектора є окремі загрози безпеці ІТС. Використовуючи інформацію про спостереження та їх класифікацію, необхідно знайти підхід, який дозволить з мінімальною кількістю помилок упорядкувати вперше отримані спостереження.

Стан ІТС задається вектором x, а його класифікація – числом ω (ω може приймати p значень: 0, 1, …, $p-1$). Вектором стану ІТС буде вектор, компонентами якого виступатимуть оцінки стану захищеності ІР. Розмірність вектора відповідатиме кількості загроз, що подаються до розгляду.

Порядок відшукання вектора наведено в [59], де задача побудови гіперплощини, що розділяє дві множини векторів, зводиться до відшукання максимуму виведеної квадратичної форми в додатному квадранті. Одним з найбільш ефективних алгоритмів максимізації недодатно визначеної квадратичної форми є метод максимізації квадратичної форми [60].

Оскільки стан захищеності ІР являє собою часовий зріз властивості захищеності ІТС і описується значенням відповідного показника в певний фіксований момент часу, то при проведенні оцінювання ІТС доцільно використовувати метод динамічного програмування.

Існує великий клас об’єктів і процесів, управління якими здійснюється на основі обмеженого числа рішень, прийнятих послідовно в деякі фіксовані моменти часу. Визначення закону керування для таких процесів пов’язане з рішенням так званої задачі багатокрокового вибору .

Кожний безперервний процес можна представити як багатокроковий, якщо розглядати його в дискретні моменти часу.

Підхід, що дозволяє знайти оптимальне рішення на основі багатокрокових процесів ухвалення рішення, одержав назву динамічного

програмування (ДП).

В основі методу динамічного програмування лежить принцип оптимальності, сформульований Ричардом Ернстом Беллманом [61].

Оптимальна стратегія визначається лише станом системи в даний момент і не залежить від того, як система прийшла в дану точку.

Під стратегією розумітимемо правило прийняття рішень. Принцип оптимальності можна сформульований наступним чином.

Якщо траєкторія системи оптимальна на відрізку часу $[t_н, t_к]$, то кінцева ділянка цієї траєкторії на відрізку $[t', t_к]$ у свою чергу є оптимальною траєкторією, де $t_н \leq t' \leq t_к$ – довільний момент часу.

Із принципу оптимальності можна одержати необхідні умови оптимальності для безперервних і дискретних систем.

Метод ДП широко застосовується для оптимізації дискретних систем. Переваги методу ДП:

1) ДП являє собою засіб рішення задач, які можуть бути вирішені й іншими методами. Цінність методу полягає в тому, що багатокроковий процес прийняття рішення заміняється послідовністю однокрокових процесів ухвалення рішення.

2) ДП дає математичний апарат для рішення задач, які раніше не вміли вирішувати. Зокрема, варіаційні задачі з обмеженнями типу нерівностей, рішення яких пов'язане зі значними труднощами, вирішуються методом ДП.

3) ДП має велику загальність і може застосовуватись для широкого кола задач.

Для вирішення поставленого завдання, визначимо основні етапи управління станом захищеності ІР в ІТС. Під час побудови етапів управління станом захищеності доцільно врахувати загальну структуру побудови системи управління подіями безпеки до складу якої входять методи оцінювання захищеності від зовнішніх і внутрішніх загроз.

Структурно–логічна схема існуючої системи управління подіями інформаційної безпеки в ІТС представлено на рис. 2.4.

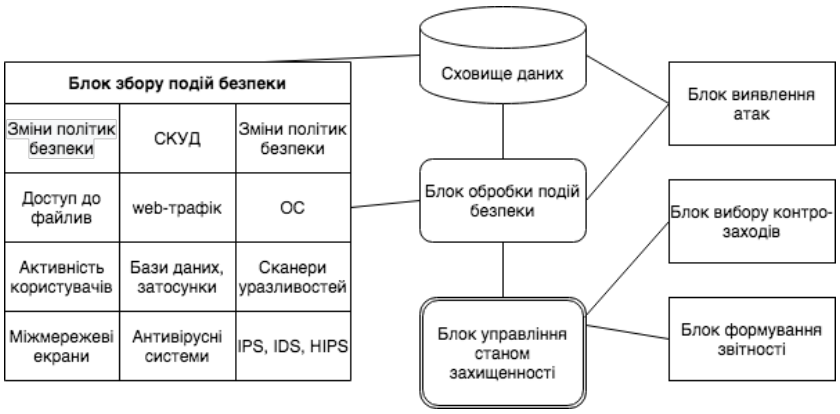

Рисунок 2.4 – Структурна схема існуючої системи управління подіями інформаційної безпеки.

Для підвищення ефективності існуючої системи управління запропоновано використати поділ вхідних даних двома методами, а саме: внутрішніх загроз та зовнішніх загроз, де для методу управління станом захищеності від внутрішніх загроз обрано метод опорних векторів, а для побудови методу управління станом захищеності від зовнішніх атак – метод динамічного програмування.

Структурно–логічна схема рекомендовано удосконаленої системи управління подіями інформаційної безпеки в ІТС представлено на рис. 2.5.

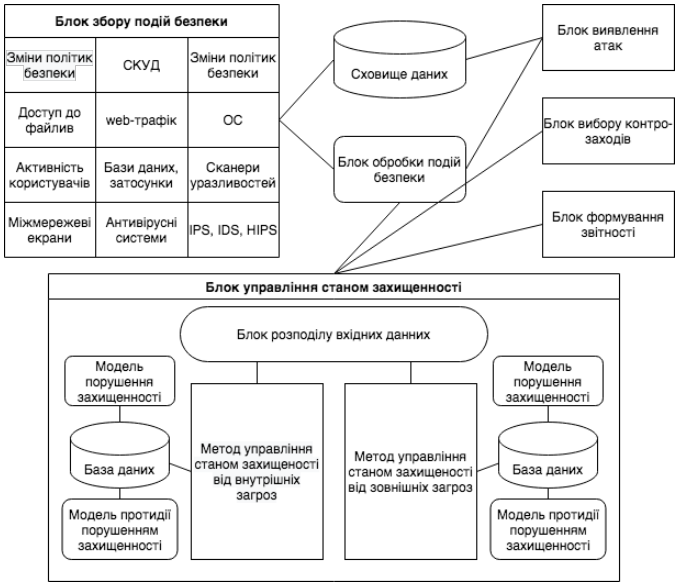

Рисунок 2.5 – Рекомендована структурна схема перспективної системи управління подіями

Основні етапи управління станом захищеності ІТС складаються з:

1. Отримання вхідних даних: множина параметрів вхідного трафіку та параметрів сенсорних індикаторів кібербезпеки;

2. Розподіл вхідних даних – розподіл параметрів трафіка відповідно до функціональних особливостей методів управління станом захищеності ІТС (від внутрішніх атак – 15, від зовнішніх атак – 18);

3. Виявлення атак – ідентифікація (*DoS, U2R, R2L, Probe, Side-channel*) категорій атак та нормальної поведінки, які впливають на стан захищеності ІТС.

4. Перевірка можливості протидіяти виявленим порушенням:

a) від внутрішніх атак $XV(t) = \{X_H(t)\} \cup \{X_S(t)\}$, $V = 1,..,25$;

b) від зовнішніх атак $XM(t) = \{x_m(t)\}$, $m = 1,..,18$.

5. Перевірка коректності ідентифікації;

6. Встановлення стану захищеності.

7. Прийняття управлінського рішення – на основі параметрів кібератак.

В свою чергу, виходячи із проведеного аналізу для побудови методу управління станом захищеності від внутрішніх атак доцільно обрати метод опорних векторів, а для побудови методу управління станом захищеності від зовнішніх атак – метод динамічного програмування. Сутність даних кроків полягає у ідентифікації станів захищеності з урахуванням множини різнорідних параметрів трафіка, що передається в ІТС.

Висновки до другого розділу

У цьому розділі проведено моделювання порушення захищеності ІР в ІТС та протидії порушенням захищеності ІР, що дає можливість встановити доцільність розробки методів управління станом захищеності від внутрішніх та зовнішніх загроз для визначення ефективності функціонування СЗІ в режимі реального часу. Розробка даних моделей дозволить побудувати ефективну підсистему управління станом захищеності ІТС з урахуванням

характеристичних особливостей ІТС для своєчасного застосування засобів захист від впливу кібератак.

РОЗДІЛ 3
РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ СТАНОМ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ В УМОВАХ ВПЛИВУ КІБЕРАТАК

3.1 Метод управління станом захищеності від зовнішніх кібератак на інформаційно-телекомунікаційну систему на основі розподільчої ідентифікації та динамічного програмування

Наразі існуючі системи управління подіями інформаційної безпеки передбачають прийняття рішень при виявленні кіберзагроз на основі обробки множини різних параметрів даних. Загрози в свою чергу реалізуються різнонаправленими кібератаками. Інформація, під час проходження в системі, аналізується за відповідними параметрами на предмет виявлення порушень захищеності. У результаті чого на виході блоку управління станом захищеності з'являється ознака щодо наявності зміни стану захищеності ІТС та можливості протидії загрозам інформаційним ресурсам.

Для навчального аналізу множин підсистеми управління станом захищеності ІТС використано конкретні різновиди атак, представлені в базах даних NSL-KDD та KYOTO [25, 62]. В цих базах даних міститься більше 8 000 000 записів щодо аномальних з'єднань та близько 2 000 000 відомостей про нормальний тип з`єднання. Кожен запис являє собою образ мережевого з`єднання, включає 41 параметр мережевого трафіка, серед яких міститься три типи ознак: символьні, логічні та числові. У загальному вигляді вони містять інформацію про тривалість з'єднання, тип протоколу, кількість спроб реєстрації тощо.

На основі вхідних параметрів трафіка відбувається перевірка на наявність порушень захищеності та маркування їх як „порушення" або „не порушення". Вказаний запис складається з 42 полів. Перші 41 поле описують

ознаки мережевого трафіка, а останнє 42-е поле вказує на тип трафіка, який описується. Вказане поле може приймати значення „normal”, якщо дане мережеве з`єднання відноситься до „нормального” стану трафіка, або найменування типу атак (наприклад, „ipsweep”).

Вирішуючи задачу класифікації кібератаки (наприклад по її сигнатурі) підсистема управління станом захищеності ставить у відповідність наведеним вище параметрам мережевого трафіка 29 типів найбільш часто застосованих атак. Відкласифіковані параметри вхідних даних (атак) співвідносяться до множини управлінських рішень щодо варіантів реагування на кожен окремий тип атаки. В наслідок чого відбувається управління станом захищеності ІТС.

З огляду на вищезазначений розроблений метод управління станом захищеності від зовнішніх кібератак враховано наступні особливості ІТС:

– різна розмірність мереж;

– територіально рознесені складові ІТС;

– вихід елементів ІТС за межі контрольованої зони;

– для доступу до оброблюваних ресурсів застосовуються не тільки ПК;

– мають високі вимоги до доступності інформаційних ресурсів;

– конфігурація ІТС змінюється (змінюється склад користувачів та їхні привілеї, оновлюються версії програм, з’являються нові сервіси, апаратура і т.п.);

– взаємозв’язок та взаємозалежність елементів ІТС.

Позначення вхідних даних: Розглядається ситуація знаходження системи у стані рівноймовірнісного протікання порушень захищеності ІТС. В один і той же час відбуваються як порушення захищеності від зовнішніх кібератак на ІТС так і пошук варіантів протидій на виявлені зміни стану захищеності. Для моделювання такої ситуації будується навчальна вибірка, яка має в собі 20 % нормальних інформаційних повідомлень та 80 % аномальних інформаційних повідомлень, які містять ризні типи атак. Також складається база з варіантами протидій на множину виявлених порушень. Так як кожна фаза атаки характеризується множиною технік проведення і

реалізується внутрішнім або зовнішнім зловмисником, тому для управління станом захищеності від зовнішніх кібератак відбувається ідентифікація типів порушень на основі параметрів даних, що характерні саме зовнішнім атакам.

Під час виявлення атак буде застосовуватись механізм логічного виводу для опису бази вхідних параметрів. На підставі співставлення вхідних параметрів, у системі формуватиметься рішення, щодо їх класифікації. В наслідок чого відбувається співвідношення стану захищеності ІТС до можливих видів порушень та наявних засобів захисту та приймається управлінське рішення щодо підтримки належного стану захищеності ІТС.

Вхідним значенням є: $X = XH \cup XM \cup XL$ – параметри вхідного трафіку;

$XM = \{x_i(t), i = \overline{1,18}\}$ – множина параметрів трафіку, що характерні зовнішнім кібератакам;

$XH = \{x_h(t), h = \overline{1,15}\}$ – множина параметрів трафіку, що характерні внутрішнім кібератакам;

XL – множина параметрів трафіку, що не задіяні при реалізації методу.

Обмеження та допущення: Ідентифікуються типи атак: DoS, U2R, R2L, Probe, Side. Аномальна поведінка ідентифікується, як нововиявлений стан захищеності. Процес управління станом захищеності є квазістаціонарним на визначеному інтервалі часу $(t_0 ... T)$.

Необхідно: збільшити достовірність прийняття управлінського рішення щодо оцінки стану захищеності IP D від зовнішніх кібератак за умов, що час прийняття управлінського рішення буде не більше ніж у подібних методів:

$$\begin{cases} D \to \max; \\ D > D_{isn} \\ T \le T_{isn} \end{cases}.$$

Сутність методу полягає у: використанні розподільчої ідентифікації параметрів зовнішніх кібератак з проведенням вибору щодо застосування

заходів із захисту системи при повному описі ІТС та врахуванням стратегій впливу на неї на основі динамічного програмування.

Управління станом захищеності ІТС від зовнішніх кіберзагроз може відбуватись при проведенні ідентифікації параметрів порушень, які реалізуються множиною різнонаправлених та різних за своїм змістом атак.

Тому проведемо ідентифікацію вхідних даних (параметрів даних) трафіка.

І. Під ідентифікацією розумітимемо знаходження оптимальної в деякому сенсі моделі, побудованої за результатами спостережень над вхідними та вихідними змінними об’єкта, а саме набором параметрів трафіку. Завданням ідентифікації є зворотне завдання системного синтезу.

З урахуванням завдань ідентифікації виділяють два типи [63]:

– структурна ідентифікація, яка дозволяє визначити форму моделі з деякого заданого класу функцій;

– параметрична ідентифікація, яка визначає параметри моделі.

Однак виходячи із поставленого завдання, щодо ідентифікації вхідних даних на основі параметрів кібератак (сигнатур), буде застосована саме параметрична ідентифікація.

При параметричній ідентифікації дані про об’єкт обробляються для отримання про нього апостеріорної інформації. При цьому оцінюються параметри обраної моделі. У найпростіших випадках така оцінка може виконуватися по графіку перехідної характеристики.

При побудові моделі оцінки захищеності за експериментально отриманими даними поширеною є ситуація, для якої практично вся інформація, що використовується пид час обробки для розв’язання поставленої задачі, обмежується вибіркою вихідних даних. Тому для розв’язання задачі параметричної ідентифікації використовують методи, орієнтовані виключно на інформацію про невідповідність між виходами об`єкта та моделі.

В загальному випадку для довільної моделі відомої структури рівень невідповідності між виходами об'єкта та моделі залежить від вибору параметрів моделі. Тому, якщо ввести показник якості параметричної ідентифікації, який поєднує в собі всю інформацію про рівні нев'язок і містить відомості про залежність рівня невідповідності між виходами об'єкта та моделі від значень параметрів моделі, то мінімізація цього показника дозволить визначити оптимальні параметри моделі.

Визначення прийнятного значення ризику для інформаційних ресурсів. Під прийнятним значенням ризику розуміють обґрунтовану величину втрат з якою керівництво установи може погодитися і діяти в умовах її існування. Інформаційними є ризики, що пов'язані з можливістю виникнення втрат при використанні установою ІР. Для визначення прийнятності ризику при побудові систем управління безпекою інформації визначають середнє значення втрат [64]:

$$A_{ср} = \frac{\sum_{i=1}^{m} A_i}{m} = \frac{\sum_{i=1}^{m} (P_{план.} - P_i)}{m} \qquad (3.1)$$

де i – кількість проведених вимірювань за період часу.

Для визначення прийнятних значень частості виникнення втрат використовують рівняння: $a_1 x_1 + a_2 x_2 + ... + a_j x_j + a_n x_n = r_n, j \in (1, n)$. Значення величини втрат a_j визначається шляхом оцінки інформаційного ресурсу власниками, частота x_j розраховується відповідними методами. В реальних умовах часто дозволяється визначення оцінок прийнятного ризику $r_{пр}$ і втрат a_j з точністю до цілих чисел.

Враховуючи стратегії проведення кібератак на ІТС, ймовірність здійснення j_z кібератак на множину об'єктів ІТС l обчислюється:

$$P(j_z, l) = \prod_{i=1}^{l} P_i^{j_z} \qquad (3.2)$$

Задачу параметричної ідентифікації можна сформулювати так: підібрати на множині $\{X\}$ можливих значень параметрів такі значення $\widetilde{X}$, щоб різниці показників досягли своїх мінімумів, тобто метою цього аналізу є пошук:

$$\widetilde{X}(t) = \arg\min_{y \in \hat{X}} \sum_{i=1}^{18} (y_i(t) - x_i(t))^2 \tag{3.3}$$

де $\hat{X}$ – параметри трафіку, що описано в БД;

$x_i(t)$ – параметри, що описують потік вхідних даних трафіку та отримано з блоку розподілу даних.

ІІ. Наступним кроком буде проведення управління станом захищеності ІТС від зовнішніх кібератак на інформаційні ресурси та інформацію, вимога щодо захисту якої встановлена законодавством, на основі ідентифікованих даних та пошуку відповідності цих даних множині варіантів протидії порушенням. Для цього отримуються з бази даних сукупність даних про стан захищеності ІТС $XM(t) = \{x_1, ..., x_{18}\}$, сукупність даних про можливі порушення безпеки $\Lambda = \{\lambda_1, ..., \lambda_n\}$, де n – кількість варіантів множин, що містяться в БД та співставляються набори сигнатур і можливі порушення.

У моделях які характеризуються динамічною структурою побудови, до яких і належить ІТС, стан захищеності являє собою часовий зріз властивості захищеності інформації цей процес описується значенням відповідного показника в певний фіксований момент часу.

Процес отримання оцінки стану захищеності ІТС і процес застосування засобів забезпечення захищеності реалізуються по крокам. На кожному кроці отримується деяка сукупність даних про стан захищеності ІТС, яка залежить від можливих порушень безпеки, що характеризують стан захищеності ІТС і впливають на вибір використовуваних ЗЗ. Використовуючи отримані і вже наявні відомості про стан захищеності ІТС, приймається управлінське рішення про застосування ЗЗ, яке може залежати і від раніше прийнятих рішень. Таким чином, повна сукупність даних про стан захищеності системи

X, рішень про застосування ЗЗ U та реалізовані варіанти впливу на порушення безпеки Λ можна описати наступним чином:

$$X(t) = \{x_1,...,x_{18}\}\ U = \{U_1,...,U_k\}\ \Lambda = \{\Lambda_1,...,\Lambda_k\}\ k = 1,2,...,N \qquad (3.4)$$

Слід врахувати, що задіяні на будь-якому кроці ЗЗ U_k можуть вплинути на можливі порушення безпеки $\Lambda_{k+1}, \Lambda_{k+2},...$ на наступних кроках, а також на обсяг і якість одержуваних на цих кроках даних про стан захищеності ІТС $X(t)$. Така наявність зворотного зв'язку характерна для ІТС загального вигляду, в яких всі або деякі компоненти рішення U_k є діями, що управляють можливими порушеннями безпеки Λ_k. Тобто вжиті ЗЗ впливають на значення Λ_k і на подальших кроках, а такі багатокрокові процеси прийняття рішення є керованими [3].

Математичним відображенням цього зворотного зв'язку є залежність розподілів ймовірностей значень Λ_k і $X(t)$ від послідовності попередньо застосованих ЗЗ $U_{k-1},...,U_k$. Повний статистичний опис багатокрокового процесу для будь-якої сукупності прийнятих ЗЗ досягається заданням послідовності умовних розподілів ймовірності для спостережуваних даних і параметрів для всіх значень $k = 1,2,...,N$. При прийнятті управлінських рішень про застосування необхідних ЗЗ U_k використовуємо тільки ті дані спостереження, які отримані до k-ого кроку включно. Тому правило прийняття рішення про застосування ЗЗ U_k можна задати ймовірнісною мірою p_k, яка залежить від X_k, а також від сукупності попередніх рішень $\{u_1,...,u_n\} = U_{k-1}$.

Знаходження оптимальної послідовності прийняття ЗЗ для багатокрокової процедури проводиться методами динамічного програмування в загальній стохастичній формі, які при певних обмеженнях на розподіл ймовірностей для X_k і Λ_k та функцію зміни стану захищеності (функцію втрат) $g(U_k, \Lambda_k, X_k)$, $k = 1,...,N$, дозволяють побудувати ефективну обчислювальну процедуру знаходження оптимальних рішень. При цьому

оптимальна послідовність прийняття рішення щодо застосування ЗЗ визначається рекурентним співвідношенням, яке містить послідовність мінімізацій і усереднень для величин апостеріорних ризиків.

Середня величина ризику виникнення порушень визначається виразом:

$$R(t) = M\{g(U, \Lambda_k, X_k)\}\ U = \{U_1, U_2, ..., U_k\} \quad (3.5)$$

де M – математичне очікування.

Тоді мінімальний (байесів) середній ризик для оптимального правила прийняття ршенні на k-ому кроці визначається, як:

$$) = \min_{U_1,...,U_k} M\{g(U, \Lambda_k, X_k)\} = \min_{U_1,...,U_{k-1}} (\min_{U_k} M\{M\{g(U, \Lambda_k, X_k) \mid X_k, U\}\}) \quad (3.6)$$

де умовне математичне очікування представляє функцію апостеріорного ризику для сукупності рішень U_k та даних спостережень X_k.

Структуру алгоритму реалізації методу управління станом захищеності від зовнішніх кібератак на ІТС на основі алгоритму розподільчої ідентифікації та динамічного програмування представлено на рис. 3.2.

Спільно з виразами (3.4) і (3.4) для кінцевого значення апостеріорного ризику співвідношення (3.6) визначає оптимальну послідовність застосування протидії порушенням (прийняття управлінського рішення).

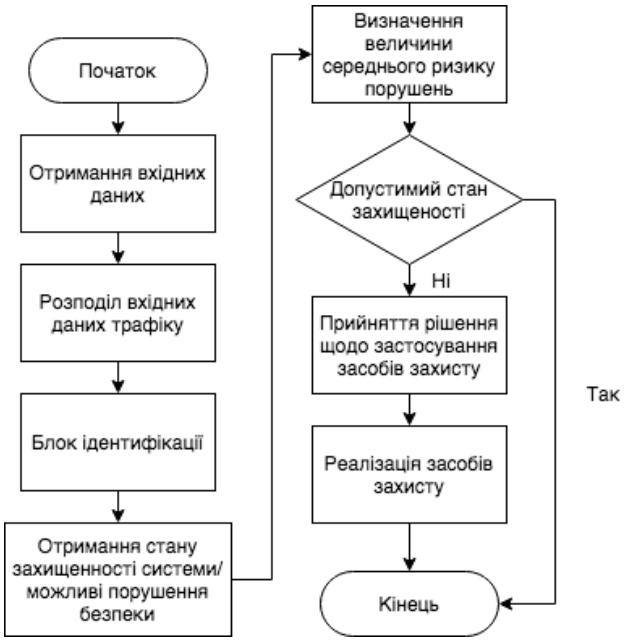

Рисунок 3.2 – Структура алгоритму реалізації методу управління станом захищеності від зовнішніх кібератак

Структурна схема управління станом захищеності ІТС від кіберзагроз, характерних зовнішньому зловмиснику представлено на рис. 3.3.

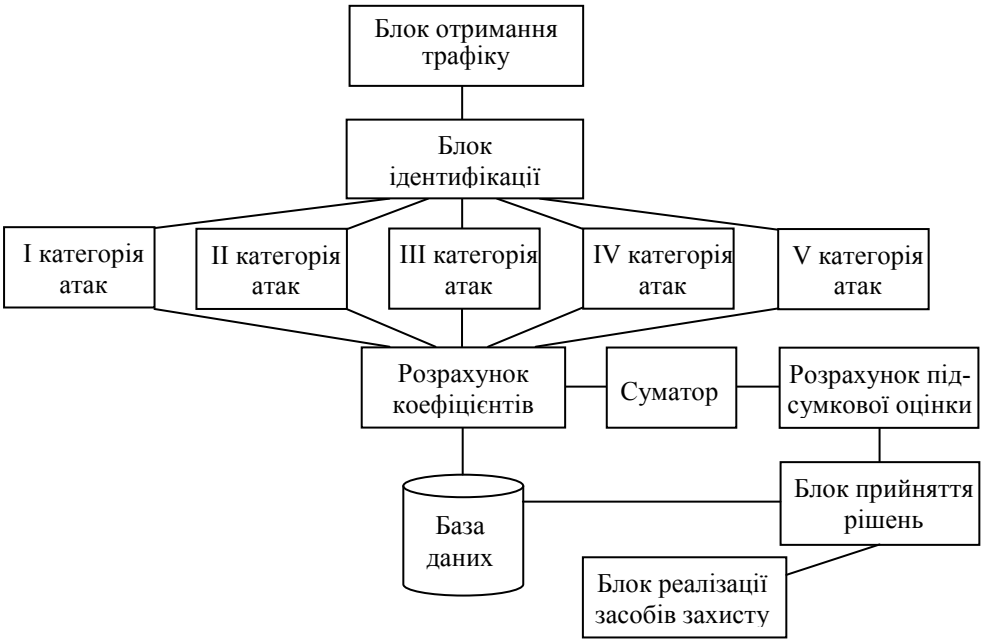

Рисунок 3.3 – Схема реалізації управління станом захищеності від зовнішніх кіберзагроз

Дана реалізація методу управління станом захищеності від зовнішніх кібератак на ІТС, на відміну від подібних методів, приймає управлінське рішення щодо стану захищеності ІР при множині вхідних параметрів зовнішніх кібератак на основі паралельно-розподільчої ідентифікації та динамічного програмування.

3.2 Рекомендації щодо удосконалення методу управління станом захищеності інформаційно-телекомунікаційної системи на основі даних про внутрішні кібератаки

Позначення вихідних даних: Розглядається ситуація рівноймовірнісного знаходження системи у стані протікання порушень захищеності ІТС. В один і той же час відбуваються як порушення захищеності від внутрішніх кібератак на ІР та інформацію, вимога щодо захисту якої встановлена законодавством, в

ІТС так і пошук варіантів протидій на виявлені зміни стану захищеності. Для моделювання такої ситуації будується навчальна вибірка, яка має в собі 20 % нормальних повідомлень та 80 % аномальних повідомлень, які містять типи атак. Також будується база з варіантами протидій на множину виявлених порушень.

Вхідним даними є: $X = XH \cup XM \cup XL$ – параметри вхідного трафіку;

$XM = \{x_m(t), m = \overline{1,18}\}$ – множина параметрів трафіку, що характерні зовнішнім кібератакам;

$XH = \{x_h(t), h = \overline{1,15}\}$ – множина параметрів трафіку, що характерні внутрішнім кібератакам;

XL – множина параметрів трафіку, що не задіяні при реалізації методу;

$S(t), s = \overline{1,10}$ – параметри сенсорних індикаторів кібербезпеки;

$XV = \{XH \cup S(t)\}$ – вхідні дані, що характерні внутрішнім кібератакам.

Обмеження та допущення: Ідентифікуються типи атак: DoS, U2R, R2L, Probe, Side. Для ідентифікації поведінки розглянуто сигнатури атак, що є загрозами для ІТС. Аномальна поведінка ідентифікується, як нововиявлений стан захищеності. Процес управління станом захищеності є квазістаціонарним на інтервалі часу $(t_0 ... T)$.

Необхідно: збільшити достовірність прийняття управлінського рішення щодо оцінки стану захищеності ІР та інформації, вимога щодо захисту якої встановлена законодавством від зовнішніх кібератак за умов, що час прийняття управлінського рішення буде не більше ніж у подібних методів.

Сутність методу полягає у розподільчому управлінні станом захищеності ІТС на основі множини вхідних параметрів характерних внутрішнім кібератакам і множини параметрів сенсорів кібербезпеки з використанням опису ІТС та методу опорних векторів.

Задача своєчасного виявлення змін стану захищеності ІР та ІТС вирішується через управління станом захищеності ІТС на основі множини

параметрів внутрішніх атак в умовах обмежених вибірок даних поточного спостереження.

Управління станом захищеності ІТС від внутрішніх кібератак відбувається у разі проведення ідентифікації параметрів порушень, які реалізуються множиною різнонаправлених та різних за своїм змістом атак. Структуру алгоритму реалізації методу управління станом захищеності ІТС на основі даних про внутрішні кібератаки представлено на рис. 3.4.

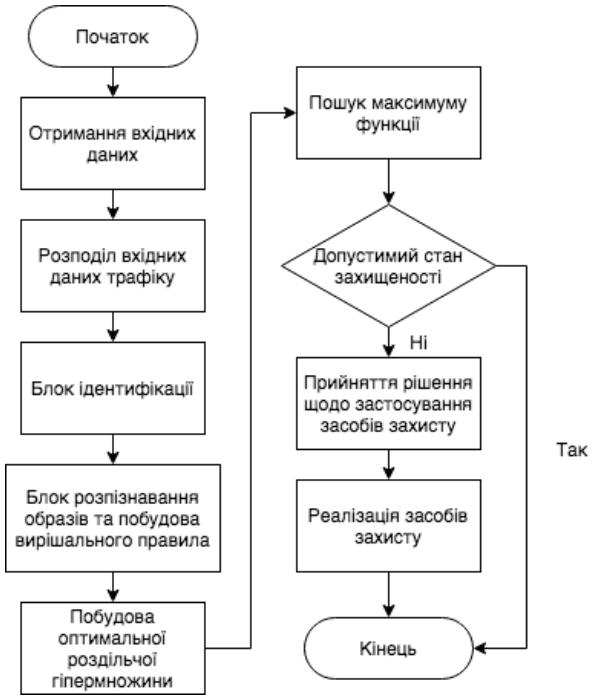

Рисунок 3.4 – Структура алгоритму реалізації методу управління станом захищеності ІТС на основі даних про внутрішні кібератаки

Процес проведення ідентифікації вхідних даних (параметрів даних) трафіка.

І. Під ідентифікацією припускається знаходження умовно оптимальної моделі, побудованої за результатами спостережень над вхідними та вихідними змінними об’єкту, а саме набором параметрів трафіку. Ідентифікація є зворотнім завданням системного синтезу.

Для ідентифікації вхідних даних на основі параметрів, що характерні внутрішнім кібератакам, буде застосована параметрична ідентифікація.

При параметричній ідентифікації дані про об'єкт обробляються для отримання про нього інформації, що засновано на досвіді попередніх подій. При цьому оцінюються параметри обраної моделі. У найпростіших випадках така оцінка може виконуватися по графіку перехідної характеристики.

II. Наступним етапом є отримання з бази даних сукупності даних про стан захищеності ІТС $X(t) = \{x_1, ..., x_{25}\}$, множини можливих порушень безпеки $\Lambda = \{\lambda_1, ..., \lambda_n\}$ та множини можливих засобів протидії порушенням (управлінських рішень) $U = \{u_1, ..., u_n\}$, де n – кількість варіантів в множинах, що містяться в базі даних; оцінювання захищеності на основі залежності середнього значення множини оптимальних значень засобів протидії порушенням $\overline{U}$ від величини Λ та встановлення стану захищеності.

Навчання розпізнаванню образів здійснюється наступним чином. Є деяка множина спостережень (стани захищеності), які відносяться до p різних класів. Компонентами вектора є окремі загрози безпеці елементам ІТС. Необхідно знайти правило класифікування змін стану захищенності, використавши яке, з мінімальним числом помилок можна групувати зміни стану захищеності, використовуючи дані під час спостереження та класифікацію такої інформації.

Класами спостережень можуть бути ситуації зміни стану захищеності елементів ІТС. Так, наприклад, для двох класів: стан захищеності елементів ІТС погіршується; стан захищеності елементів ІТС покращується. Приклад для трьох класів: стан захищеності елементів ІТС погіршується; стан захищеності елементів ІТС залишається без змін; стан захищеності елементів ІТС покращується. Очевидно, що кількість класів може бути довільною та визначатися умовою однозначної класифікації поточної ситуації.

Вважатимемо, що спостереження задається вектором x, а його класифікація – числом ω (ω може приймати p значень: 0, 1, …, $p-1$). На практиці таким вектором буде вектор з компонентами, що виступають чисельними оцінками захищеності ІТС.

Виходячи з цього, слід, маючи послідовність із l спостережень та класифікацій $x_1, \omega_1; ...; x_l, \omega_l$, побудувати таке вирішуюче правило $\omega = F(x)$, яке з можливо найменшим числом помилок класифікувало б нові спостереження.

Для формалізації слова «помилка» вважатимемо, що існує (хоча воно є невідомим) деяке правило Φ, що визначає для кожного вектора x класифікацію $\omega = \Phi(x)$, яку називають «істинною». Помилкою класифікації вектора x за допомогою правила $F(x)$ назвемо таку класифікацію, при якій $F(x)$ та $\Phi(x)$ не співпадають.

Щоб мати можливість використовувати математичний аналіз, будемо вважати, що правило $F(x)$ є однією із функцій деякої заданої множини функцій $\{F(x)\}$, а правило класифікації $\Phi(x)$ визначається умовною імовірністю $P(\omega|x)$.

Прийнято вважати, що на просторі векторів x існує невідома нам імовірнісна міра (позначатимемо її щільністю $P(x)$). У відповідності до $P(x)$ випадково і незалежно з'являються ситуації x, які класифікуються за допомогою правила $P(\omega|x)$. Таким чином, визначається навчальна послідовність $x_1, \omega_1; ...; x_l, \omega_l$.

Отже, для будь-якого вирішального правила $F(x)$ необхідно визначити якість як імовірність різної класифікації за допомогою правила $F(x)$ та правила $P(\omega|x)$. Чим менше дана імовірність, тим вище якість. Формально якість вирішального правила можна записати у вигляді:

$$I(F) = \sum_{i=0}^{p-1} \int \Theta(F(x) - \omega_i) P(\omega_i|x) P(x) dx \qquad (3.7)$$

де $\Theta(z) = \begin{cases} 0, & z = 0 \\ 1, & z \neq 0 \end{cases}$.

Безпосередньо обчислити імовірність безпомилкової класифікації неможливо ні для якого вирішуючого правила F(x), так як щільності P(x) та

$P(\omega|x)$ не відомі.

Використовуючи вибірку $x_1, \omega_1; ...; x_l, \omega_l$, необхідно знайти у класі $\{F(x)\}$ таке правило, яке мінімізує функціонал (3.12).

Для більшої зручності, надалі, будемо вважати, що:

1) змінна ω приймає тільки два значення: 0 та 1 (тобто ситуація *x* належить одному з двох класів); це обмеження не є принциповим, так як послідовним розділенням на два класи можна отримати розділення на будь-яке скінчене число класів;

2) клас індикаторних функцій $\{F(x)\}$, тобто функцій, що приймають два значення: 0 та 1, є параметричним $\{F(x,\alpha)\}$ (тут α – параметр, що належить множині Λ, конкретне значення якого $\alpha = \alpha^*$ визначає конкретну функцію $F(x,\alpha^*)$ класу $F(x,\alpha)$; знайти потрібну функцію у класі – значить встановити потрібне значення параметра в класі; вивчення лише параметричного класу функцій ніяк не знижує абсолютності у заданному класі функцій, так як множина Λ довільна: вона може бути множиною скалярних величин, множиною векторів чи множиною абстрактних елементів);

3) функціонал з минулого кроку (2) слід записати у вигляді:

$$I(\alpha) = \int (\omega - F(x,\alpha))^2 P(x,\omega) dx d\omega \qquad (3.8)$$

де функцію $P(x,\omega) = P(\omega|x)P(x)$ будемо в подальшому називати сумісною щільністю пар x, ω, заданою на просторі X, Ω.

Таким чином, задача з навчання розпізнаванню образів полягає у тому, що у класі індикаторних функцій $F(x,\alpha)$ необхідно відшукати таку функцію, яка б мінімізувала функціонал (3.13) в умовах, коли сумісна щільність $P(x,\omega)$ невідома, але задана імовірна і незалежна вибірка пар, отриманих відповідно до цієї щільності.

За основу алгоритмів навчання розпізнавання образів взято спеціальний метод відшукування вирішального правила, який базується на побудові

роздільної гіперплощини.

Отже, отримуємо, що при побудові оптимального направляючого вектору необхідно знайти максимум недодатно визначеної квадратичної форми $W(\alpha)$ в додатному квадранті $\alpha_{ij} \geq 0$ або встановити, що максимум функції $W(\alpha)$ переважає задану величину W_0. Останнє значення передбачає, що побудова розділяючої гіперплощини неможлива.

Метод спряжених градієнтів є одним з найбільш ефективних алгоритмів максимізації недодатно визначеної квадратичної форми. За його допомогою можливо досягнути максимуму за n кроків ($n-$ розмірність форми). Розглянемо метод спряжених градієнтів для максимізації від'ємно визначеної квадратичної форми $F(y) = b^T y - y^T Ay$, де A – додатно визначена матриця, b, y – вектори.

За методом спряжених градієнтів, пошук максимуму функції починається з довільної точки $y_0 = y(0)$. Перший крок робиться в напрямку градієнта функції $F(y)$ в точці $y(0)$. Позначимо градієнт функції в точці $y(0)$ через $g(1)$, а напрямок руху з точки $y(0)$ через $z(1)$.

Таким чином $z(1) = g(1)$.

Крок робиться за напрямком $z(1)$ до досягнення максимуму по цьому напрямку. Максимум за напрямком $z(1)$ задається виразом

$$y(1) = y(0) + \frac{z^T(1)g(1)}{z^T(1)Az(1)} z(1) \qquad (3.9)$$

Починаючи з другого кроку, напрямок руху визначається вектором:

$$z(t+1) = g(t+1) + \frac{\|g(t+1)\|^2}{\|g(t)\|^2} z(t) \qquad (3.10)$$

де $g(t+1)$ та $g(t)$ – градієнт функції $F(y)$ в точках $y(t+1)$ та $y(t)$ відповідно; $z(t)$ – напрямок руху в точці $y(t-1)$.

Рух за напрямком $z(t)$ ведеться до досягнення умовного максимуму. Цей максимум досягається в точці:

$$y(t) = y(t-1) + h(t)z(t) \tag{3.11}$$

де крок руху визначає величина:

$$h(t) = \frac{z^T(t)g(t)}{z^T(t)Az(t)} \tag{3.12}$$

Таким чином вирази (3.9) – (3.12) задають, алгоритм пошуку максимуму квадратичної форми *F(y)*.

Модифікація методу спрямована на обмеження області пошуку за допомогою додатного квадранту.

За допомогою розглянутого базового алгоритму будується розділяюча гіперплощина, яка мінімізує число неправильно класифікованих векторів. Принципово ця задача може бути вирішена точно, але потребує значно більшого перебору варіантів, що збільшує час на її вирішення. Тому для побудови гіперплощини, "близької до оптимальної", використовується стандартний прийом "послідовної мінімізації".

Загальна структурна схема управління станом захищеності ІТС від внутрішніх кіберзагроз зазначена на рис. 3.5.

Рисунок 3.5 – Схема управління станом захищеності ІТС від внутрішніх кіберзагроз

Якщо безпомилкове розділення гіперплощиною неможливе, з навчальної послідовності виключається один елемент, “що найбільше перешкоджає розділенню”. Якщо розділення все ще неможливе, із множини, що залишилася, виключається ще один елемент. В решті решт, виключивши m векторів, що перешкоджають розділенню, вдається розділити множину векторів, що залишилися.

Таким чином, особливість алгоритму полягає у визначенні вектора навчальної послідовності x_* чи $\bar{x}_*$, що “найбільше перешкоджає розділенню”.

На відміну від відомих методів управління станом захищеності ІТС, які не передбачають розподілу систем оцінювання станів з врахуванням функціональних особливостей складових ІТС та, як наслідок, застосовують послідовний алгоритм процесу оцінки, що призводить до великої математичної складності обчислень, великого обсягу вхідний даних, удосконалений метод використовує множину параметрів трафіку, що характеризують внутрішні атаки на ІТС, та побудовано з використанням опису ІТС та методу опорних векторів.

Висновки до розділу 3

У даному розділі цієї магістерської роботи вперше запропоновано метод управління станом захищеності від зовнішніх кібератак на ІТС на основі розподільчої ідентифікації та динамічного програмування. Сутність використання такого методу полягає у застосуванні розподільчої ідентифікації параметрів зовнішніх кібератак з проведенням вибору щодо застосування заходів із захисту системи при повному описі ІТС та врахуванням стратегій впливу на неї беручи за основу динамічне програмування. Запропонований метод, на відміну від подібних методів, приймає управлінське рішення про стан захищеності інформаційних ресурсів при множині вхідних параметрів зовнішніх кібератак на основі паралельно-розподільчої ідентифікації та динамічного програмування. Використання такого підходу дозволяє

збільшити достовірність прийняття управлінського рішення щодо оцінювання стану захищеності ІР в ІТС, за умов часу прийняття управлінського рішення щодо оцінювання стану захищеності, що не перевищує час прийняття рішень при використанні подібних методів.

В другому підрозділі третьої частини дипломної роботи пропонуються рекомендації з вдосконалення методу управління станом захищеності ІТС на основі даних про внутрішні кібератаки. Пропонується використовувати метод опорних векторів на основі параметрів, що характерні внутрішнім кібератакам на ІТС. Даний метод дозволяє розподільно ідентифікувати вхідні параметри внутрішніх кібератак та підвищити достовірність прийняття управлінського рішення з оцінювання стану захищеності інформаційних ресурсів за умов коли час прийняття управлінського рішення не перевищує час прийняття рішень при використанні подібних методів. Використаний математичний підхід дозволяє зменшити обсяг вхідних даних для управління станом захищеності ІТС, збільшити достовірність прийняття управлінського рішення щодо оцінки стану захищеності ІР.

ВИСНОВКИ

В результаті виконання магістерської роботи було вирішено актуальну задачу, яка полягає в розробці рекомендацій щодо управління станом захищеності інформаційних ресурсів від кібератак на інформаційно-телекомунікаційні системи з використанням ідентифікації, методів динамічного програмування та опорних векторів.

За підсумками вирішення поставленної задачі в рамках магістерської роботи зроблено наступні висновки:

1. В результаті аналізу атак на інформаційні ресурси, функціонування ІТС та їх вразливостей, аналізу методів управління станом їх захищеності та методів прийняття рішень з забезпечення захищеності ІТС було встановлено невідповідність між можливостями існуючих методів управління станом захищеності ІТС та вимогами до методів управління станом захищеності державних інформаційних ресурсів в ІТС. До основних особливостей ІТС відносяться різна розмірність мереж, територіально рознесені складові ІТС, вихід елементів ІТС за межі контрольованої зони, для доступу до оброблюваних ресурсів застосовуються не тільки ПК, мають високі вимоги до доступності інформаційних ресурсів, конфігурація ІТС змінюється (змінюється склад користувачів та їхні привілеї, оновлюються версії програм, з’являються нові сервіси, нова апаратура і т.п.). Також було встановлено, що запропоновані на сьогоднішній день методи управління станом захищеності ІТС не враховують особливостей проведення кібератак внутрішніми і зовнішніми зловмисниками, а також мають низьку достовірність прийняття управлінського рішення в рамках оцінювання стану захищеності ІТС та застосування засобів захисту. Основними вимогами, які висуваються до методів управління станом захищеності інформаційних ресурсів в ІТС є:

– робота в режимі реального часу;
– врахування впливу загроз, що характерні ІТС;

– забезпечення адаптивного функціонування елементів систем захисту інформації з можливістю її самоорганізації;

– децентралізація управління та наявність ієрархічно-розподільної структури;

– збільшення достовірності та повноти прийняття управлінського рішення;

– зменшення математичної складності та ресурсної обтяжливості методів.

2. Взявши до уваги можливості існуючих методів управління станом захищеності ІТС та особливостей функціонування ІТС, що були проаналізовані у першому розділі цієї дипломної роботи, у ході досліджень було визначено наступні напрямки усунення вищезазначеної невідповідності, а саме:

– розподіл системи управління станом захищеності ІТС на основі зовнішніх та внутрішніх кібератак

– рекомендацію щодо розроблення нових та удосконалення існуючих методів управління станом захищеності при проведенні зовнішніх та внутрішніх кібератак на ІТС на основі динамічного програмування, розподільчої ідентифікації та опорних векторів.

3. Вперше було запропоновано метод управління станом захищеності від зовнішніх кібератак на ІТС на основі розподільчої ідентифікації та динамічного програмування. Суть методу полягає у використанні розподільчої ідентифікації параметрів зовнішніх кібератак з проведенням вибору щодо застосування заходів із захисту системи при повному описі інформаційно-телекомунікаційної системи та врахуванням стратегій впливу на неї на основі динамічного програмування. На відміну від подібних, розроблений метод приймає управлінське рішення щодо стану захищеності інформаційних ресурсів при множині вхідних параметрів зовнішніх кібератак на основі паралельно-розподільчої ідентифікації та динамічного програмування. Запропонований метод дає змогу збільшити достовірність

прийняття управлінського рішення при оцінюванці стану захищеності інформаційних ресурсів в ІТС за рахунок використання розподільчої ідентифікації, за умов часу на прийняття управлінського рішення щодо оцінювання стану захищеності не більше ніж у подібних методів.

4. Запропоновано кроки щодо удосконалення методу управління станом захищеності ІТС при використанні даних про внутрішні кібератаки. Суть запропонованого методу полягає у розподілі управління станом захищеності ІТС на основі множини вхідних параметрів характерних для внутрішніх кібератак і множини параметрів сенсорів кібербезпеки з використанням опису ІТС та методу опорних векторів. На відміну від існуючих методів, рекомендації щодо удосконалення методу управління станом захищеності ІТС пропонують використання модифікації методу опорних векторів на основі параметрів, які характерні впливу внутрішніх кібератак на ІТС. Таке використання даного методу дає можливість використовувати розподільну ідентифікацію вхідних параметрів внутрішніх кібератак та збільшити достовірність прийняття управлінського рішення при оцінюванці стану захищеності інформаційних ресурсів за умов часу на прийняття управлінського рішення щодо оцінювання стану захищеності не більше ніж у подібних методів.

5. Мета досліджень щодо підвищення ефективності управління станом захищеності інформаційних ресурсів від зовнішніх та внутрішніх кібератак на ІТС досягнута, всі часткові завдання вирішено повністю. Результати досліджень є внеском у розвиток теоретичних і прикладних основ розробки систем забезпечення безпеки ІТС. В цілому представлені в дипломній роботі рекомендації дозволяють проводити управління станом захищеності інформаційними ресурсами в ІТС.

7. Отримані результати досліджень можуть бути використані під час розробки та проектування систем управління інформаційними ресурсами в умовах впливу кібератак. Для впровадження одержаних методів управління станом захищеності ІР в ІТС, доцільно провести розробку методів

прогнозування станів системи, що дозволить ефективно використати одержані наукові результати у мережах та системах спеціального призначення.

8. Практичне значення отриманих результатів.

Застосування запропонованих рекомендацій щодо методів управління станом захищеності ДІР в ІТС дозволяє збільшити достовірність прийняття управлінських рішень за умов часу на прийняття управлінського рішення щодо оцінювання стану захищеності не більше ніж у подібних методів.

Отримані результати можуть бути використані при розробці комплексної системи захисту ІР та проектуванні систем управління ІР в умовах впливу кібератак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 02.01.2020 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

3. Сторчак А.С. Метод оцінки захищеності інформації на основі багатокрокових процесів прийняття рішень. *Східно-Європейский журнал передових технологій. Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано - і мікроелектроніки*. 2013. Т.6, Вип. 2(66). С. 82-85.

4. Дудикевич В.Б., Опірський І.Р. Аналіз моделей захисту інформації в інформаційних мережах держави. *Системи обробки інформації*. 2016. Вип. 4 (141). С. 86-89.

5. Климович О.К. Застосування мобільних телекомунікаційних мереж спеціального призначення в Збройних Силах України. *Системи обробки інформації*. 2015. Вип. 5 (130). С. 135-140.

6. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2015. Вип. 1(29). С. 56-61.

7. Дудикевич В.Б., Микитин Г.В., Крет Т.Б. Концепція та базовий підхід до побудови системи захисту інформації в багаторівневій інтелектуальній системі керування. *Системи обробки інформації*. 2016. Вип. (145). С. 105-110.

8. МСЭ-Т X.1205. Серия X: сети передачи данных, взаимосвязь открытых систем и безопасность. Безопасность электросвязи. Обзор кибербезопасности. Женева. 2009. 64с.

9. Сторчак А.С., Сальник С.В., Крамський А.Є. Аналіз вразливостей та атак на державні інформаційні ресурси, що обробляються в інформаційно-телекомунікаційних системах. *Системи обробки інформації.* 2019. Вип. 2(157). С. 121-128.

10. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

11. Яковів І.Б. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека. *Information Technology and Security*. 2017. Вип. (9). с.134-144.

12. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних *Реєстрація, зберігання і обробка даних*. 2015. Вип. 17(2). С. 39-46.

13. Офіціальний сайт Common Vulnerabilities and Exposures. Режим доступу: http://cve.mitre.org (дата звернення: 24.03.2019).

14. Офіціальний сайт National Vulnerabilities Database. Режим доступу: http://nvd.nist.gov (дата звернення: 24.03.2019).

15. Офіціальний сайт United States Computer Emergency Readiness Team. Режим доступу: http://www.us-cert.gov (дата звернення: 24.03.2019).

16. Офіціальний сайт X-Force. Режим доступу: http://xforce.iss.net (дата звернення: 24.03.2019).

17. Офіціальний сайт Secunia. Режим доступу: http://secunia.com (дата звернення: 24.03.2019).

18. Офіціальний сайт BugTraq. Режим доступу: http://securityfocus.com (дата звернення: 24.03.2019).

19. Офіціальний сайт Офіціальний сайт Open Source Vulnerabilities Data Base. Режим доступу: http://osvdb.org (дата звернення: 24.03.2019).

20. Офіціальний сайт The MITRE Corporation. Режим доступу: http://attack.mitre.org (дата звернення: 24.03.2019).

21. Офіціальний сайт KDD Cup 1999 Data. Режим доступу: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99 (дата звернення: 24.03.2019).

22. Мехед Д., Ткач Ю., Базилевич В., Гур'єв В., Усов Я. Аналіз вразливостей корпоративних інформаційних систем *Захист інформації*. 2018. Вип. 20(1). С.61-66. DOI: 10.18372/2410-7840.20.12453.

23. Грищук Р., Охрімчук В., Ахтирцева В. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак *Захист інформації*. 2016. Вип. 18(1). С.21-29.

24. Труш О.В., Хахлюк О.А. Цілісність інформації в інформаційно-телекомунікаційних системах спеціального призначення: загрози та методи захисту *Сучасний захист інформації*. 2013. Вип.2. С.31-35.

25. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ: НАУ, 2013. 432 с.

26. Сторчак А.С., Сальник С.В., Микитюк А.В., Дівіцький А.С. Аналіз методів прийняття рішень з забезпечення захищеності комунікаційних систем. *Наука і техніка Повітряних Сил Збройних Сил України*. 2019. Вип. 3(36). С. 122-131.

27. Конахович Г.Ф., Корченко О.Г., Юдін О.К. Захист інформації в мережах передачі даних. Київ: Видавництво ТОВ "НВП "ІНТЕРСЕРВІС". 2009. 716 с.

28. Kubecka C., 28c3: Security Log Visualization with a Correlation Engine. December 29, 2011.

29. Subach I., Mykytiuk A., Kubrak V. Architecture and functional model of a perspective proactive intellectual siem for cyber protection of objects of critical infrastructure. *Information Technology And Security*. 2019. Вип. 7 № 2. С. 208-215. DOI: 10.20535/2411-1031.2019.7.2.190570

30. Зоріна Т.І. Системи виявлення і запобігання атак в комп'ютерних мережах. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2013. Вип. 15(1). С. 48-52.

31. Бурячок В.Л. Сучасні системи виявлення атак в інформаційно-телекомунікаційних системах і мережах. Модель вибору раціонального варіанта реагування на прояви стороннього кібернетичного впливу. *Інформаційна безпека*. 2013. Вип. 1. С. 33–40.

32. Сєвєрінов О.В., Хрєнов А.Г. Аналіз сучасних систем виявлення вторгнень. *Системи обробки інформації*. 2014. Вип. 6(122). С. 122-124.

33. Duravkin I.V., Carlsson Anders, Loktionova A.S. Method of slow-attack detection *Системи обробки інформації*. 2014. Вип. 8(124). С.102–106.

34. Шипова Т.Н., Босько В.В., Березюк И.А., Пархоменко Ю.М. Анализ современных методов обнаружения вторжений в компьютерные системы. *Системи обробки інформації*. 2016. Вип. 1(138). С. 133–137.

35. Рубан І.В. Мартовицький В.О., Партика С.О. Класифікація методів виявлення аномалій в інформаційних системах. *Системи озброєння і військова техніка*. 2016. Вип. 3(47). С. 100–105.

36. More S., Matthews M., T.Finin T. A Knowledge-Based Approach To Intrusion Detection Modeling. *Proceedings of the IEEE Workshop on Semantic Computing and Security.* 2012. С. 75–81.

37. Кучук Г.А., Косенко В.В., Давікоза О.П. Метод управління розподілом ресурсів багатосерверного вузла обробки інформації. *Збірник наукових праць Харківського національного університету Повітряних Сил.* 2013. Вип.3(36). С. 111–115.

38. Zhang Y., Lee W., Huang Y. Intrusion detection techniques for mobile wireless networks. *Wireless Networks Journal (ACM WINET).* 2003. № 9(5). P. 545–556.

39. Janakiraman R., Waldvogel M., Zhang Qi. A peer-to-peer approach to networkintrusion detection and prevention. *Enabling Technologies: Infrastructure for Collaborative Enterprises.* 2003. P. 226–231, DOI:10.1109/ENABL. 2003.1231412

40. Горбенко В.І., Картавих В.Ю., Субач І.Ю. Модель моніторингу домену управління інформаційної мережі військового призначення *Системи обробки інформації*. 2013. Вип. 4(111). С. 118-122.

41. Alshboul Y., Streff K., Analyzing Information Security Model for Small-Medium Sized Businesses, *Twenty-first Americas Conference on Information Systems*, Puerto Rico, 2015.

42. Safa N.S., Solms R.V., Furnell S. Information security policy compliance model in organizations. *Computers & Security*. 2016. Vol. 56. P. 70-82. DOI:10.1016/j.cose.2015.10.006

43. Nazareth D.L., Choi J. A system dynamics model for information security management. *Information & Management*. 2015. Vol. 52, issue 1. P. 123-134. DOI:10.1016/j.im.2014.10.009

44. Антонюк А.О. Моделювання систем захисту інформації: монографія. Ірпінь: Національний університет ДПС України, 2015. 273 с.

45. Ільяшов О.А., Бурячок В.Л. До питання захисту інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу. *Наука і оборона*. 2010. Вип. 4. С.35–40.

46. Романов О.І., Лівенцев С.П., Павлов І.М. Математична модель захисту інформації в автоматизованих мережах спеціального призначення. *Збірник наукових праць ВІТІ НТУУ "КПІ"*. 2004. Вип. 5. С. 23–31.

47. Шипова Т.Н., Босько В.В., Березюк И.А., Пархоменко Ю.М. Анализ современных методов обнаружения вторжений в компьютерные системы. *Системи обробки інформації*. 2016. Вип. 1(138). С. 133–137.

48. Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П. Методика оцінки кібернетичної захищеності системи зв'язку організації. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2018. Вип. 1 (31). С. 43-46.

49. Кучернюк П.В., Довгаль А.О. Модель загроз безпеки в інформаційно-комунікаційних системах на основі регресійного аналізу. *Електроніка та зв'язок*. 2017. Вип., № 2(97), т. 22. С. 79–84.

50. Бурячок В.Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем. *Захист інформації*. 2011. Вип. 3(52). С. 19–27.

51. Хусаінов П.В. Показник кібернетичної безпеки автоматизованої системи у часі. *Збірник наукових праць ВІТІ*. 2015. Вип. 1. С. 101–111.

52. Куцаєв В.В., Радченко М.М., Козубцова Л.М., Терещенко Т.П. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку. *Збірник наукових праць ВІТІ*. 2018. Вип. 2. С. 67–76.

53. Мірошник М.А. Розробка методів оцінки ефективності захисту інформації в розподілених комп'ютерних системах. *Інформаційно-керуючі системи на залізничному транспорті*. 2015. Вип. 4(113). С. 39–43.

54. Raiyn J. A survey of Cyber Attack Detection Strategies. *International Journal of Security and Its Applications*. 2014. Vol. 8, issue 1. P. 247–256. DOI: 10.14257/ijsia.2014.8.1.23

55. Лантвойт О.Б., Гришин С.П., Винярський Я.Я. Інформаційне забезпечення комплексного керування захистом складних систем управління. *Сучасна спеціальна техніка*. 2011. Вип.2(25). С.112–117.

56. Лєнков С.В., Винярський Я.Я., Мелкумян Р.Г. Щодо задач оперативного оцінювання стану військової безпеки держави. *Вісник хмельницького національного університету. Технічні науки*. 2011. Вип. 5. С. 201–203.

57. Беллман Р. Динамическое программирование. М.: Изд-во иностранной литературы, 1960. 400 с.

58. Danijela D. Review of KDD CUP '99, NSL-KDD and KYOTO 2006+ Datasets. *Protić vojnotehni čki glasnik military technical courier*. 2018. Vol. 66, issue 3. DOI: 10.5937/vojtehg66-16670

59. Безкоровайний В.В., Трофименко І.В. Структурно-параметрична ідентифікація моделей багатофакторного оцінювання. *Системи озброєння і військова техніка*. 2006. Вип. № 3(7). С. 56–58.

60. Дивак М. П. Задачі математичного моделювання статичних систем з інтервальними даними: монографія. Тернопіль: Видавництво ТНЕУ «Економічна думка», 2011. 216 с.

61. Коршунов Ю.М. Математические основы кібернетики: учебное пособие для вузов. Москва: Энергия, 1980. 424 с.

62. Лівенцев С.П., Сторчак А.С. Виявлення комп'ютерних атак в інформаційно-телекомунікаційних системах на основі методів індуктивного прогнозування станів. *Information Technology And Security.* 2012. Вип. 1(1). С. 100–104.

63. Ливенцев С.П., Сторчак А.С. Модели и методы анализа защищенности автоматизированных систем / *Безопасность информации в информационно-телекоммуникационных системах*: тезисы докладов XV Юбилейной Междунар. Науч.-практич. Конференции, Киев. 2012. С.74–75.

64. Черемных С.В., Семенов И.А., Ручкин В.С. Моделирование и анализ систем. IDEF-технологии. Москва: Финансы и статистика. 2006. 192 с.

65. Котенко И.В., Степашкин М.В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак. *Труды ИСА РАН*. 2007. Т. 31. С. 126–207.

ДОДАТОК А

Параметри мережевого трафіка

№ з/п	Параметр	Опис	Тип атаки
Основні ознаки			
1.	*duration*	Тривалість з'єднання (у секундах)	зовнішня
2.	*protocol_type*	Тип протоколу (TCP, UDP, etc.)	внутрішня, зовнішня
3.	*service*	Сервіс атакованого рівня	внутрішня
4.	*flag*	Статус з'єднання	внутрішня
5.	*src_bytes*	Вхідний потік, байт	внутрішня, зовнішня
6.	*dst_bytes*	Вихідний потік, байт	внутрішня, зовнішня
7.	*land*	Співпадіння адрес, 1 якщо з'єднання від/до того самого вузла	внутрішня, зовнішня
8.	*wrong_fragment*	Кількість неправільних фрагментів	внутрішня, зовнішня
9.	*urgent*	Кількість термінових пакетів	внутрішня, зовнішня
Статистичні ознаки			
10.	*count*	Кількість з'єднань з співпадаючим вузлом в поточній сесії.	внутрішня
11.	*serror_rate*	% з'єднань що мали помилки „SYN"	внутрішня, зовнішня
12.	*rerror_rate*	% з'єднань що мали помилки „REJ" та з`єнання з однаковим вихідним вузлом	внутрішня
13.	*same_srv_rate*	% з'єднань з однаковим сервісом	внутрішня, зовнішня
14.	*diff_srv_rate*	% з'єднань на різні сервіси	внутрішня
15.	*srv_count*	Кількість з'єднань на такий самий сервіс.	зовнішня
16.	*srv_serror_rate*	% з'єднання з помилкою „SYN" в пакеті	внутрішня, зовнішня
17.	*srv_rerror_rate*	% з'єднання, що мають помилки „REJ"	внутрішня, зовнішня
18.	*srv_diff_host_rate*	% з'єднаннь з різними вузлами	внутрішня, зовнішня
Ознаки окремого з`єднання			
19.	*hot*	Кількість „гарячих" індикаторів	зовнішня
20.	*num_failed_logins*	Кількість невдалих спроб входу	зовнішня

21.	*logged_in*	Вдалий вхід в систему - 1, невдалий - 0	внутрішня
22.	*num_compromised*	Кількість „компроментуючих” умов	внутрішня, зовнішня
23.	*root_shell*	Доступ з адміністративними повноваженнями - 1; інакше 0	внутрішня
24.	*su_attempted*	1, якщо виконувалась „su root”; інакше 0	внутрішня
25.	*num_root*	Кількість спроб доступа з правами користувача	внутрішня
26.	*num_file_creations*	Кількість операцій створення файлів	внутрішня
27.	*num_shells*	Кількість спроб використання запитів на надання доступу	внутрішня
28.	*num_access_files*	Кількість операцій с файлами контролю доступу	зовнішня
29.	*num_outbound_cmds*	Кількість вихідних команд для FTP сесії	зовнішня
30.	*is_hot_login*	1, якщо логін належав до „гарячого” списку	зовнішня
31.	*is_guest_login*	1, якщо „гостьовий” вхід	зовнішня
Додаткові ознаки			
32.	*dst_host_count*	Кількість з`єднань до вузла, встановлених віддаленою стороною та використовуючих різні служби	зовнішня
33.	*dst_host_srv_count*	Кількість з`єднань до вузла, встановлених віддаленою стороною та використовуючих одну службу	зовнішня
34.	*dst_host_same_srv_rate*	% з`єднань до вузла, встановлених віддаленою стороною та використовуючих одну службу	зовнішня
35.	*dst_host_diff_srv_rate*	% з`єднань до вузла, встановлених віддаленою стороною та використовуючих різні служби	зовнішня
36.	*dst_host_same_src_port_rate*	% з`єднань до вузла з поточним джерелом	зовнішня
37.	*dst_host_srv_diff_host_rate*	% з`єднань до вузла з різним джерелом	зовнішня
38.	*dst_host_serror_rate*	% з`єднань з помилкою типу SYN для даного приймача	зовнішня
39.	*dst_host_srv_serror_rate*	% з`єднань з помилкою типу SYN для служби приймача	зовнішня
40.	*dst_host_rerror_rate*	% з`єднань з помилкою типу REJ для даного приймача	зовнішня
41.	*dst_host_srv_rerror_rate*	% з`єднань з помилкою типу REJ для служби приймача	зовнішня

ДОДАТОК Б

Список наукових публікацій

1. А.А. Кулько, С.В. Толюпа Виявлення атак за допомогою методу опорних векторів. III міжнародна науково-практична конференція. Проблеми кібербезпеки інформаційно-телекомунікаційних систем. Збірник матеріалів доповідей та тез. м. Київ, 2020 р. КНУ імені Тараса Шевченка. с. 105-109.

2. Толюпа С.В., Шестак Я.В., Кулько А.А., Чечуга А.М. Автоматизація процесу управління інцидентами інформаційної безпеки. Збірник тез IV Міжнародної науково-практичної конференції «Прикладні системи та технології в інформаційному суспільстві». К.: Київський нац. ун-т імені Тараса Шевченка, 2020. – 215-222с.

3. Сергій Толюпа, Олександр Успенський, Андрій Кулько, Олег Кулініч. Вплив кібернетичних атак на інформаційну систему. Збірник матеріалів доповідей та тез. IV Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS). – К.: ВПЦ"Київський університет", 2021. – 149-151 с.