МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Безпека комп'ютерних систем і мереж»

Група: 4КБ-02

Дипломний проект

здобувача освіти денної форми навчання
КБ.02.23.000.ДП

ЧІРКОВА
ЄВГЕНА ВІКТОРОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітньо-професійна програма: «**Безпека комп'ютерних систем і мереж»**

Група: **4КБ-02**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту на тему:

Розробка програмної моделі оцінки рівня стійкості комп'ютерних систем і мереж

Проектний матеріал складається з пояснювальної записки на 76 сторінках та графічного (презентаційного) матеріалу на 18 аркушах (слайдах)

Дипломник _____ (Чірков Є.В.)

Керівник _____ (Кривченко А.А.)

Консультанти:

з економічного розділу _____ (Канський М.Ю.)

з розділу охорони праці та техніки безпеки _____ (Чорновол Н.І.)

з нормоконтролю _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Голова циклової комісії _____ (Кривченко Ю.В.)

Завідувач відділення _____ (Краснокутська К.Г.)

Захист «27» червня 2025 р. Протокол ЕК № 6

Оцінка ЕК 5 (відмінно) / 90 б.

Секретар ЕК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Комісія *КТ та ПІ*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітньо-професійна програма *«Безпека комп'ютерних систем і мереж»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР *Беркань І.В.*

"19" 05 2025 р.

ЗАВДАННЯ

на дипломний проект

Здобувачеві освіти *Чіркову Євгену Вікторовичу*

(прізвище, ім'я, по батькові)

1. Тема проекту *Розробка програмної моделі оцінки рівня стійкості комп'ютерних систем і мереж*

затверджена наказом по коледжу від "14" 11 2024 р. № 246

2. Термін здачі закінченого проекту 16.06.25

3. Вихідні данні до проекту *1. Реалізувати програмну модель оцінки рівня стійкості КСМ завдяки розрахунку надійності, захищеності та живучості; 2. Передбачити можливість додавання та видалення подій спуфінгу при визначенні показника надійності; 3. Передбачити розрахунок показника захищеності на основі ймовірності реалізації загальних кібератак та ймовірності реалізації цілеспрямованих кібератак; 4. Створити візуальний інтерфейс застосунку, дружній до користувача*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Аналіз методів та засобів оцінки рівня стійкості комп'ютерних систем і мереж; Розробка моделі загроз інформаційним об'єктам у комп'ютерних системах і мережах; Розробка системи захисту інформації комп'ютерних систем і мереж; Розробка програмної моделі оцінки рівня стійкості комп'ютерних систем і мереж; Економічні розрахунки; Заходи охорони праці та ТБ

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Схема класифікації атак; Аналіз ефективності різних підходів таксономій загроз ІБ; Ієрархічна структура атаки на інформаційну систему; Функціональна схема атаки на інформаційну систему; Матриця загроз для програмних та апаратних засобів КСМ; Модель бази даних з розподілом ролей користувачів (СУБД); Модель бази даних загроз інформаційним об'єктам; Структурна модель багаторівневої системи виявлення впливів; Класифікація стану об'єкта КСМ за рівнем живучості; БСА методології оцінювання стійкості КСМ; Розрахунок комплексного показника стійкості об'єктів КСМ (інтерфейс застосунку)

6. Консультанти по проекту, із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основний розділ	*Кривченко А.А.*		
Економічний розділ	*Канський М.Ю.*		
Розділ охорони праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання 13.05.25

Керівник *Кривченко А.А.* _____
(підпис)

Завдання прийняв до виконання *Чірков Є.В.* _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1	*Вступ. Постановка задачі проектування*	16.05.25.	виконано
2	*Аналіз технічного завдання та пошук літератури*	17.05.25.	виконано
3	*Аналіз методів та засобів оцінки рівня стійкості*		виконано
	комп'ютерних систем і мереж	19.05.25.	
4	*Розробка моделі загроз інформаційним об'єктам у*		виконано
	комп'ютерних системах і мережах	20.05.25.	
5	*Розробка системи захисту інформації комп'ютерних*		виконано
	систем і мереж	21.05.25.	
6	*Вибір програмних засобів розробки*	22.05.25.	виконано
7	*Розробка програмної моделі оцінки рівня стійкості*		
	комп'ютерних систем і мереж	23.05.25.	виконано
8	*Реалізація візуального інтерфейсу застосунку*	01.06.25.	виконано
9	*Написання коду програми мовою С++*	03.06.25	виконано
10	*Випробування застосунку та аналіз результатів*	05.06.25	виконано
11	*Виконання економічних розрахунків*	07.06.25.	виконано
12	*Розробка питань з охорони праці та техніки безпеки*	08.06.25	виконано
13	*Підготовка мультимедійної презентації проекту*	09.06.25.	виконано

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КБ 02. 23 000. 00 ДП	Дипломний проект		
А4			КБ 02. 23 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	КБ 02. 23 000. 00 ДП		
Розробив		Чірков Є.В.		16.06	Розробка програмної моделі оцінки рівня стійкості комп'ютерних систем і мереж	Літ.	Аркуш 4 / Аркушів 76
Перевірив		Кривченко А.А.		16.06		Н Д П	
Н. контр.		Петрашова В.І.		16.06		ВСП "ОТФК ОНТУ" гр.4КБ-02	
Затверд.		Кривченко Ю.В.		16.06			

ЗМІСТ

ВСТУП

Сучасні загрози та події демонструють необхідність покращення захисту комп'ютерних систем та мереж від кіберзагроз. Це спонукає до розробки програмної моделі для оцінки рівня безпеки комп'ютерних систем та мереж. Цей дипломний проект спрямований на підвищення рівня захисту інформації від кібератак.

Для досягнення цієї мети необхідно виконати аналіз існуючих методів та засобів захисту інформації, створити таксономію кіберзагроз, розробити матрицю залежності об'єктів захисту від типу загроз, створити модель бази даних загроз, розробити методи розпізнавання кіберзагроз та методики оцінки кіберстійкості. Планується також створити багаторівневу систему виявлення підозрілих впливів та розробити програмний застосунок для розрахунку рівня кіберстійкості.

Цей проект передбачає такі основні етапи: аналіз сучасних методів захисту, створення таксономії інформаційних загроз, розробка моделі бази даних загроз, розробка методів розпізнавання та оцінки кіберстійкості, створення багаторівневої системи виявлення підозрілих впливів та розробка програмного забезпечення для оцінки рівня стійкості комп’ютерних систем і мереж.

Проект охоплює процеси захисту інформації у комп'ютерних системах та мережах, з акцентом на методи та засоби захисту від кіберзагроз. Практична значущість проекту полягає у створенні програмного застосунку, що автоматизує процес оцінки рівня безпеки комп'ютерних систем і мереж та забезпечує ефективний захист від кіберзагроз.

Результати проекту дозволять підвищити рівень кібербезпеки та забезпечити надійний захист інформації в сучасному інформаційному середовищі. Це надасть користувачам інструменти для виявлення та запобігання кіберзагрозам, забезпечуючи надійну інформаційну безпеку комп'ютерних систем та мереж. Впровадження таких засобів захисту допоможе зменшити ризики інформаційних атак та забезпечити стабільну роботу комп'ютерних систем у різних сферах діяльності.

1 ОСНОВНИЙ РОЗДІЛ

1.1 Аналіз методів та засобів оцінки рівня стійкості комп’ютерних систем і мереж

1.1.1 Огляд підходів до класифікації загроз інформаційній безпеці комп'ютерних систем і мереж

Зростаюча кількість комп'ютерних атак вимагає створення організованих структур, які б забезпечували актуальну інформацію про кіберзагрози, кібератаки та вразливості систем, а також їх оперативне усунення. З цієї причини існує значна кількість інформації про актуальні атаки та вразливості комп'ютерних мереж і систем. Проте ця інформація часто є неструктурованою, що ускладнює її аналіз. Тому виникає необхідність у розробці моделі та інструментарію, які б дозволили систематизувати накопичені знання, тобто створити таксономію. Таксономія забезпечує систематичний опис комп'ютерних атак і використовується для подальшого аналізу та оцінки ризиків, створення моделей загроз та порушників на етапах проектування критичних систем, розробки політики безпеки та засобів активного аудиту.

Таблиця 1.1. Основні вимоги до таксономії загроз

Вимога	*Опис*
Взаємне виключення	Кожна категорія повинна бути взаємно виключаючою
Повнота	Таксономія повинна охоплювати всі можливі атаки
Детермінованість	Процес класифікації повинен бути чітко визначеним
Чіткість термінів	Всі терміни повинні бути чітко визначені
Об'єктивність	Розглядати тільки ті дані, що можуть бути об'єктивно спостережені
Застосовність	Таксономія повинна бути корисною для практичного застосування
Зрозумілість	Таксономія повинна бути зрозумілою навіть неекспертам
Однозначність	Категорії повинні бути чітко визначені для уникнення двозначностей
Узгодженість	Термінологія має узгоджуватися з загальноприйнятою
Повторюваність	Класифікація повинна давати однакові результати незалежно від класифікатора

Щоб таксономія була ефективною, вона повинна задовольняти певним вимогам (табл.1.1): взаємне виключення (категорії не повинні перетинатися), повнота (охоплення всіх можливих атак), детермінованість (чіткість класифікаційної схеми), чіткість термінів, об'єктивність, застосовність, зрозумілість, однозначність, узгодженість з загальноприйнятою термінологією та повторюваність результатів. Всі ці вимоги мають забезпечити, щоб класифікація була ефективною та корисною для подальшого аналізу атак. Приклад таксономії комп'ютерних атак наведено у табл.1.2.

Таблиця 1.2. Класифікація за типом вразливостей

Категорія	*Підкатегорія*	*Опис*
Вразливості мережі	Неправильна конфігурація, відсутність шифрування	Вразливості, пов'язані з некоректною конфігурацією мереж та відсутністю захисту
Вразливості програмного забезпечення	Помилки в коді, відсутність оновлень	Вразливості, що виникають через помилки в програмному коді або відсутність оновлень
Фізичні вразливості	Доступ до обладнання, відсутність фізичного захисту	Вразливості, пов'язані з фізичним доступом до комп'ютерних систем та відсутністю відповідного захисту

Діаграма на рис.1.1 представляє собою дерево атак, що класифікує загрози інформаційній безпеці. Структура діаграми:

1. Кореневий вузол:
   - "Атаки" – загальне поняття, що об'єднує всі види загроз;
2. Дві основні гілки:
   - "Конфіденційність" – загрози, що пов’язані з несанкціонованим доступом до даних;
   - "Цілісність" – загрози, що стосуються модифікації даних.
3. Дочірні вузли:
   - для Конфіденційності:
     - "Викрадення даних" – отримання доступу до конфіденційної інформації;
     - "Перехоплення" – підслуховування або запис переданих даних;

- для Цілісності:
  - "Модифікація даних" – несанкціонована зміна або підміна інформації;
  - "Внесення шкідливого коду" – впровадження вірусів, троянів або бекдорів.

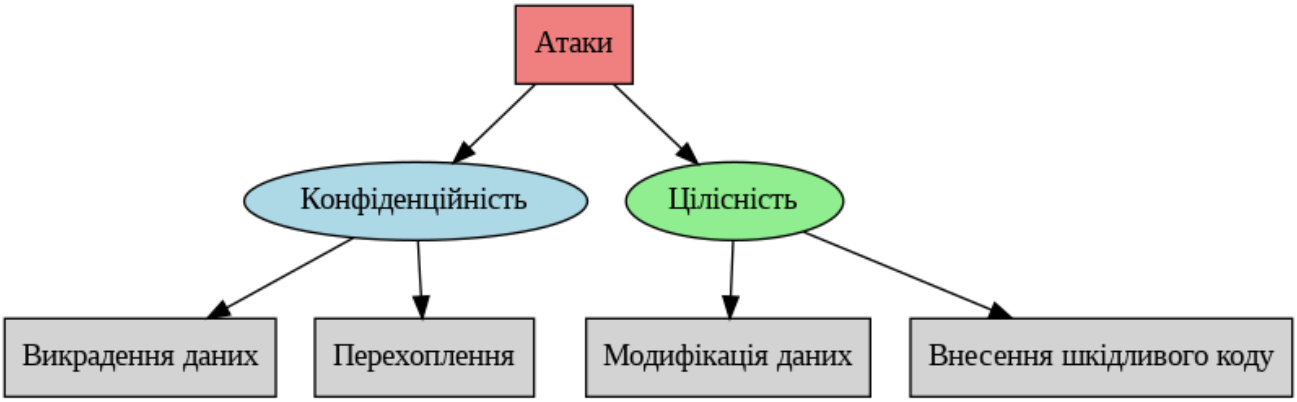


Рисунок 1.1. Схема класифікації атак

Приклади атак відповідно до рис.1.1 є такими:

1. Перехоплення даних: Атака на конфіденційність, коли злочинець перехоплює дані під час їх передачі через незахищену мережу.

2. Внесення шкідливого коду: Атака на цілісність, коли шкідливий код додається до програмного забезпечення, змінюючи його поведінку.

Класифікація та розробка таксономії кіберзагроз є важливим завданням, яке потребує врахування багатьох чинників та підходів, щоб забезпечити ефективну та всебічну систему захисту інформаційної безпеки комп'ютерних систем і мереж. Впровадження таких засобів захисту допоможе зменшити ризики інформаційних атак та забезпечити стабільну роботу комп'ютерних систем у різних сферах діяльності.

Таксономія загроз інформаційній безпеці комп'ютерних систем і мереж, представлена у графічному вигляді на рис. 1.2, являє собою структуроване дерево, де кореневою вершиною є "вторгнення". Це дерево має ребра, що несуть смислове навантаження. Одне з них позначає "здійснено з допомогою", а інше – "мало результат". Такий підхід дозволяє систематизувати різні аспекти загроз та відобразити логічні зв'язки між ними. Пунктирні стрілки на діаграмі вказують на

відношення "є підкласом", що допомагає виявити підкатегорії загроз, наприклад, такі як переповнення буфера чи некоректні вхідні дані. Це робить модель більш деталізованою, що дозволяє краще розуміти різні рівні атак і загроз.

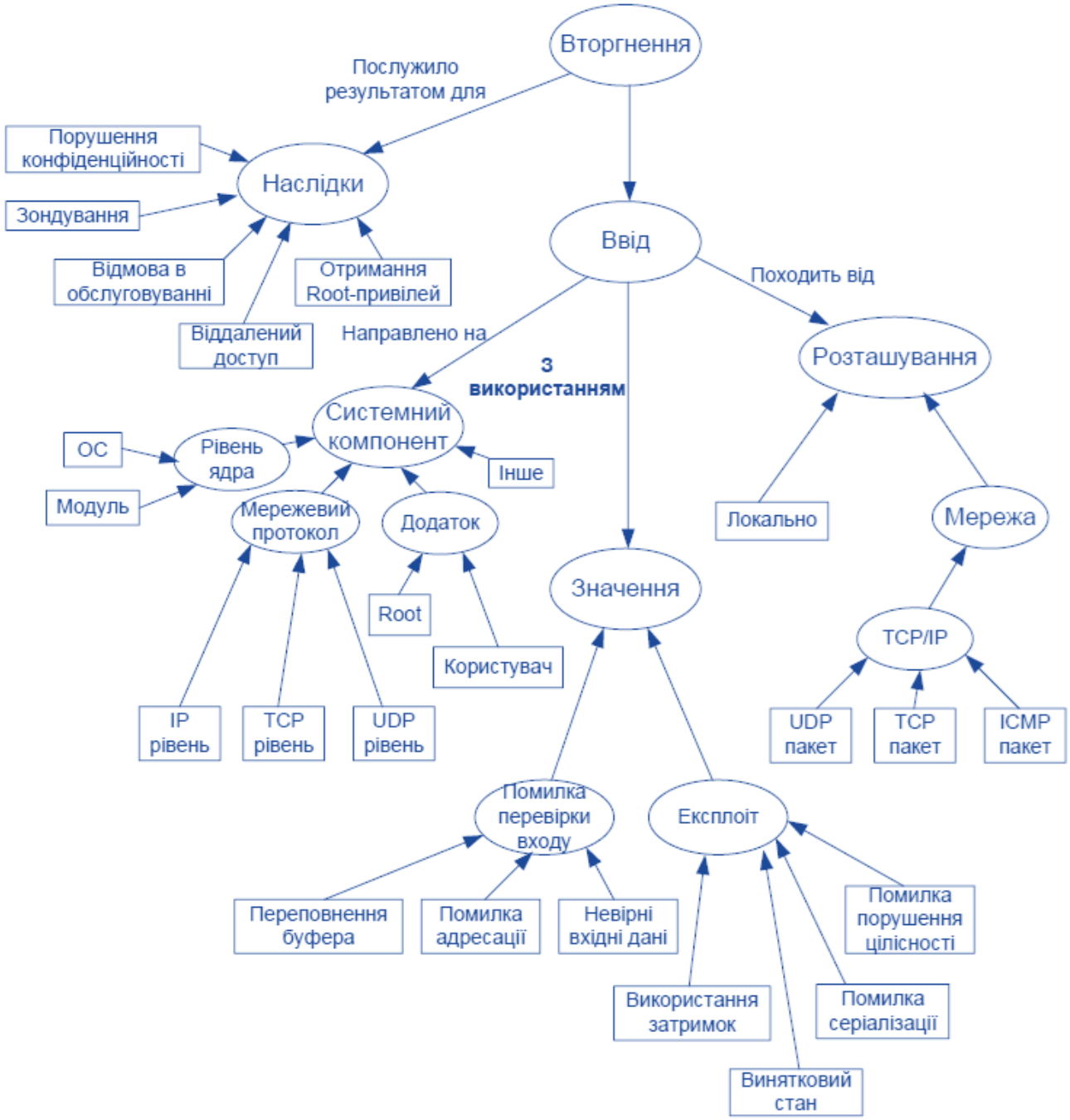


Рисунок 1.2. Таксономія загроз інформаційній безпеці на основі вторгнення

Однак, попри таку деталізацію, підхід має свої обмеження. Він не завжди може відобразити складні сценарії атак, які можуть складатися з кількох етапів або змінювати стратегію в процесі. Деревоподібна структура добре підходить для статичних описів, але атаки часто динамічні та мають різні фази, які важко

класифікувати таким чином. Зазначено, що цей недолік є суттєвим, оскільки сучасні системи захисту вдосконалюються, а методи атак стають більш складними та витонченими. Тому класична таксономія не завжди може повною мірою відобразити сучасні загрози.

Ще один виклик полягає в тому, що із зростанням складності атак і захисних систем, таксономія повинна постійно оновлюватися. Впровадження нових видів атак, які можуть використовувати інтелектуальні системи чи нові техніки, не завжди вписується у вже існуючі моделі загроз. Це означає, що навіть такий детальний підхід, як цей, потребує адаптації до нових умов. Також важливо зазначити, що хоча таксономія дозволяє чітко визначати різні типи атак, вона не враховує динамічних взаємозв'язків між ними. Багато атак можуть змінювати свої характеристики в залежності від відповідних дій системи захисту або зовнішніх факторів, що не відображено у фіксованій структурі таксономії.

Враховуючи постійне вдосконалення атакуючих технік, таксономії необхідно еволюціонувати разом із загрозами, інтегруючи нові підходи до класифікації. Це може включати сценарії атак або адаптивні моделі, що дозволяють враховувати різні стадії атаки. Такий підхід забезпечить більш глибокий аналіз та допоможе побудувати ефективніші системи захисту.

Таксономія, представлена на рис. 1.3, фокусується на понятті «інцидент», що є ключовим елементом у цій моделі. Інцидент включає в себе такі компоненти, як атакуючий, атака та мета атаки. Поняття «атака» охоплює ті сутності, що безпосередньо стосуються процесу нападу: інструмент, вразливість, дія, цільовий об'єкт і несанкціонований результат. Інструментом вважається засіб, який атакуючий застосовує для виконання атаки. Подія, згідно з цією таксономією, складається з двох елементів – дії та цільового об'єкта.

Головна відмінність цієї моделі полягає в тому, що вона включає структурні елементи і передбачає можливість комбінування подій у рамках інциденту. Така особливість дозволяє описувати складні багатокрокові атаки, зокрема враховувати сценарій їхнього розвитку, що є важливим для сучасного аналізу загроз, коли атаки стають все більш складними та багатофазними.

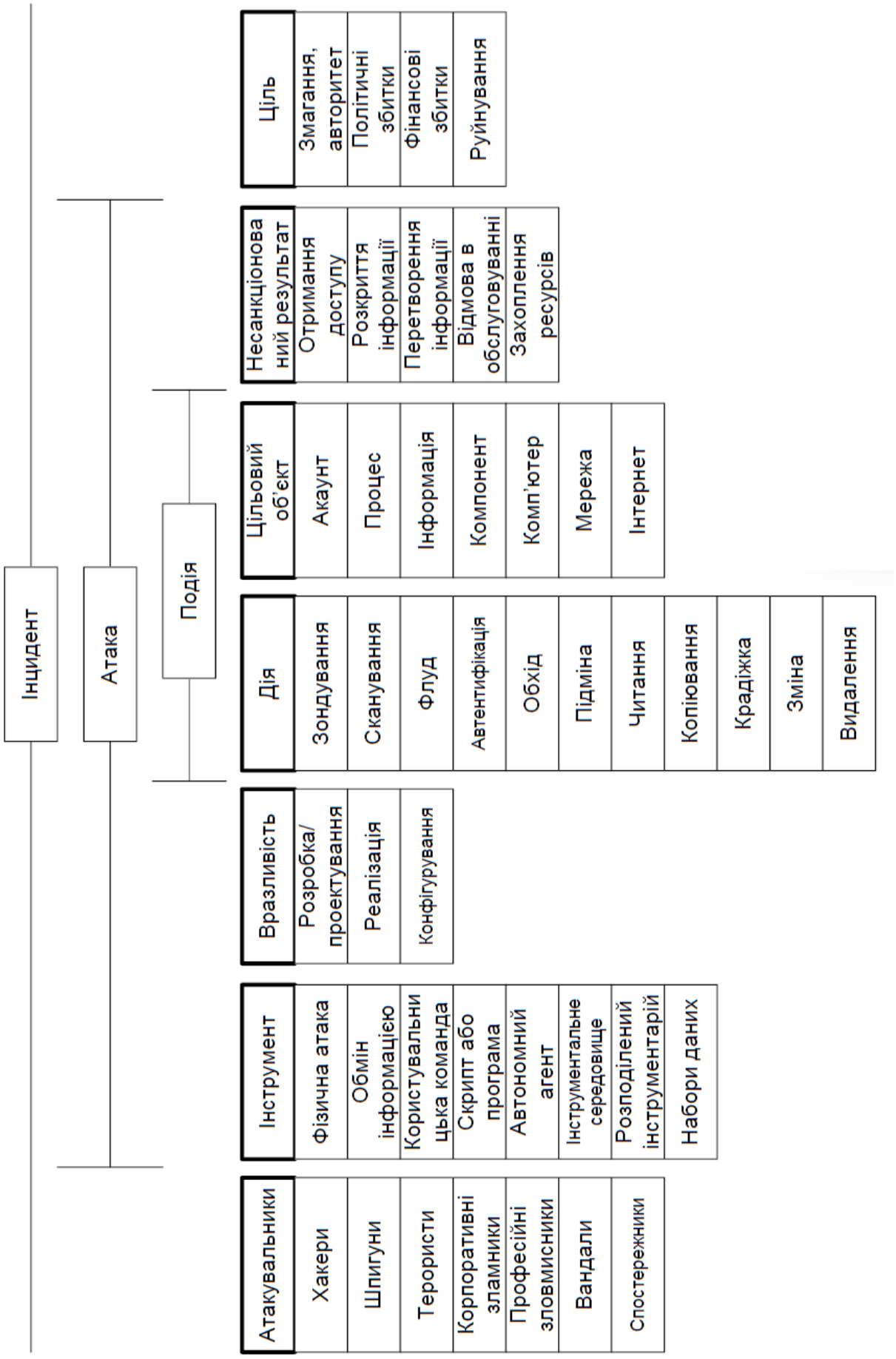


Рисунок 1.3. Таксономія загроз інформаційній безпеці на основі інцидентів

У табл. 1.3 наведено аналіз різних підходів до розробки таксономій загроз інформаційній безпеці за низкою критеріїв, таких як інформативність, повнота, детермінованість, чіткість термінів, об'єктивність та інші. У таблиці зазначені підходи до класифікації загроз, зокрема підходи на основі впливу на інформацію, вразливості апаратного і програмного забезпечення, загальних списків атак та комбіновані підходи. Кожен з підходів оцінюється за різними характеристиками, відображаючи їх переваги та недоліки.

Таблиця 1.3. Аналіз ефективності різних підходів таксономій загроз ІБ

Властивості / підходи до класифікації	Застосовуваність (інформативність)	Повнота	Детермінованість	Взаємне виключення	Чіткість термінів	Об' єктивність	Зрозумілість	Однозначність	Узгодженість	Повторюваність результатів
За ефектом впливу на властивості інформації	-	+	+	-	-	+	-	-	+	-
Вразливості апаратного та програмного забезпечення	+	-	+	+	+	+	+	+	-	-
Загальний список атак	+	-	-	-	+	+	-	-	+	-
Комбінований підхід	+	+	+	+	+	+	+/-	+	+	+

1.1.2. Аналіз мети проектування та уточнення технічного завдання

При розробці програмної моделі оцінки рівня захищеності комп'ютерних систем і мереж, першочергове завдання полягає у визначенні та уточненні мети проектування, а також у формуванні точного технічного завдання. На основі аналізу сучасних підходів до забезпечення інформаційної безпеки, розробка такої моделі повинна забезпечити підвищення стійкості комп'ютерних систем до кібервпливів, а також адаптацію до новітніх загроз, що постійно еволюціонують в умовах швидкого розвитку інформаційних технологій.

На основі технічного завдання на проектування та виконаного у п.1.1.1 аналізу, мета і задачі дипломної роботи є такими:

Головною метою розробки програмної моделі є підвищення рівня захищеності інформації, яка циркулює в комп'ютерних системах і мережах, від

різних типів кібератак та кіберзагроз. Для цього необхідно створити універсальну методику оцінки стійкості інформаційних об'єктів захисту до впливу потенційних загроз, а також розробити інструменти для виявлення та нейтралізації можливих вразливостей на ранніх етапах. Ця мета відповідає сучасним вимогам щодо захисту критичної інформаційної інфраструктури в умовах стрімкого зростання кількості та складності кібератак.

Підвищення рівня кіберзахисту комп’ютерних мереж та систем передбачає:

1. Покращення методів і засобів аналізу загроз. Це включає в себе розробку детальної таксономії інформаційних загроз, яка враховує сучасні загрози та нові кіберзлочинні техніки;

2. Підвищення стійкості до атак за допомогою розпізнавання вразливостей. Розроблена методика повинна забезпечувати автоматизований аналіз комп’ютерних систем і мереж для своєчасного виявлення кіберзагроз і відповідної оцінки їх впливу на інформаційні ресурси;

3. Оцінка рівня кіберстійкості систем. Успішне досягнення мети потребує створення інструменту, який дозволяє кількісно оцінювати кіберстійкість систем, що враховує як технічні характеристики, так і поведінкові патерни системи у відповідь на різні типи атак.

Для досягнення мети проектування визначено такі основні задачі:

1. Аналіз сучасних методів і засобів захисту інформації в комп'ютерних мережах та системах. Необхідно дослідити існуючі рішення для забезпечення інформаційної безпеки з метою виявлення їх слабких та сильних сторін, що дозволить визначити актуальні напрями покращення кіберзахисту;

2. Розробка таксономії інформаційних загроз. Цей крок передбачає класифікацію сучасних кіберзагроз за різними критеріями: типом атак, векторами вторгнень, метою атакуючих та впливом на інформаційні ресурси. Створена таксономія допоможе більш точно оцінювати ризики для інформаційних систем;

3. Створення матриці залежності інформаційних об'єктів захисту від потенційних загроз. Необхідно розробити модель, яка відображатиме взаємозв'язки між різними інформаційними об'єктами та типами загроз, що

дозволить оцінювати ступінь їх вразливості;

4. Розробка моделі бази даних загроз інформаційним об'єктам. Така база повинна включати інформацію про відомі типи атак, їхні характеристики, а також методи протидії, що сприятиме автоматизації процесів ідентифікації загроз;

5. Розробка методу розпізнавання кіберзагроз. Метод повинен базуватися на використанні машинного навчання або експертних систем для автоматизованого виявлення підозрілих активностей у мережах;

6. Розробка методики оцінювання кіберстійкості комп'ютерних систем і мереж. Оцінювання кіберстійкості дозволить більш чітко визначати слабкі місця у системах захисту і своєчасно їх усувати;

7. Розробка структурної моделі багаторівневої системи виявлення підозрілих активностей. Ця система повинна забезпечувати контроль за мережевою активністю в реальному часі і бути здатною до адаптації під нові типи атак;

8. Розробка алгоритму та програмного забезпечення для оцінки рівня стійкості комп'ютерних систем. Результатом роботи має стати програмний продукт, який дозволить автоматично оцінювати рівень стійкості мереж та систем на основі наданих даних про кіберзагрози і вразливості.

Технічне завдання передбачає розробку програмного комплексу, який повинен виконувати такі функції:

- Збір і аналіз даних про поточний стан інформаційної безпеки КС і М;
- Ідентифікація вразливостей та оцінка ймовірності їх використання зловмисниками;
- Розпізнавання кіберзагроз на основі розроблених алгоритмів і їх відповідна класифікація;
- Оцінка ефективності існуючих методів захисту та рекомендації щодо їх покращення.

1.2 Розробка моделі загроз інформаційним об’єктам у комп’ютерних системах і мережах

1.2.1 Розробка таксономії загроз інформаційній безпеці комп’ютерних систем і мереж

У цьому розділі розглянуто створення таксономії загроз для захисту інформації в комп'ютерних системах та мережах. Пропонується комбінований підхід до класифікації загроз, який доповнює попередні дослідження. Основна відмінність полягає у впровадженні ієрархічної структури з деревоподібною організацією категорій, що дозволяє детальніше описати складні загрози. У межах цієї таксономії окремим важливим об’єктом вводиться поняття «етап атаки», що дозволяє описувати багаторівневі атаки, які на сьогодні є дуже поширеними.

Багатоетапні атаки складаються з кількох етапів, кожен із яких може включати кілька дій, а дії – серії подій. Наприклад, атака через уразливість pro-ftpd може бути частиною одного з етапів і складатися з чотирьох окремих подій, які можуть відбуватися в різних комбінаціях. Крім того, кожен елемент вищого рівня (наприклад, етап або дія) також має власні атрибути та може розкриватися за допомогою дерева підкатегорій.

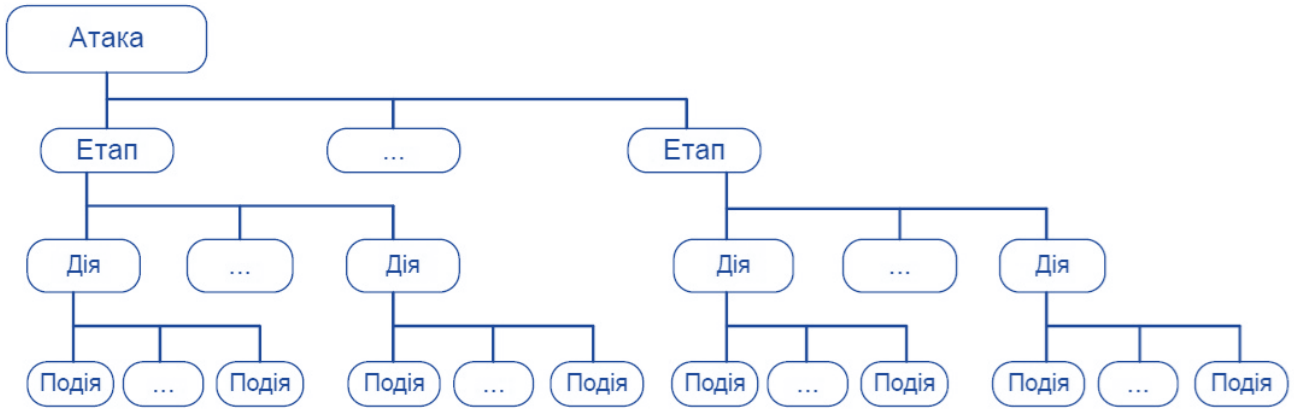


Рисунок 1.4. Ієрархічна структура атаки на інформаційну систему

Загальна схема атаки наведена на рис. 1.4. Атака є найвищим рівнем у цій структурі. Вона має атрибути, такі як глобальна мета/результат, характеристики атаки, об'єкт атаки та атакуючий. Кожен із цих атрибутів має власну структуру і розширюється на підкатегорії, що забезпечує детальне описання. Важливо зазначити, що мета атаки поділяється на дві складові: інформаційну та соціально

значущу. Інформаційна частина відображає наслідки атаки на рівні інформаційної безпеки, такі як порушення конфіденційності (для збору інформації або розголошення), недоступність інформаційних ресурсів (для блокування захисту або порушення роботи системи) або порушення цілісності інформації (втручання для отримання контролю). Соціально значуща частина описує ширші наслідки атаки, які виходять за межі інформаційної сфери.

Прикладом таких наслідків може бути захоплення комп'ютерів інформаційної мережі атомної електростанції з метою виведення реактора з ладу і створення техногенної катастрофи. У цьому випадку інформаційна мета полягає в захопленні контролю над системою, а соціальна – у спричиненні надзвичайної ситуації та потенційної загрози життю людей.

Іншим ключовим елементом атаки є об'єкт, на який спрямовані дії атакуючого, оскільки атаки на об'єкти різних типів мають індивідуальні характеристики. Серед основних властивостей об'єкта виділяються такі: тип атакованої системи, її фізичний компонент (обладнання, що забезпечує функціонування інформаційно-обчислювального середовища), засоби безпеки, що використовуються в системі, рівень її захищеності (жорсткість правил безпеки) та зовнішні комунікаційні канали системи.

Ще одним значущим параметром є атакуючий. Його основні властивості включають положення щодо атакованої системи, початкові привілеї і права доступу. Якщо в атаці бере участь декілька зловмисників, утворюється багатоагентна система, де важливими є кількість атакуючих і наявність між ними координації.

Найбільшу увагу слід приділити положенню атакуючого щодо об'єкта атаки. Атакуючий може перебувати безпосередньо на тому ж комп'ютері, на який спрямована атака. Такий сценарій називається локальною атакою. Наприклад, підвищення привілеїв через переповнення буфера в привілейованій програмі дозволяє отримати доступ до конфіденційних даних. Якщо атакуючий знаходиться в тій же мережевій сегменті, але на іншому комп'ютері, це можна вважати внутришньосегментною атакою.

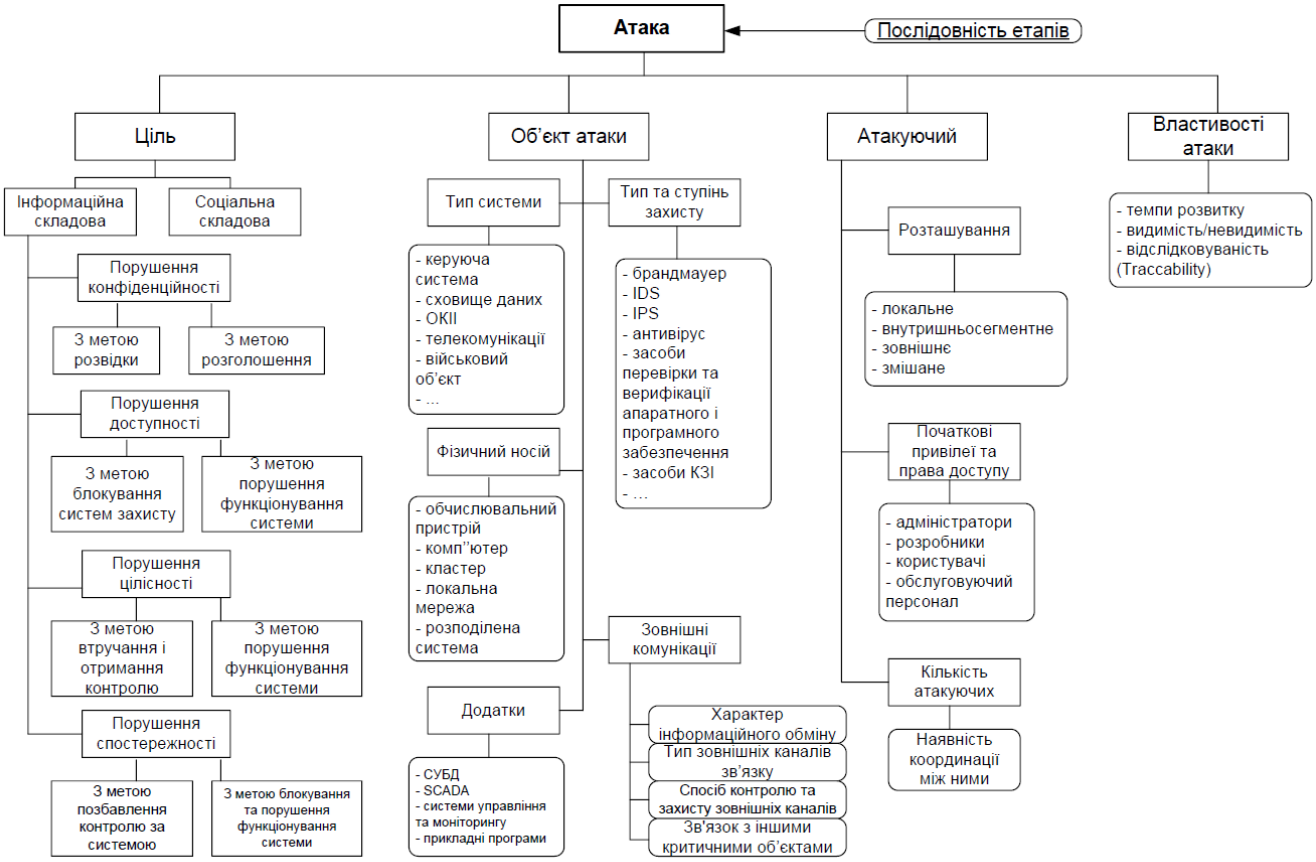


Рисунок 1.5. Функціональна схема атаки на інформаційну систему

На рис. 1.5 наведено функціональну схему кібератаки, послідовність і характеристики кібератак. Атакуючий може скористатися уразливостями мережевих сервісів, захищених фаєрволом від зовнішніх атак. Зовнішня атака, навпаки, здійснюється з віддаленого розташування через Інтернет. Існує також комбінований тип атак, за якого група атакуючих діє узгоджено. Наприклад, один з них, перебуваючи в мережевому сегменті, отримує доступ до інформації та передає її іншим за допомогою прихованих каналів зв'язку. Така атака, здійснювана з різних точок, називається розподіленою, прикладом чого може бути DDoS-атака.

Останній атрибут атаки, представлений на схемі, – це характеристики атаки. Деякі атаки можуть тривати кілька місяців для зменшення ймовірності виявлення, інші ж тривають лічені секунди, щоб уникнути реакції адміністратора. Темп атаки є критичним для її класифікації. Також важливими є видимість та можливість відстеження джерела атаки. Видимість визначає, наскільки атака залишається непомітною під час виконання, а відстежуваність визначає, наскільки легко

виявити джерело атаки під час розслідування. Ці два параметри тісно пов'язані й залежать від цілей зловмисника. Наприклад, якщо мета – непомітно проникнути в систему для викрадення інформації, зловмисник може вибрати сценарій з низькою видимістю, але потенційною відстежуваністю, щоб мінімізувати сліди після атаки.

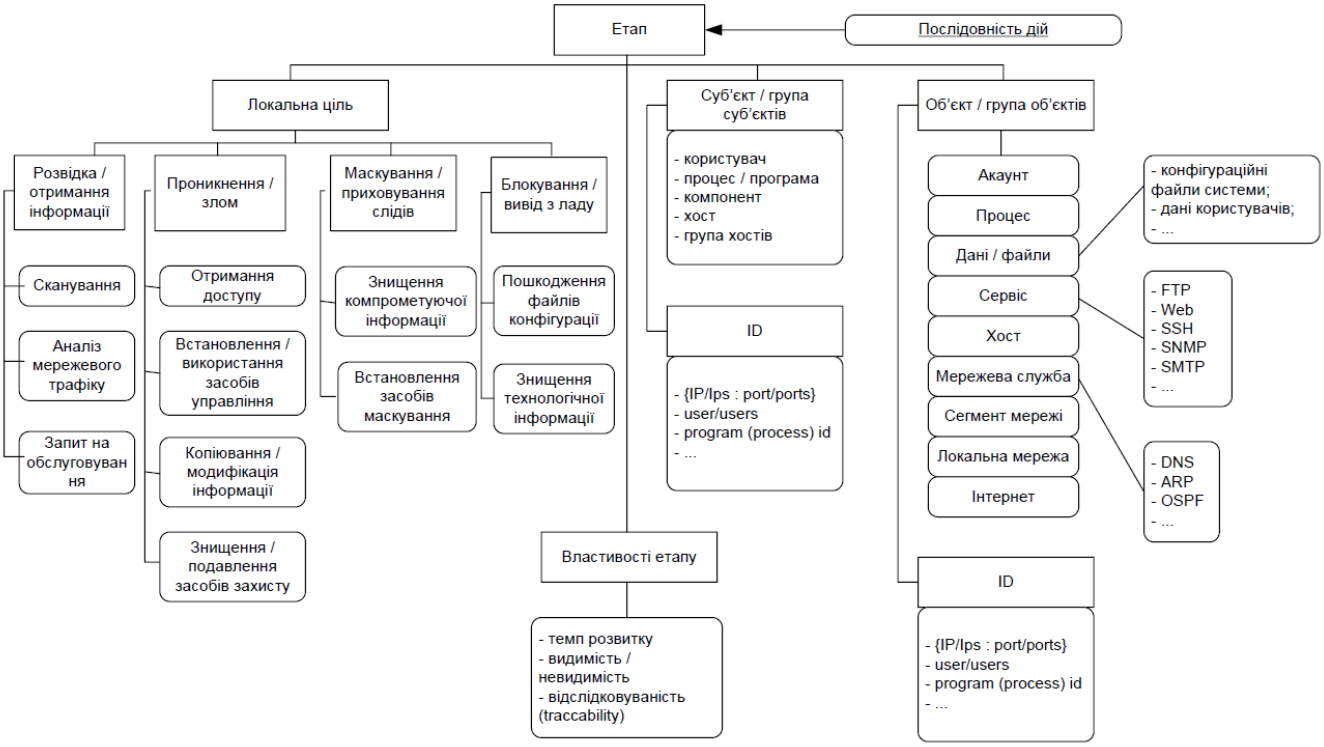


Рисунок 1.6. Функціональна схема етапу атаки на інформаційну систему

Атака розбивається на кілька стадій, кожна з яких має власні характеристики. Етап (стадія) являє собою відокремлену частину атаки і виконує певну локальну задачу (рис.1.6). Прикладом може бути стадія розвідки – наприклад, сканування внутрішньої мережі організації, на яку здійснюється напад. Головна мета такої стадії – непомітно вивчити топологію та архітектуру мережевого сегмента для подальшого пошуку вразливостей системи оборони та забезпечення можливості наступного вторгнення. Для досягнення цієї мети існує широкий спектр методів, серед яких чимало складних та хитромудрих рішень.

Кожна стадія атаки складається з окремих операцій. Операція є своєрідною елементарною дією в межах атаки (наприклад, перевірка відкритих портів або експлуатація відомих програмних недоліків). Дія також має певні характеристики, серед яких: тип операції, виконавець, ціль, наслідки та результат (рис.1.7).

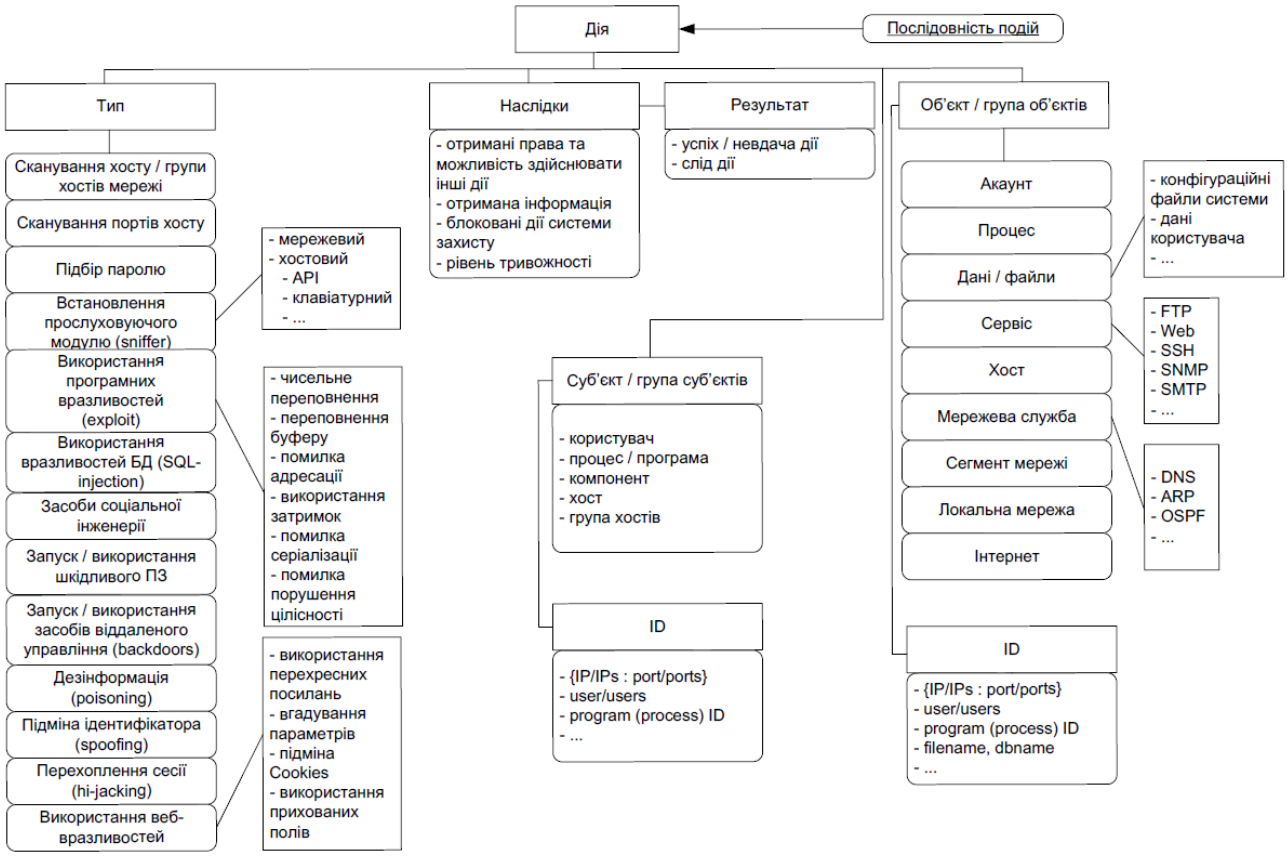


Рисунок 1.7. Функціональна схема дії при атаці на інформаційну систему

Операція є найменшою змістовною одиницею в ході атаки. Характеристика «тип операції» детально описує те, що відбувається на конкретній стадії. Цей параметр є надзвичайно інформативним, оскільки перелік можливих операцій часто перегукується зі списком типових атак. Тому цей перелік не є вичерпним і може вимагати доповнень залежно від конкретної області застосування. Об'єкт операції – це те, на що спрямована дія (програма, комп'ютер чи мережа), тоді як суб'єкт – це виконавець цієї операції. Наприклад, якщо зловмиснику вдалося взяти під контроль один із вузлів мережі (наприклад, комп'ютер А), і він використовує його для сканування іншого вузла (назвемо його комп'ютером Б), то суб'єктом дії буде вузол А, а об'єктом – вузол Б. Наслідки операції визначають, які привілеї або доступ отримав атакуючий, а також рівень загрози, що викликає ця дія. Цей рівень може бути суб'єктивним і залежить від різних факторів, тому оцінюється за допомогою деяких апріорних мірок.

З погляду системи, дія не завжди є елементарною. Наприклад, перевірка відкритих портів складається з цілого ланцюжка послідовних операцій, які

можуть варіюватися залежно від ситуації. Тому для більш детального аналізу атаки вводиться додатковий рівень – рівень подій (рис.1.8). Подія є найменшим кроком, який можна виділити на заданому рівні деталізації. Кожна подія має такі характеристики: тип, результат, час виконання, суб'єкт та об'єкт.

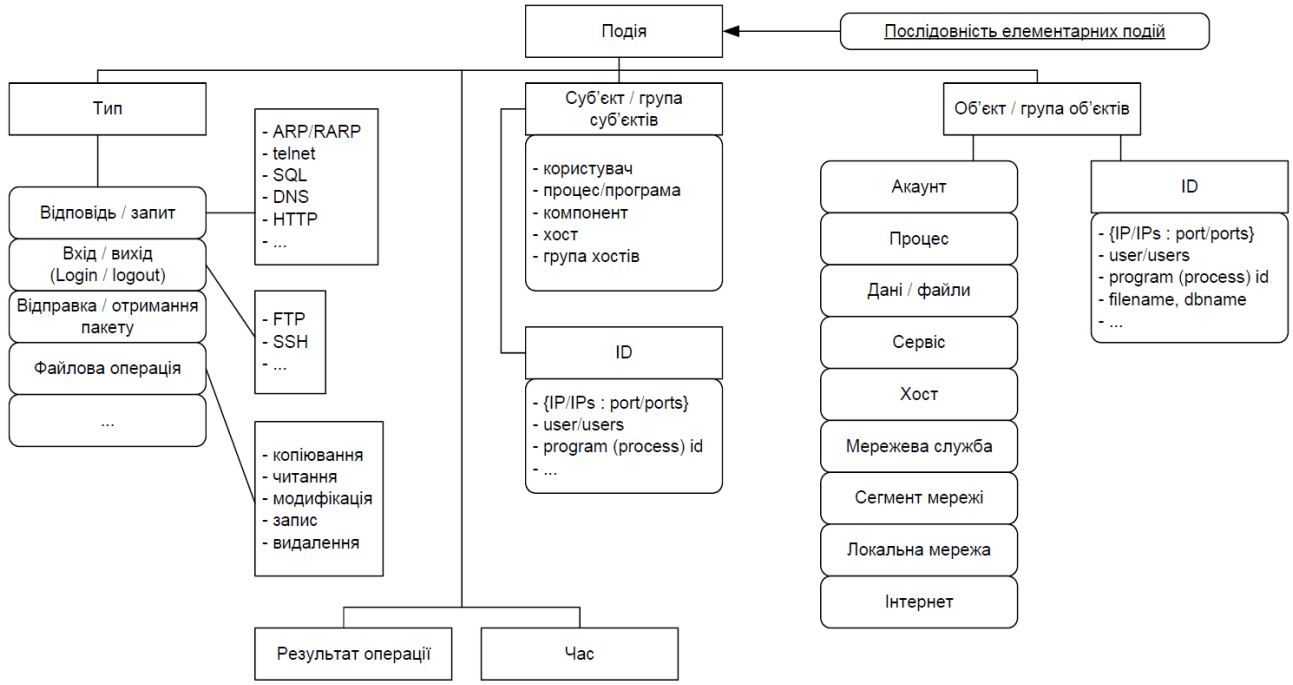


Рисунок 1.8. Функціональна схема події при атаці на інформаційну систему

У цьому підрозділі було розглянуто етапи, дії та події, що складають основу структуризації атаки на інформаційні системи. Запропоновано підхід, який дозволяє описати атаки на комп'ютерні системи шляхом розподілу їх на складові частини – етапи, дії та події, кожна з яких виконує свою конкретну роль. Це дозволяє глибше розуміти послідовність кроків атакуючого, що є важливим для розробки ефективних методів захисту. Такий підхід до таксономії загроз в інформаційній безпеці дозволяє систематизувати процеси, що відбуваються під час атак, ідентифікувати ключові фактори ризику та потенційні вразливості. Кожен етап атаки має свої цілі, які можуть бути досягнуті через виконання окремих дій та подій. Деталізований підхід до аналізу дозволяє покращити методи виявлення та реагування на загрози в інформаційних системах і мережах.

Загалом, розробка таксономії загроз допомагає створювати більш структуровані моделі захисту. Це є основою для розробки гнучких та адаптивних систем інформаційної безпеки, здатних ефективно протистояти сучасним атакам.

1.2.2 Розробка матриці залежності об’єктів захисту від типу загроз

Матриця (табл.1.4) відображає залежність інформаційних об'єктів захисту від конкретних загроз, що можуть виникати у процесі їх функціонування. Вона включає загрози для мережевих систем, засобів захисту, передаваних даних та інших ключових елементів інформаційної інфраструктури. Представлена в таблиці інформація є основою для подальшого вдосконалення захисних механізмів та забезпечення комплексної безпеки комп'ютерних систем і мереж. Етапи розробки матриці:

1. Ідентифікація інформаційних об'єктів захисту: Першим етапом є визначення ключових об'єктів, які потребують захисту. Це можуть бути апаратні компоненти (сервери, мережеві пристрої), програмне забезпечення (системи управління базами даних, операційні системи), а також мережеві та інформаційні ресурси (дані, обмін інформацією між системами);

2. Аналіз типів загроз: Після ідентифікації об'єктів слід визначити можливі загрози для кожного з них. Це можуть бути атаки на цілісність, доступність або конфіденційність даних. Серед можливих загроз можна виділити зловмисне програмне забезпечення, вторгнення з мережі, експлуатацію вразливостей програмного забезпечення або фізичні атаки на обладнання;

3. Структуризація загроз і об’єктів: Далі відбувається структуризація загроз, які впливають на конкретні об’єкти захисту. На цьому етапі будується зв'язок між типами загроз і об’єктами, які вони можуть вразити. Це дозволяє створити відповідні залежності та виділити найкритичніші загрози для кожного об’єкта;

4. Побудова матриці: Матриця створюється на основі виявлених залежностей. Вона є двовимірною таблицею, де рядки відображають об’єкти захисту, а стовпці – типи загроз. На перетині рядків і стовпців фіксуються загрози, які можуть вплинути на відповідний об’єкт. Така структура дозволяє легко візуалізувати загрози для кожного об’єкта та аналізувати їхній вплив;

5. Оцінка критичності загроз: Визначається, наскільки серйозно такий тип загрози може вплинути на інформаційний об'єкт, що дозволяє пріоритезувати заходи для протидії загрозам.

Таблиця 1.4. Матриця загроз для програмних та апаратних засобів КСМ

Об'єкти / загрози	*Кабельна система*	*Мережеве обладнання*	*Засоби мережевого захисту*	*Технологічна інф. захисту активного мереж. обладнання*	*Технологічна інформація захисту хостів*	*Дані, що передаються мережею*	*Програмне забезпечення*	*Файли*	*Записи баз даних*	*Обчислювальні ресурси*
Відсутність фізичного з'єднання	•	•								
Помилки та непрацездатність АМО		•	•							
Розголошення даних про мережу				•	•					
Перехоплення (сніффінг) пакетів				•	•	•				
Підміна отримувача (спуфінг пакетів)				•	•					
Відмова в обслуговуванні (DoS)				•	•		•			
Дзеркалювання трафіку					•	•				
Непрацездатність мережевих застосувань							•	•	•	
Бекдор		•	•	•			•	•		•
Віддалене захоплення (боти, ботнети)				•	•		•			
Сканування системи		•	•	•						
Фітинг, маскарад			•	•		•	•	•	•	•
Соціальна інженерія	•	•	•	•	•	•	•	•	•	•
Цільова кібератака (APT)		•	•	•	•	•				
Помилка, збій та відмова прикладного ПЗ							•	•	•	•
Виконання недокументованих функцій					•			•	•	
Розповсюдження вірусів та хробаків					•		•	•	•	•
Несумісність версій ПЗ							•			
Перехоплення інформації					•					
Підміна або дезорганізація							•			
Злам					•		•			
Використання вразливостей (експлоіт)					•		•	•	•	•
Кейлогер					•			•	•	
Атака під час реєстрації					•		•	•	•	
Захоплення облікового запису (АТО)					•		•	•	•	
Помилка системного ПЗ							•	•		•
Перехоплення технологічної інформації					•					
Пошкодження файлів ОС					•		•			
Збирання «сміття»					•			•		
Втручання в роботу ОС з мережі					•		•	•		
Руткіт (rootkit)					•		•	•	•	•
Атака нульового дня							•	•		•

1.2.3 Розробка моделі бази даних загроз інформаційним об’єктам

Модель бази даних загроз об’єктам інформаційної інфраструктури, створена у контексті впровадження концепції розумних мереж, призначена для використання у системах автоматизованого виявлення несанкціонованого впливу на операційні режими об'єктів інформаційної інфраструктури. База даних має ієрархічну структуру та дозволяє зберігати дані про оперативні параметри роботи системи та інформацію, що надходить від систем управління SCADA та EMS у реальному часі.

Метою розробки моделі бази даних є забезпечення ефективного збору, зберігання і обробки даних для виявлення загроз у режимі реального часу. На основі загальних принципів побудови баз даних, БД підтримує функціональні можливості, що забезпечують доступ до даних для авторизованих користувачів, включаючи адміністратора, програмістів та інших спеціалістів.

Функціональні режими бази даних:

1. Доступ до даних. Користувачі отримують можливість додавати, змінювати, видаляти та витягувати інформацію з бази даних;

2. Опис даних. Управління даними бази здійснюється через системний каталог, в якому зберігається:

- структура даних;
- зв’язки між даними;
- правила цілісності даних;
- реєстраційні дані користувачів;
- інша службова інформація.

Метадані допомагають структурувати інформацію для додатків, спрощують доступ до даних та забезпечують заходи безпеки;

3. Управління паралельністю. Система підтримує багатокористувацький доступ до інформації, гарантуючи коректне оновлення даних навіть при паралельному виконанні запитів;

4. Обробка транзакцій. Операції з даними виконуються в межах транзакцій, що гарантує цілісність даних у разі будь-яких збоїв під час обробки. Транзакція

повинна бути або виконана повністю, або скасована (відкат транзакції);

5. Забезпечення цілісності даних. Система стежить за коректністю та узгодженістю даних у відповідності до правил підтримки цілісності:

- цілісність доменів;
- цілісність відносин;
- зв'язки між таблицями;

6. Відновлення даних. У разі збоїв система має можливість відновлювати дані через механізми резервного копіювання;

7. Обмін даними. База даних підтримує сучасні технології обміну даними, дозволяючи віддаленим клієнтським комп’ютерам отримувати доступ до бази;

8. Контроль доступу. Користувачі можуть отримувати доступ до інформації лише згідно з наданими правами.

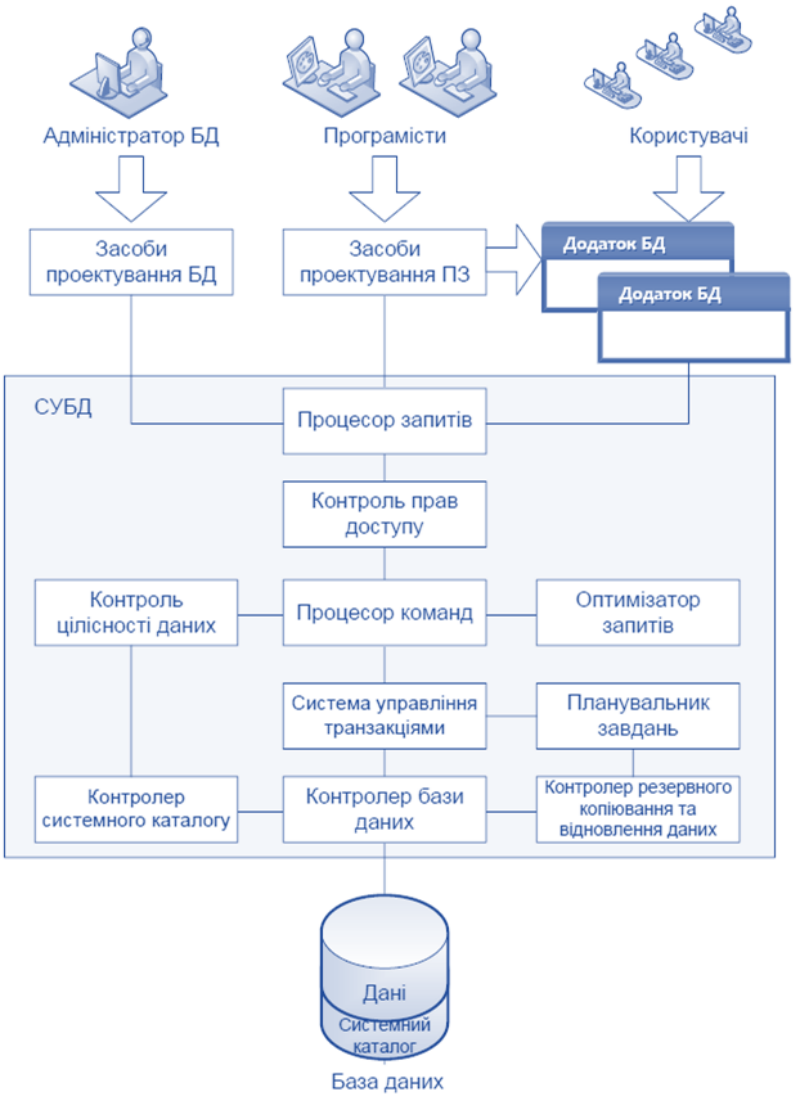


Рисунок 1.9. Модель бази даних з розподілом ролей користувачів (СУБД)

Архітектура бази даних: Для забезпечення всіх вищенаведених можливостей, модель бази даних побудована на основі клієнт-серверної архітектури (рис.1.9). Це означає, що сервер бази даних розташований на окремому апаратному середовищі, на якому встановлено СУБД, а користувацькі запити до бази даних обробляються через мережевий доступ.

Клієнт-серверна архітектура (рис.1.10) має такі переваги:

1. Висока доступність. Клієнтські пристрої можуть працювати під різними операційними системами, але підключатися до одного серверу.

2. Паралельність обробки. Сервер забезпечує одночасну обробку запитів від багатьох користувачів.

3. Централізація управління. Правила щодо підтримки цілісності та безпеки даних реалізовані на рівні сервера, що полегшує адміністрування.

4. Гнучкість. Клієнтські пристрої можуть працювати з різним програмним забезпеченням, зберігаючи доступ до сервера.

5. Єдина мова запитів. Мова SQL дозволяє легко взаємодіяти з базою даних через різні інтерфейси.

Рисунок 1.10. Клієнт-серверна архітектура бази даних

Адміністративний персонал і користувачі бази даних (рис.1.11): Модель бази даних передбачає декілька рівнів користувачів, які взаємодіють із системою:

1. Адміністратор даних (Data Administrator, DA) відповідає за управління даними, розробку стандартів, планування та впровадження бази даних, а також

визначає політику інформаційної безпеки.

2. Адміністратор бази даних (Database Administrator, DBA) керує всіма аспектами фізичного проектування, забезпечення безпеки та цілісності даних, а також контролює працездатність системи.

3. Розробники бази даних займаються проектуванням і реалізацією структури бази відповідно до концептуальних і логічних моделей.

4. Прикладні програмісти розробляють клієнтські додатки та інтерфейси для доступу до бази даних, тестують та впроваджують їх.

5. Користувачі є кінцевими користувачами, які взаємодіють із базою даних у своїй професійній діяльності, використовуючи інформацію для вирішення повсякденних завдань.

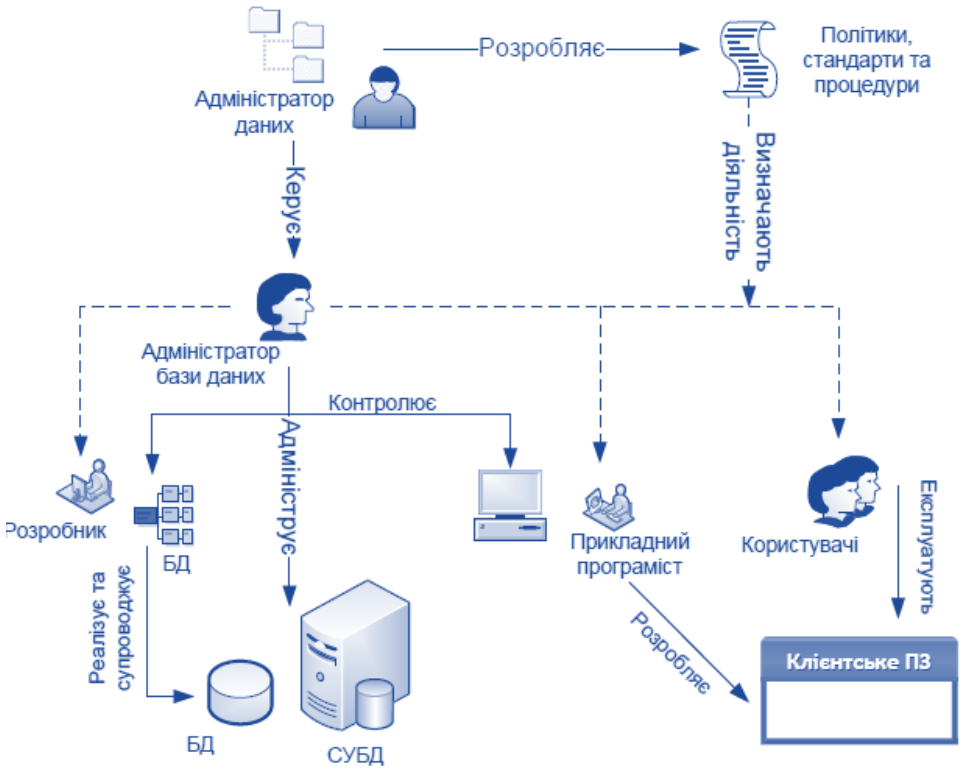


Рисунок 1.11. Організація процесів адміністрування та розробки баз даних

Модель бази даних передбачає комплексну архітектуру з урахуванням сучасних вимог до інформаційної безпеки, гнучкості та масштабованості, що дозволяє ефективно обробляти дані, забезпечуючи їх захист та цілісність.

Нижче наведено структуру бази даних загроз для об’єктів інформаційної інфраструктури, яка організована у вигляді таблиць з ключовими параметрами, характеристиками та захисними заходами.

Таблиця 1.5. Кіберзагрози

ID	*Тип загрози*	*Опис загрози*
1	Підробка (Spoofing)	Неправомірне використання IP-адреси для підробки особистості
2	Прослуховування (Sniffing)	Нелегальний перехоплення мережевих пакетів з метою збору даних
3	Відмова в обслуговуванні (DoS)	Атаки на сервер, що призводять до його перевантаження або недоступності

Таблиця 1.6. Специфікації

ID	*Загроза*	*Специфікація*
1	Підробка (Spoofing)	Кількість виявлених IP-адрес у спам-базах
2	Підробка (Spoofing)	Кількість спам-слів у темі повідомлення
3	Прослуховування (Sniffing)	Кількість пакетів з однаковими IP-адресами відправника та отримувача
4	DoS-атака	Кількість одночасних з'єднань до сервера
5	DoS-атака	Затримка між запитами від одного користувача

Таблиця 1.7. Властивості

ID	*Властивість*	*Опис*
1	Цілісність	Забезпечення повноти та правильності даних
2	Конфіденційність	Обмежений доступ до інформації
3	Доступність	Гарантія доступу до сервісів у випадку загроз
4	Спостережність	Можливість моніторингу дій у системі.

Таблиця 1.8. Захисні заходи

ID	*Загроза*	*Захисний захід*
1	Підробка (Spoofing)	Налаштування управління доступом.
2	Підробка (Spoofing)	Використання двофакторної автентифікації.
3	Прослуховування (Sniffing)	Впровадження криптографічного захисту даних.
4	Прослуховування (Sniffing)	Установлення систем для розпізнавання сниферів.
5	DoS-атака	Блокування шкідливих IP-адрес.
6	DoS-атака	Забезпечення високої пропускної здатності мережі.

Дана структура бази даних розроблена для обліку кіберзагроз, що впливають на об'єкти критичної інформаційної інфраструктури. База даних містить ключові загрози, специфікації, властивості та заходи захисту, що дозволяє здійснювати моніторинг і контроль за станом безпеки інформаційних систем.

Структурні елементи таблиць бази даних:

1. Кіберзагрози – перелік найбільш поширених типів атак на інформаційні системи;
2. Специфікації – метрики або параметри, що відстежують загрози та їх вплив на систему;
3. Властивості – важливі характеристики системи, такі як цілісність, конфіденційність і доступність;
4. Захисні заходи – рекомендовані дії для захисту від конкретних кіберзагроз.

Ця структура дозволяє легко інтегрувати нові типи загроз і захисні заходи, а також здійснювати гнучке адміністрування безпеки. На рис. 1.12 показана структура бази даних загроз об'єктів інформаційної інфраструктури. Фізичні параметри логічних атрибутів відображені у табл. 1.9.

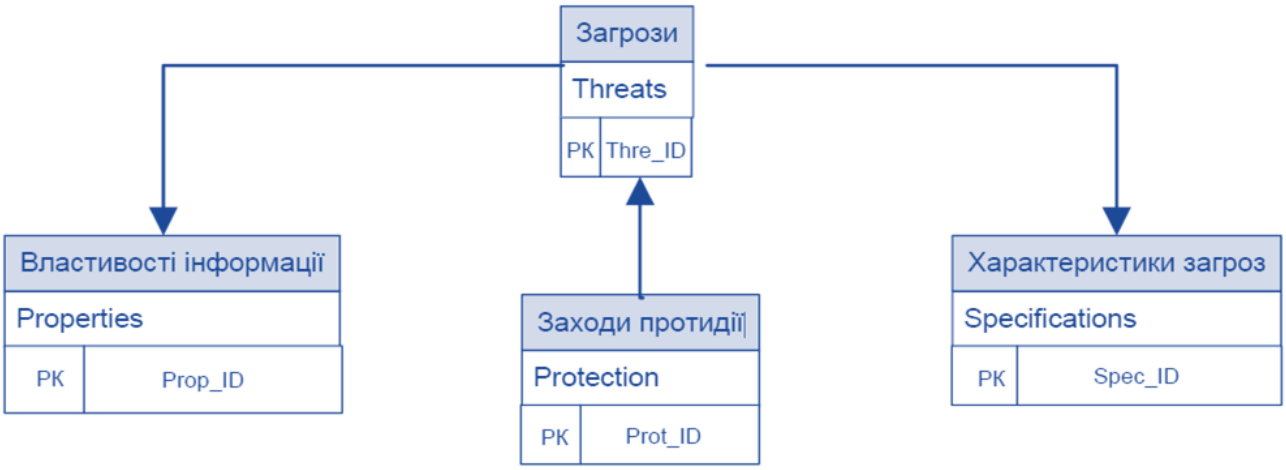


Рисунок 1.12. Модель бази даних загроз інформаційним об'єктам

Таблиця 1.9. Фізичні параметри логічних атрибутів загроз

№	*Назва атрибуту*	*Фізичний формат*	*Опис*
1	Threats	TXT	Загрози
2	Properties	TXT	Характеристики інформації
3	Protection	TXT	Заходи захисту
4	Specifications	TXT	Тип документації
5	Thre_ID	BINARY	Унікальний ідентифікатор загрози
6	Prop_ID	BINARY	Унікальний ідентифікатор властивості
7	Prot_ID	BINARY	Ідентифікатор заходу захисту
8	Spec_ID	BINARY	Ідентифікатор характеристики загрози

1.3 Розробка системи захисту інформації комп’ютерних систем і мереж

1.3.1 Реалізація методу розпізнавання загроз інформаційній безпеці

На основі здійсненого у п.1.1 аналізу методів та засобів оцінки рівня стійкості комп’ютерних систем і мереж та виконаної у п.1.2. розробки моделі загроз інформаційним об’єктам, а також досліджень науково-технічних матеріалів з впровадження захисних систем були ідентифіковані загрози інформаційній безпеці комп'ютерних систем і мереж. Використаний підхід орієнтований на аналіз трафіку, що потрапляє до внутрішніх інформаційних систем з Інтернету. Він інтегрований в багатошарову систему для моніторингу, оцінки та обробки вхідного трафіку для виявлення підозрілих активностей. Методологія базується на трьох ключових етапах перевірки:

1) Автоматизоване перевірення мережевого трафіку з ідентифікацією протоколів;

2) Виявлення аномальних подій, як-от DDoS-атаки, підміна IP-адрес та уразливості мережевих протоколів і додатків;

3) Виявлення спроб несанкціонованого доступу, викрадення привілеїв та впровадження шкідливих програм, таких як трояни, а також аналіз прихованих атак.

Існуючі методи моніторингу телекомунікаційних мереж, засновані на сигнатурному аналізі за допомогою антивірусного ПЗ, забезпечують перевірку файлів та мережевих пакетів на наявність вірусів зі своїх баз даних. Якщо виявляється збіг коду з відомим зразком, програмне забезпечення виконує один із трьох заходів: видалення зараженого файлу, його ізоляцію або спробу відновлення. Цей підхід є надійним завдяки тривалому часу його застосування, що сприяло вдосконаленню механізмів виявлення шкідливого ПЗ. Водночас, через постійне зростання кількості нових вірусів, бази даних збільшуються, що негативно впливає на продуктивність системи. Ще однією слабкістю цього підходу є залежність від оновлення баз даних, що уповільнює реакцію на нові загрози.

Іншим методом виявлення шкідливих програм є евристичний аналіз, що полягає у спостереженні за поведінкою додатків. При виявленні відхилень від нормальної поведінки система повідомляє про потенційну небезпеку. Цей підхід перспективний, оскільки його можливості зростатимуть із розвитком штучного інтелекту. Однак він також має недоліки, такі як помилкові спрацьовування та високі вимоги до ресурсів.

Також широко застосовується метод захисту через міжмережеві екрани, що контролюють трафік між локальною мережею і зовнішніми ресурсами, використовуючи списки дозволених та заборонених адрес. Цей підхід дозволяє уникнути небезпечних з'єднань, але вимагає високої кваліфікації персоналу для налаштування ефективного функціонування системи.

1.3.2 Розробка структурної моделі системи виявлення підозрілих впливів на комп'ютерні системи і мережі

Як було зазначено вще, використовуваний метод виявлення загроз інформаційної безпеки комп'ютерних систем і мереж реалізує трирівневу модель захисту, яка охоплює аналіз мережевого трафіку, захист від загроз на рівні додатків і системного програмного забезпечення, а також від шкідливих програм. На базі цього підходу була розроблена багаторівнева система виявлення підозрілих впливів на комп'ютерні системи і мережі. Її структурна схема зображена на рис. 1.13.

На першому рівні ця система виконує функції захисту від зловмисних спроб сканування портів. Оскільки хакери часто намагаються сканувати TCP і UDP порти для виявлення активних точок підключення, можливість виявити факт сканування допомагає заздалегідь виявити потенційну загрозу і визначити місце можливого проникнення.

Основою для реалізації цього рівня є сучасні методи виявлення вторгнень на мережевому рівні (IDS), які дозволяють фіксувати такі дії. Крім того, на цьому етапі реалізовано захист від спроб виявлення протоколів взаємодії між інформаційно-телекомунікаційною системою (ІТС) і зовнішньою мережею.

Другий рівень системи призначений для аналізу вхідного трафіку з метою

виявлення потенційних атак типу «відмова в обслуговуванні» (DDoS). Тут аналізується декілька типів атак, зокрема:

- Атаки на мережеві пристрої, що можуть використовувати вразливості апаратної або програмної реалізації пристроїв для вичерпання їх ресурсів, як це відбувається при переповненні буфера під час автентифікації;
- Атаки на операційні системи, наприклад, через використання уразливостей TCP/IP стека, як у випадку атаки Ping of Death;
- Атаки на додатки, які використовують помилки мережевих програм, щоб виснажити ресурси цільового хоста, або здійснюють атаки типу finger bomb.
- Атаки на рівні каналу, що спрямовані на заповнення смуги пропускання, як у випадку з атакою ping flood;
- Атаки на протоколи, де зловмисники можуть підміняти IP-адресу відправника або маніпулювати кешем DNS.

Для захисту від таких загроз на другому рівні система виявлення підозрілих впливів використовує технології, які аналізують трафік на кордоні мережі, блокуючи потенційно небезпечні запити і сигналізуючи адміністратору про загрозу. Це дозволяє ефективно захищати інформаційні системи від DDoS-атак у межах наявних ресурсів смуги пропускання.

Третій рівень відповідає за моніторинг і виявлення підозрілих дій, що стосуються системних параметрів і конфігурацій додатків. На цьому рівні система відстежує такі типи загроз:

- Атаки на паролі;
- Захоплення привілеїв;
- «Троянські коні»;
- Аудит мережевої активності;
- Скриті дії.

Цей рівень функціонує за принципом чорного списку: виявлення хоча б однієї ознаки підозрілої активності призводить до блокування трафіку від джерела загрози і сигналізації адміністратору.

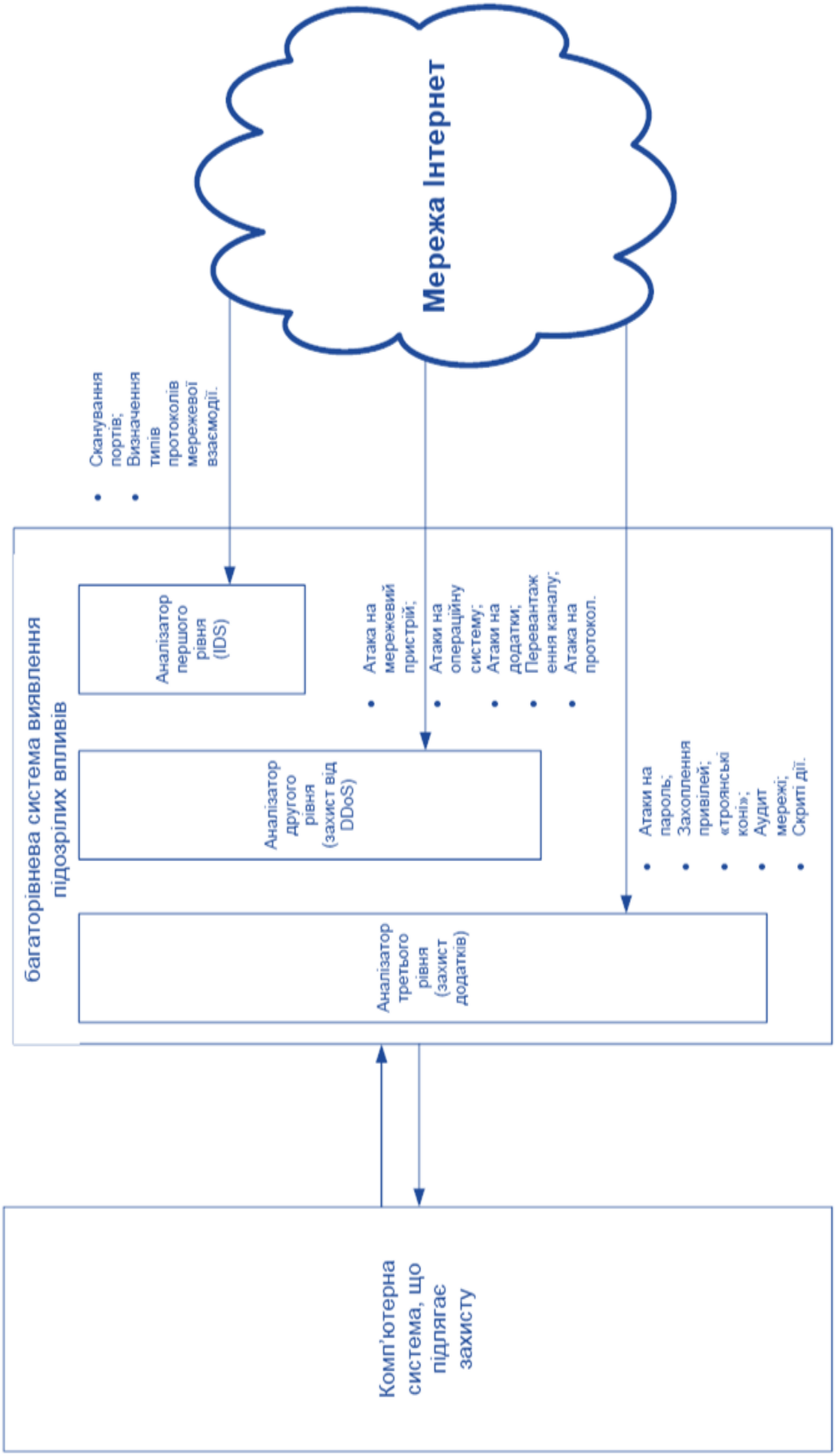


Рисунок 1.13. Структурна модель багаторівневої системи виявлення впливів

Запропонована на рис.1.13 схема багаторівневої системи виявлення підозрілих впливів дозволяє забезпечити інтелектуальний аналіз трафіку в реальному часі. Такий підхід дає змогу охопити широкий спектр характеристик мережі, захищаючи її від різних загроз – від спроб вторгнення на рівні портів до атак на операційні системи. Механізми захисту, розподілені на трьох рівнях, значно підвищують стійкість інформаційно-телекомунікаційної системи до зовнішніх загроз, збільшуючи витрати зловмисників на можливе проникнення, що в багатьох випадках робить такі атаки економічно недоцільними.

1.3.3 Реалізація методики оцінювання стійкості комп’ютерних систем і мереж

Реалізація методики оцінювання стійкості комп'ютерних систем та мереж базується на необхідності забезпечення їх стабільного функціонування в умовах зростаючої кількості кібератак та впливів на об'єкти інфраструктури. Сучасні інформаційно-комунікаційні технології часто виявляються вразливими до різноманітних кіберзагроз, що підкреслює потребу в нових методах підтримки стійкості та забезпеченні безпеки.

Ключовим елементом управління стійкістю є обізнаність про поточний стан інформаційних систем, навколишнє середовище, в якому вони функціонують, та можливі загрози. Ефективність управління стійкістю об’єктів безпосередньо залежить від підсистеми підтримки рішень, що має забезпечувати керівника достовірною інформацією щодо стану об'єктів і пропонувати оптимальні інструменти для захисту. Методика оцінки стійкості комп'ютерних систем та мереж полягає у вивченні технічних систем з високою критичністю. Вона застосовується для підвищення ефективності управління інфраструктурою, а також для розробки нових заходів кіберзахисту. Глобалізація та широке використання Інтернету сприяли зростанню важливості стійкості IT-систем, які стають невід'ємною частиною функціонування критичних об'єктів.

Незважаючи на кількість досліджень у сфері кібербезпеки, все ще є потреба в розробці моделей, методів та засобів для адаптивного управління критичними системами в умовах кіберзагроз.

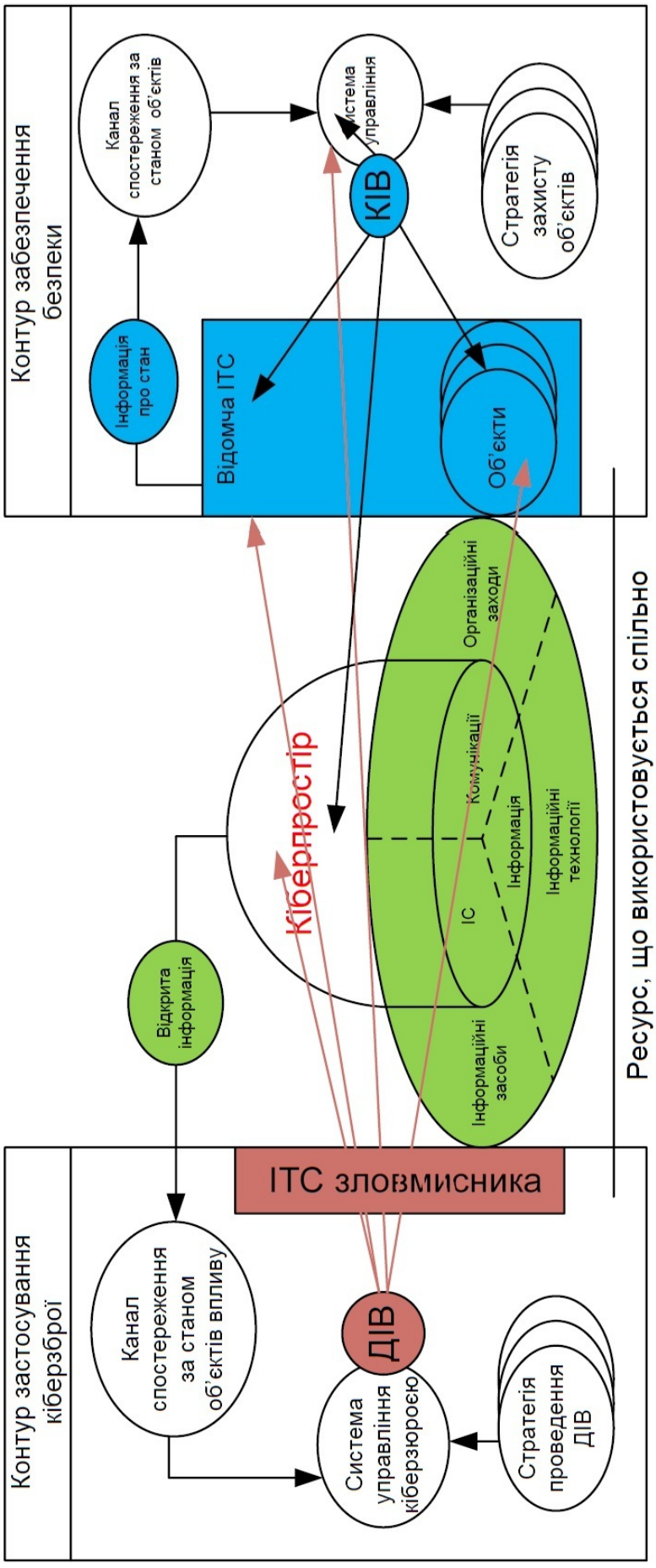


Рисунок 1.14. Контури забезпечення кібербезпеки та застосування кіберзброї

Це включає збір, аналіз та уніфікацію даних про стан об'єктів, а також розробку нових методик для оцінки їх стійкості.

Оцінювання стійкості комп'ютерних систем і мереж здійснюється через визначення їхньої здатності виконувати свої функції в умовах кібератак. Враховуються такі фактори, як адекватність управління, оперативність прийняття рішень, стійкість до впливу деструктивних чинників та прихованість процесу управління. Система кіберзахисту має бути здатна не тільки вчасно реагувати на загрози, але й компенсувати негативні наслідки атак.

Загальна стійкість об'єктів критичної інфраструктури залежить від їх кіберживучості (здатності підтримувати працездатність в умовах виходу з ладу окремих компонентів) та кібернадійності (ймовірності забезпечення виконання функцій при програмних та технічних збоях). Тому при розробці методик стійкості важливо враховувати ймовірності різних подій, що можуть спричинити збої в роботі системи, і передбачити можливість їх компенсації через відповідні механізми захисту (рис.1.14).

Таким чином, методика оцінки стійкості комп'ютерних систем і мереж дозволяє прогнозувати й аналізувати вплив кіберзагроз на функціонування систем, пропонуючи ефективні рішення для зменшення їхньої вразливості та забезпечення високого рівня кіберзахисту.

Попри суттєве спрощення та ідеалізацію, модель, представлена на рис. 1.14, дозволяє виділити ключові властивості, характерні для процесів управління в умовах кібервоєн (КВ): адекватність, оптимальність, оперативність, стійкість та скритність.

1. Адекватність: Ця властивість управління полягає у здатності системи перетворювати інформацію про стан об'єкта, отриману від підсистеми моніторингу, на керуючий інформаційний вплив (КІВ), що переводить об'єкт в стан, який відповідає поточній ситуації. Важливість адекватності залежить від достовірності отриманої інформації та правильності визначення цільової функції об'єкта управління;
2. Оптимальність: Оптимальне управління передбачає вибір таких керуючих

впливів, які мінімізують втрати системи (ресурси, час тощо) та забезпечують досягнення екстремального значення критерію, що характеризує якість управління;

3. Оперативність: Це здатність системи перетворювати інформацію у відповідності до часових обмежень та темпу зміни поточної ситуації. Оперативність поділяється на семантичне (вироблення рішень) та технічне (передача даних або виконання обчислень) перетворення;
4. Стійкість: Стійкість управління визначається здатністю системи виконувати свої функції в умовах впливу деструктивних факторів (технічні відмови, кіберзагрози), зберігаючи необхідний рівень показників ефективності управління;
5. Скритність: Ця властивість означає збереження в таємниці від протиборчої сторони процесу перетворення інформації, а також її змісту та належності до керованих об'єктів.

Об'єкти комп'ютерних систем і мереж (КСМ) за своєю структурною організацією можуть бути як одноланкові, так і багатоланкові. Одноланковий об'єкт КСМ є самостійнім елементрм, який має всю необхідну структуру для виконання своєї основної функції. Прикладом можуть бути окремі автоматизовані системи (АС). Багатоланковий об'єкт КСМ складається з декількох одноланкових об'єктів КСМ, об'єднаних у єдину систему для виконання спільної цільової функції.

За функціональною однорідністю багатоланкові об'єкти можуть бути однорідними і неоднорідними. Багатоланковий однорідний об'єкт КСМ складається з кількох одноланкових об'єктів, які виконують однакову цільову функцію. Наприклад, складна мережа передачі даних, яка об'єднує різнотипні системи передачі даних. Багатоланковий різнорідний об'єкт КСМ складається з одноланкових об'єктів, які виконують різні функції, наприклад, інформаційно-телекомунікаційна мережа або інформаційні системи. Зазвичай, об'єкти КСМ, що використовують інформаційно-телекомунікаційні мережі загального користування (ІТКМ ЗК), є багатоланковими. Склад окремих ланок залежить від

обраних маршрутів передачі інформації та відомчих інформаційно-телекомунікаційних систем.

Для оцінки стійкості пропонується використовувати узагальнений показник стійкості, який для одноланкового об'єкта КСМ виглядає так:

$$К^{уп}_{ОКСМ} = К^{жив}_{ОКСМ} * К^{зах}_{ОКСМ} * К^{над}_{ОКСМ} \quad (1.1)$$

де:

- $К^{уп}_{ОКСМ}$ – узагальнений показник стійкості;

- $К^{жив}_{ОКСМ}$ – живучість об'єкта КСМ, тобто здатність зберігати працездатність в умовах виходу з ладу технічних засобів внаслідок загроз;

- $К^{зах}_{ОКСМ} = (1 - Р_{ЗКА})*(1 - Р_{ЦКА})$ – захищеність об'єкта КСМ, яка оцінюється як ймовірність забезпечення виконання цільової функції в умовах загальних і цілеспрямованих загроз;

- $Р_{ЗКА}$ і $Р_{ЦКА}$ – ймовірності ураження технічних засобів загальними та цілеспрямованими загрозами відповідно;

- $К^{над}_{ОКСМ}$ – надійність об'єкта КСМ, яка визначається ймовірністю забезпечення виконання цільової функції в умовах виникнення різних подій (i = 1,…., N), зокрема програмних і технічних відмов засобів об'єкта КСМ внаслідок деструктивних інформаційних впливів, де

$$К^{над}_{ОКСМ} = \prod_{i=1}^{N} К_{ОКСМнад\,i}(1 - Р_i) \quad (1.2)$$

де $Р_i$ – ймовірність *i*-ї події (від i = 1 до N).

На етапі проєктування об'єктів КСМ висуваються суворі вимоги до технічної надійності, і передбачаються різноманітні спеціальні заходи для запобігання технічним і програмним відмовам інформаційних систем. Це включає такі заходи, як кластеризація серверів і резервування окремих компонентів. Відповідно, під час оцінки стійкості КСМ можна вважати ймовірність програмних та технічних відмов, за умови своєчасного і якісного технічного обслуговування та оновлення, незначною. Тобто, ймовірність технічного неспрацювання ($Р_{ТН}$) можна вважати рівною нулю ($Р_{ТН}=0$). У цьому випадку надійність одноланкового об'єкта КСМ буде розраховуватися як:

$$К^{0}_{ОКСМ} = К^{жив}_{ОКСМ} * К^{зах}_{ОКСМ} \quad (1.3)$$

Якщо розглядати виходи з ладу ланок КСМ в умовах кібервпливів як незалежні події, стійкість багатоланкового об’єкта КСМ ($К_{КСМстб}$) можна визначити за формулою:

$$К^{стб}_{ОКСМ}(N) = \prod_{i=1}^{N} К_{ОКСМ0\,i} \quad (1.4)$$

де: N – кількість різних шкідливих подій, викликаних кібервпливами;

$К_{ОКСМ0\,i}$ – стійкість кожного окремого і-го одноланкового об’єкта КСМ.

Надійність багатоланкового об'єкта КСМ визначається як ймовірність забезпечення виконання цільової функції об'єкта протягом заданого часового інтервалу в умовах виникнення програмних помилок і технічних збоїв одноланкових об'єктів, з яких складається багатоланковий об'єкт.

Таким чином, стійкість багатоланкового об'єкта КСМ має обчислюватися як спільна N-мірна функція розподілу ймовірності збереження працездатності всіх N ланок одночасно, що утворюють цей багатоланковий об'єкт КСМ:

$$К_{ОКСМсб}(К_{ОКСМсо1}, \dots, К_{ОКСМсоN}) =$$
$$P\{К_{ОКСМсо1} \geq К_{ОКСМсопотр1}, \dots, К_{ОКСМсоN} \geq К_{ОКСМоспотрN}\} \quad (1.5)$$

де:

- $К_{ОКСМсб}$(N) – стійкість багатоланкового об’єкта КСМ;
- $К_{ОКСМсо1}$ – стійкість першого одноланкового об’єкта КСМ;
- $К_{ОКСМсопотр}$ – необхідний рівень стійкості першого одноланкового об’єкта КСМ;
- $К_{ОКСМсоN}$ – стійкість N-го одноланкового об’єкта КСМ;
- $К_{ОКСМоспотр}$ – необхідний рівень стійкості N-го одноланкового об’єкта КСМ.

Основою для визначення стійкості багатоланкових об'єктів КСМ є розрахунок показників захищеності та живучості окремих ланок об'єкта. Тому необхідно розробити методику для обчислення цих показників, враховуючи, що живучість є визначальною характеристикою, що дозволяє оцінити здатність

об'єкта КІІ виконувати свою цільову функцію. Захищеність буде складовою частиною цієї функції.

Характеристики, які визначають живучість об'єкта КСМ в умовах деструкційних інформаційних впливів Ω, починають проявлятися тільки після впливу. Тому міра живучості має визначатися умовною ймовірністю збереження працездатності системи за умови локального пошкодження. Під показником живучості одноланкового об’єкта КСМ ($К_{ОКСМ\ ЖИВ}$) розуміється умовна ймовірність того, що кінцевий стан об’єкта КСМ залишиться в межах заданої області безпечних станів S^I у просторі безпечних станів S після проведення кібервпливу S0:

$$К_{ОКСМ\ ЖИВ} = P[(\|S - s_0\| < S^I) / \Omega] \qquad (1.6)$$

Враховуючи функціональну вразливість системи V_S, тобто ймовірність виходу кінцевого стану системи за межі безпечної області S_I, можна записати:

$$К_{ОКСМ\ ЖИВ} = 1 - V_S, \qquad (1.7)$$

або $К_{ОКСМ\ ЖИВ}(t) = 1 - VS(t)$ у конкретний момент часу.

При цьому мірою визначення живучості одноланкового об’єкта КСМ буде вираз:

$$К^{пот}_{ОКСМ\ ЖИВ}(t) \geq К^{тр}_{ОКСМ\ ЖИВ}(t), \qquad (1.8)$$

де $К^{пот}_{ОКСМ\ ЖИВ}(t)$ – поточний рівень живучості одноланкового об’єкта КСМ, а $К^{тр}_{ОКСМ\ ЖИВ}(t)$ – необхідний рівень живучості в умовах кібервпливу.

Також необхідно визначити критерій здатності об’єкта КСМ виконувати цільову функцію при деструктивних інформаційних впливах $W_б$:

$W_б = К^{пот}_{ОКСМ\ ЖИВ}(t) > H1$ – об′єкт КСМ повністю дієздатний,

$W_б = H2 \leq К^{пот}_{ОКСМ\ ЖИВ}(t) < H1$ – об′єкт КСМ загалом дієздатний,

$W_б = H3 \leq К^{пот}_{ОКСМ\ ЖИВ}(t) < H2$ – об′єкт КСМ обмежений,

$W_б = H4 \leq К^{пот}_{ОКСМ\ ЖИВ}(t) < H3$ – об′єкт КСМ недієздатний (підлягає відновл.)

$W_б = К^{пот}_{ОКСМ\ ЖИВ}(t) < H4$ – об′єкт КСМ недієздатний (не підлягає відновл.),

де:

- H_1 – система повністю справна та функціонує відповідно документації;

- H_2 – система в цілому справна та функціонує відповідно документації, можливі відхилення;

- H_3 – система вийшла з ладу, функціональні характеристики не відповідають документації;

- H_4 – система недієздатна, функціональні характеристики не відповідають документації.

Наведені нижче рівні живучості дозволяють визначити поточного показник живучості $К^{пот}_{ОКСМ\ ЖИВ}(t)$:

$$К_{ОКСМ\ ЖИВ}(t) = К^{пот}_{ОКСМ\ ЖИВ}(t) - К^{тр}_{ОКСМ\ ЖИВ}(t) > 0 - \text{оптимальний рівень}$$

$$К_{ОКСМ\ ЖИВ}(t) = К^{пот}_{ОКСМ\ ЖИВ}(t) - К^{тр}_{ОКСМ\ ЖИВ}(t) = 0 - \text{допустимий рівень}$$

$$К_{ОКСМ\ ЖИВ}(t) = К^{пот}_{ОКСМ\ ЖИВ}(t) - К^{тр}_{ОКСМ\ ЖИВ}(t) < 0 - \text{критичний рівень}$$

$$К_{ОКСМ\ ЖИВ}(t) = К^{пот}_{ОКСМ\ ЖИВ}(t) = 0 - \text{надкритичний рівень}$$

За отриманими у вищенаведених виразах результатами виконано візуалізацію (рис.1.15). Методологія оцінки стійкості включає такі кроки:

1. Оцінка живучості кожного об'єкта КСМ окремо.

а) Оцінка живучості одноланкових об'єктів КСМ. Рівень безпеки – ймовірність збереження функціональності і-го компонента в умовах кібератак. Оцінити коефіцієнт пов'язаності і-го елемента та його вклад у цільову функцію об'єкта КСМ.

б) Оцінка живучості багатоланкових об'єктів КСМ. Рівень безпеки – ймовірність збереження функціональності j-го одноланкового об'єкта КСМ в умовах здійснення кібератак. Оцінити коефіцієнт пов'язаності j-го одноланкового об'єкта КСМ та його вплив на цільову функцію багатоланкового об'єкта КСМ.

2. Оцінка живучості взаємодіючих об'єктів КСМ (групи об'єктів КСМ). Рівень захищеності – ймовірність збереження функціональності n-го

багатоланкового об'єкта КСМ в умовах проведення кібератак.

3. Оцінка живучості КСМ через сукупну стійкість її компонентів з урахуванням їх коефіцієнта взаємозв'язку. Оцінка загальної живучості КСМ, залежно від актуального стану системи та важливості виконуваних функцій.

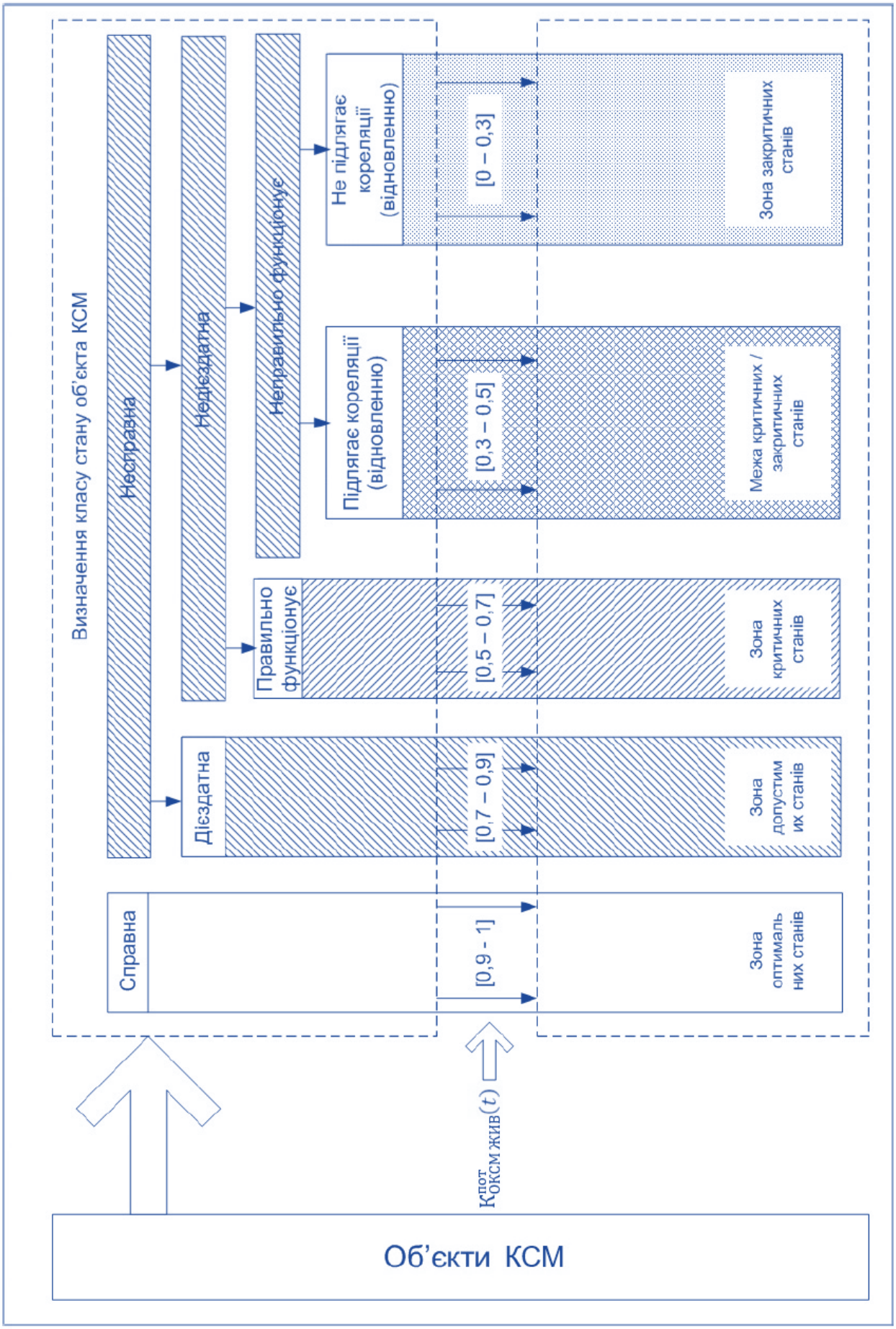


Рисунок 1.15. Класифікація стану об'єкта КСМ за рівнем живучості

Під час розробки методології оцінки стійкості об'єктів КСМ пропонується введення нової характеристики – стійкості. Необхідність введення цієї властивості зумовлена специфікою середовища, в якому функціонує мережева інфраструктура об'єктів КСМ (кіберпростір), і, як наслідок, виникненням нових вразливостей та загроз для об'єктів КСМ. Запропонована методика, шляхом декомпозиції КСМ на окремі об'єкти із врахуванням коефіцієнтів взаємозв'язку та ступеня важливості виконуваних у цей момент функцій, дозволяє провести оцінку стійкості КСМ відповідно до встановленого рівня. Отриманий результат, відповідно до розробленої схеми відповідності стану об'єкта КСМ рівню захищеності (рис. 1.15), дозволяє точно визначити стан безпеки КСМ в умовах кібератак.

1.4 Розробка програмної моделі оцінки рівня стійкості комп’ютерних систем і мереж

1.4.1 Розробка блок-схем алгоритмів системи захисту інформації комп’ютерних систем і мереж

На основі запропонованої у п.1.3 методики було розроблено блок-схему алгоритму, який став основою для програмного забезпечення, призначеного для оцінки рівня стійкості комп’ютерних систем і мереж. Блок-схема алгоритму, побудованого на основі методології оцінки стійкості КСМ наведений на рис. 1.16. У межах розробки цього алгоритму було створено прикладний програмний продукт, що реалізує методи, представлені в даній роботі.

Виявлення та нейтралізації кібератак на комп'ютерні системи та мережі (рис.1.17) починається з первинного аналізу мережевої активності. Це включає перевірку на наявність спроб сканування портів і ідентифікацію типів мережевих протоколів, що використовуються в системі. У випадку відсутності підозрілої активності цикл роботи системи завершується, і вона повертається до режиму моніторингу. Якщо виявлено сканування портів або інші підозрілі дії, система негайно блокує джерела небезпеки, зокрема підозрілі IP-адреси, після чого здійснюється детальний аналіз вхідного трафіку. У разі, якщо під час аналізу не було виявлено шкідливих дій, система продовжує роботу в штатному режимі.

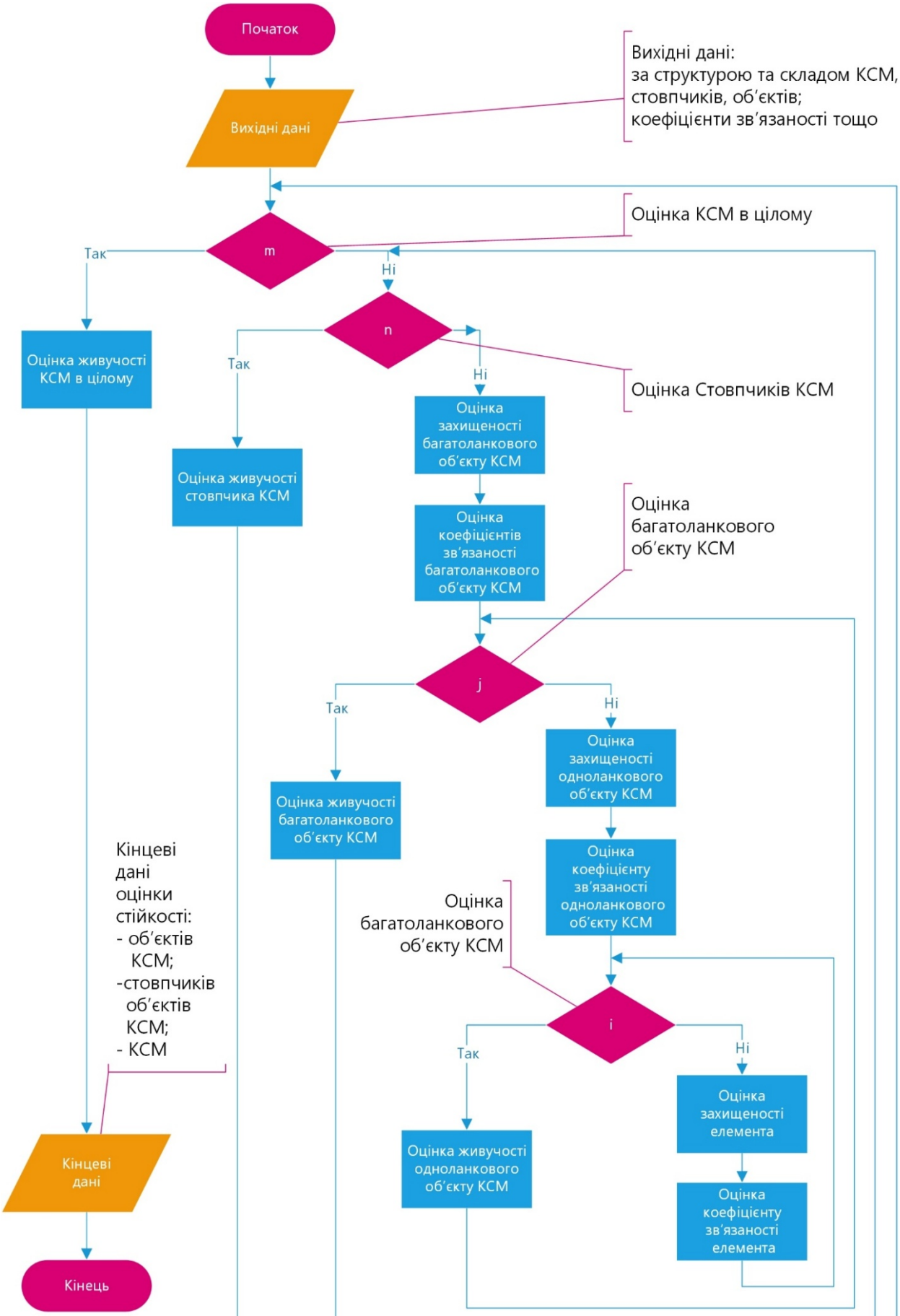


Рисунок 1.16. БСА методології оцінювання стійкості КСМ

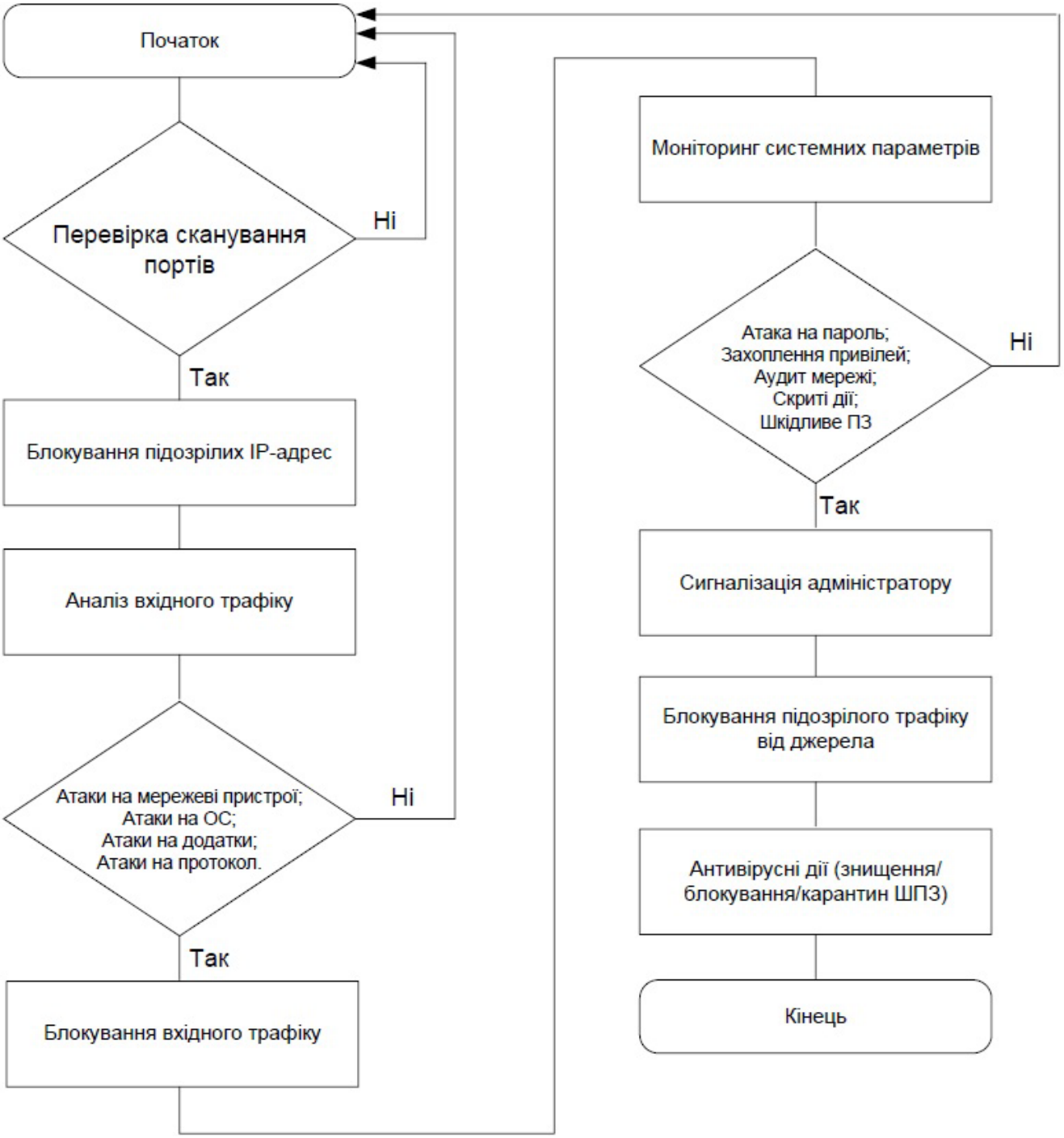


Рисунок 1.17. БСА виявлення та нейтралізації кібератак на комп'ютерні системи та мережі

Проте, якщо виявляються атаки на мережеві протоколи, операційні системи або інші компоненти, система автоматично блокує весь небезпечний вхідний трафік. Після цього починається моніторинг системних параметрів для виявлення можливих шкідливих змін.

Якщо система виявляє спроби атаки на паролі, захоплення привілей, аудиту мережевих ресурсів або шкідливе програмне забезпечення, вона сигналізує

адміністратору про загрозу і блокує трафік від джерела загрози. Після цього активуються антивірусні механізми для обробки виявленого шкідливого ПЗ, включаючи його видалення, блокування або переміщення в карантин. БСА на рис.1.17 забезпечує комплексну багаторівневу систему захисту інформації в комп'ютерних системах і мережах, забезпечуючи ефективну протидію кіберзагрозам на всіх рівнях роботи системи, починаючи з мережевої безпеки і закінчуючи моніторингом системних параметрів для забезпечення максимальної безпеки даних.

1.4.2 Реалізація програмного застосунку для оцінки рівня стійкості комп’ютерних систем і мереж

На базі представлених на рис.1.16 та 1.17 алгоритмів розроблено програмний застосунок для оцінки рівня стійкості комп’ютерних систем і мереж. Оскільки написання програмного коду розрахунку рівня стійкості комп’ютерних систем і мереж не містить специфічних вимог, зазначена програма була написана об’єктно-орієнтованою мовою програмування С++ у інтегрованому середовищі розробки Embarcadero RAD Studio 10.3, якт має зручний інтерфейс розробника, більш ніж достатні можливості для вирішення даної задачі.

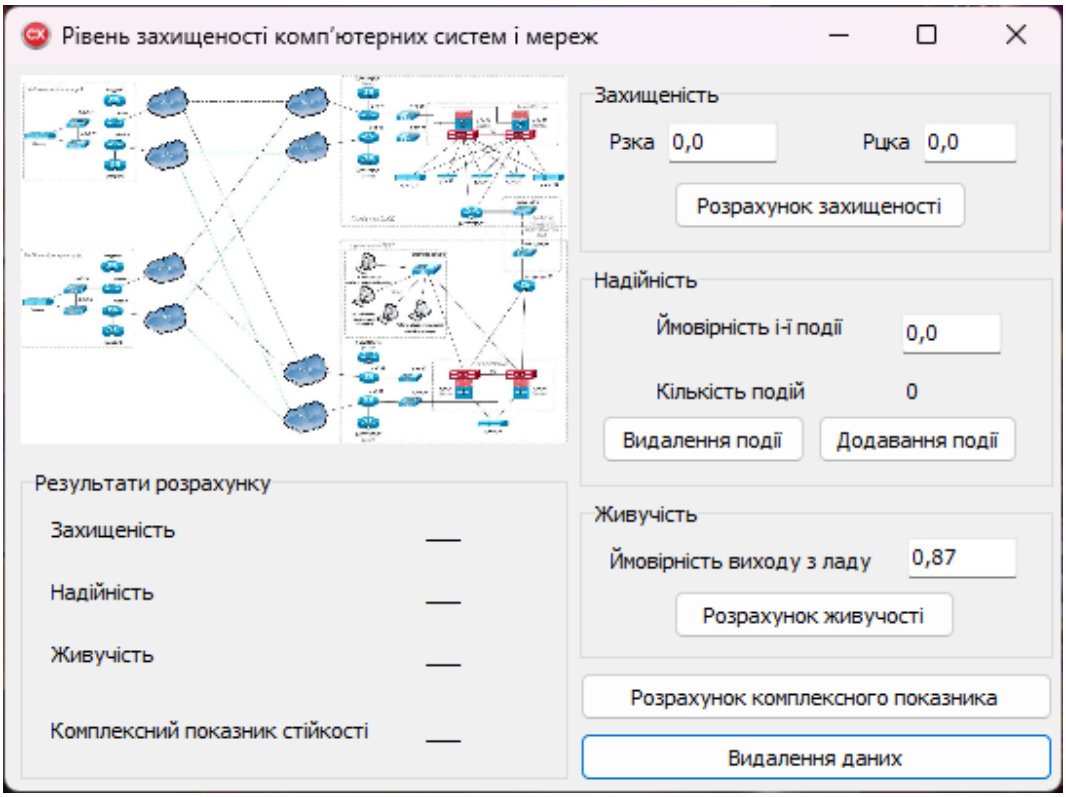


Рисунок 1.18. Інтерфейс застосунку для оцінки рівня стійкості і стійкості КСМ

Інтерфейс програмного застосунку для оцінки рівня стійкості комп’ютерних систем і мереж представлено на рисунку 1.18. Введення вхідних даних здійснюється у відповідних групах (GroupBox) праворуч у інтерфейсному вікні програми. Ці групи включають: Захищеність (Security), Надійність (Reliability) та Живучість (Survivability). Вхідні дані є характеристиками об'єкта комп'ютерних систем і мереж (КСМ), які оцінюються за показниками живучості, захищеності та надійності. Розрахунковий метод для формування вхідних даних базується на формулах, наведених у п. 1.3. Ймовірність визначається у діапазоні від 0 до 1, а стани об'єкту КСМ можуть виражатися у відносних одиницях щодо максимального значення. Натискаючи кнопку «Додавання події», користувач може вводити параметри необхідної кількості об'єктів КСМ. Після введення вхідних даних, натискаючи кнопки «Розрахунок захищеності», «Розрахунок живучості» та «Додавання події», слід натиснути на кнопку «Розрахунок комплексного показника» знизу вікна програми, після чого внизу зліва з'являться результати розрахунку. Для розробки програмного застосунку були використані наступні інструменти: мова програмування C++, середовище розробки Embarcadero RAD Studio C++Builder, бібліотеки для побудови графічного інтерфейсу користувача (GUI) та інструменти для моделювання мережевих структур. Інтерфейс програми складається з таких основних елементів: групи для введення даних (GroupBox), що містять поля для введення різних показників та параметрів, область результатів, де відображаються результати розрахунків для показників захищеності, надійності, живучості та комплексного показника стійкості, кнопки для виконання розрахунків та видалення даних, а також схема мережі, яка розташована ліворуч і ілюструє структуру комп'ютерної системи або мережі, що оцінюється. Лістинг (код) програмного застосунку мовою C++ наведено у додатку А пояснювальної записки.

1.4.3 Визначення рівня стійкості комп’ютерних систем і мереж

Для перевірки адекватності реагування розроблених моделей та методів на різноманітні ініціалізуючі величини було проведено експериментальне дослідження. Основна мета полягала у перевірці практичної придатності

розробленого програмного забезпечення для розрахунку рівня стійкості декількох комп’ютерних систем і мереж (КСМ).

За допомогою розробленого програмного застосунку було проведено розрахунок захищеності, що визначається як ймовірність забезпечення виконання цільової функції об'єкта КСМ із заданою якістю в умовах загальних та цілеспрямованих деструктивних інформаційних впливів. Формула розрахунку захищеності виглядає наступним чином: $К_{оксм}^{зах} = (1 - Рзка) * (1 - Рцка)$ де *Р*зка – ймовірність реалізації загальних кібератак, а *Р*цка – ймовірність реалізації цілеспрямованих кібератак. Використовуючи розроблений програмний застосунок, у відповідні поля були введені значення *Р*зка та *Р*цка, після чого натисканням кнопки "Розрахунок захищеності" було отримано показник захищеності об’єкта КСМ.

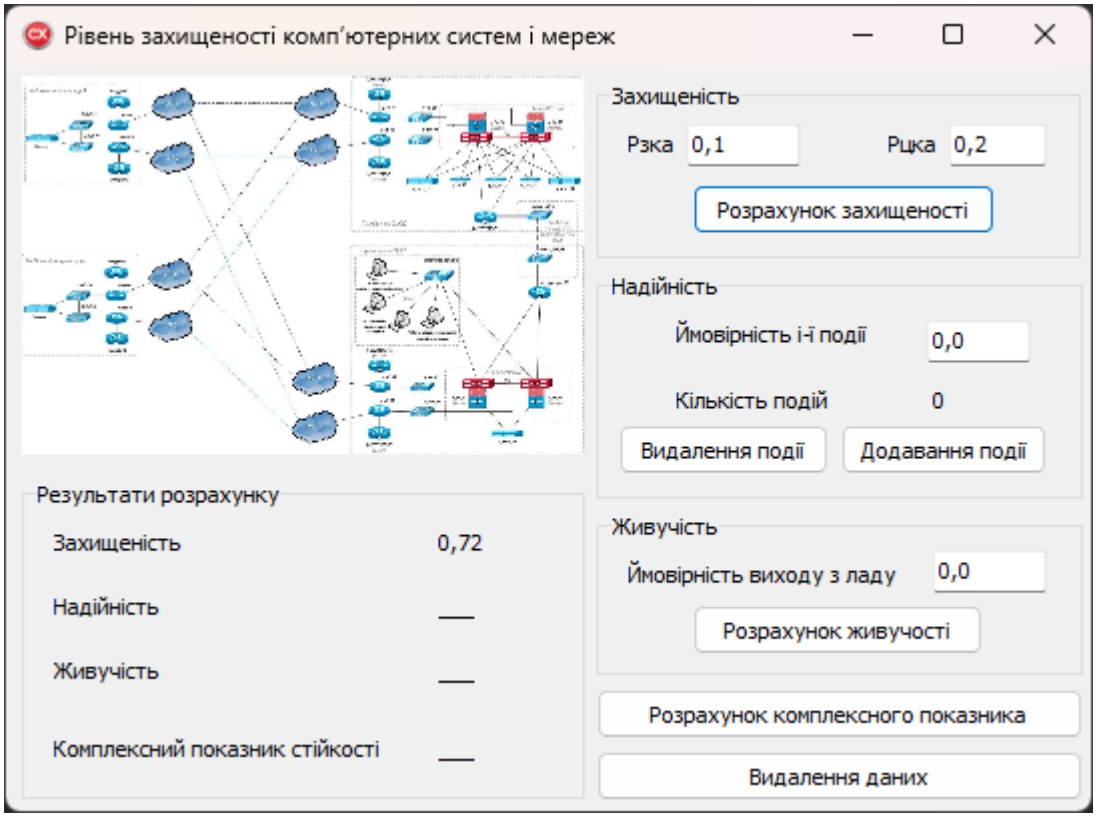


Рисунок 1.19. Розрахунок захищеності об’єкта КСМ

На рис. 1.19 показано результат розрахунку захищеності об’єкту КСМ при виникненні пожежі (загальний деструктивний інформаційний вплив) та навмисного пошкодження або крадіжки обладнання (цілеспрямований

деструктивний інформаційний вплив).

Окрім цього, розроблений програмний застосунок дозволяє здійснювати розрахунок надійності об'єкта КСМ. Надійність трактується як ймовірність забезпечення виконання цільової функції об'єкта КСМ протягом визначеного часового інтервалу в умовах періодичного виникнення програмних та технічних відмов засобів об'єкта КСМ внаслідок деструктивних інформаційних впливів (i = 1,…., N). Формула для розрахунку надійності виглядає наступним чином: $К_{ОКСМ}^{над} = \prod_{i=1}^{N} К_{ОКСМнад\,i}(1 - P_i)$, де Pi – ймовірність реалізації певної події. Введення значень ймовірності реалізації події у поле "Ймовірність і-ї події" та додавання кількості таких подій дозволяє отримати показник надійності об’єкта КСМ.

На рис. 1.20 показано результат розрахунку надійності об’єкту КСМ при здійсненні п’яти спроб спуфінгу (підміна отримувача).

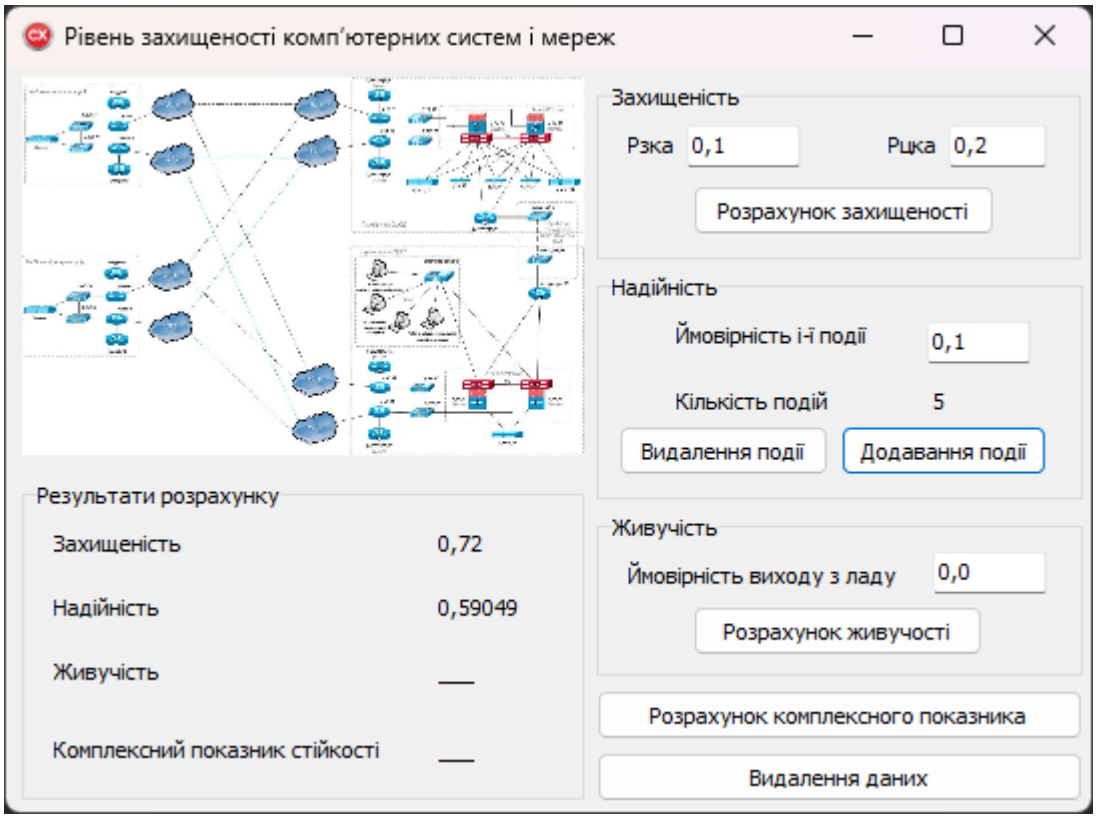


Рисунок 1.20. Розрахунок надійності об’єкта КСМ

Також розроблений програмний застосунок дозволяє розрахувати живучість об’єкта КСМ, яка трактується як ймовірність невиходу кінцевого стану системи із

заданої безпечної області *S* (невиходу з ладу). Формула для розрахунку живучості виглядає наступним чином: $К_{оксм\ жив} = 1 - V_S$, де V_S – ймовірність виходу кінцевого стану системи із заданої безпечної області S (виходу з ладу). Введення значення ймовірності виходу кінцевого стану системи із заданої безпечної області у поле "Ймовірність виходу з ладу" дозволяє отримати показник живучості об’єкта КСМ.

На рис. 1.21 представлено результат розрахунку живучості об’єкту КСМ при здійсненні пошкодження файлів операційної системи.

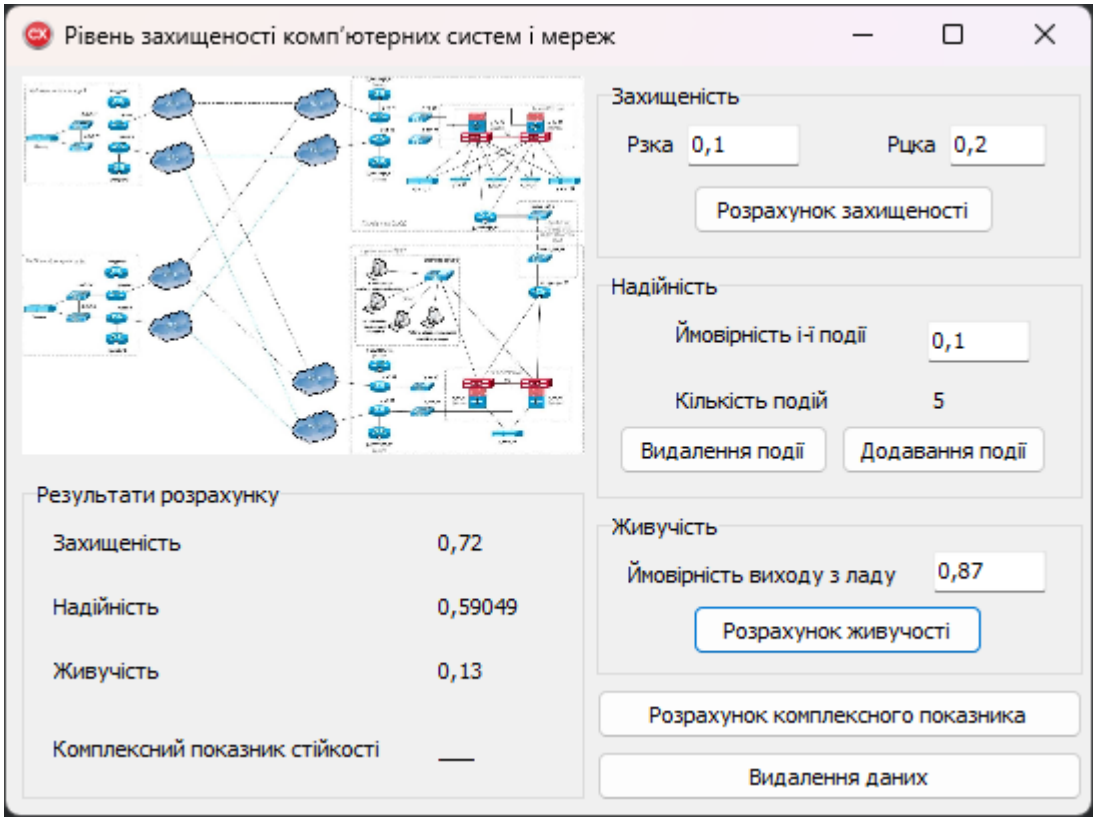


Рисунок 1.21. Розрахунок живучості об’єкта КСМ

З урахуванням того, що узагальнений показник стійкості трактується як добуток показників живучості, надійності та захищеності, його було обчислено за допомогою розробленого програмного застосунку. Після натискання кнопки "Розрахунок комплексного показника" у полі "Комплексний показник стійкості" з'являється результат (рис. 1.22).

Отримані результати підтверджують функціонування системи оцінювання стійкості об’єктів комп’ютерних систем і мереж та її успішне практичне

застосування. Розроблене алгоритмічне забезпечення та програмний застосунок дозволяють здійснювати автоматизований розрахунок стійкості з урахуванням показників надійності, захищеності та живучості, що підтверджує ефективність використаного методу та методики захисту інформації в комп'ютерних системах і мережах. Експериментальні дослідження показали, що запропоновані рішення є ефективними при забезпеченні безпеки інформаційних систем об'єктів КСМ.

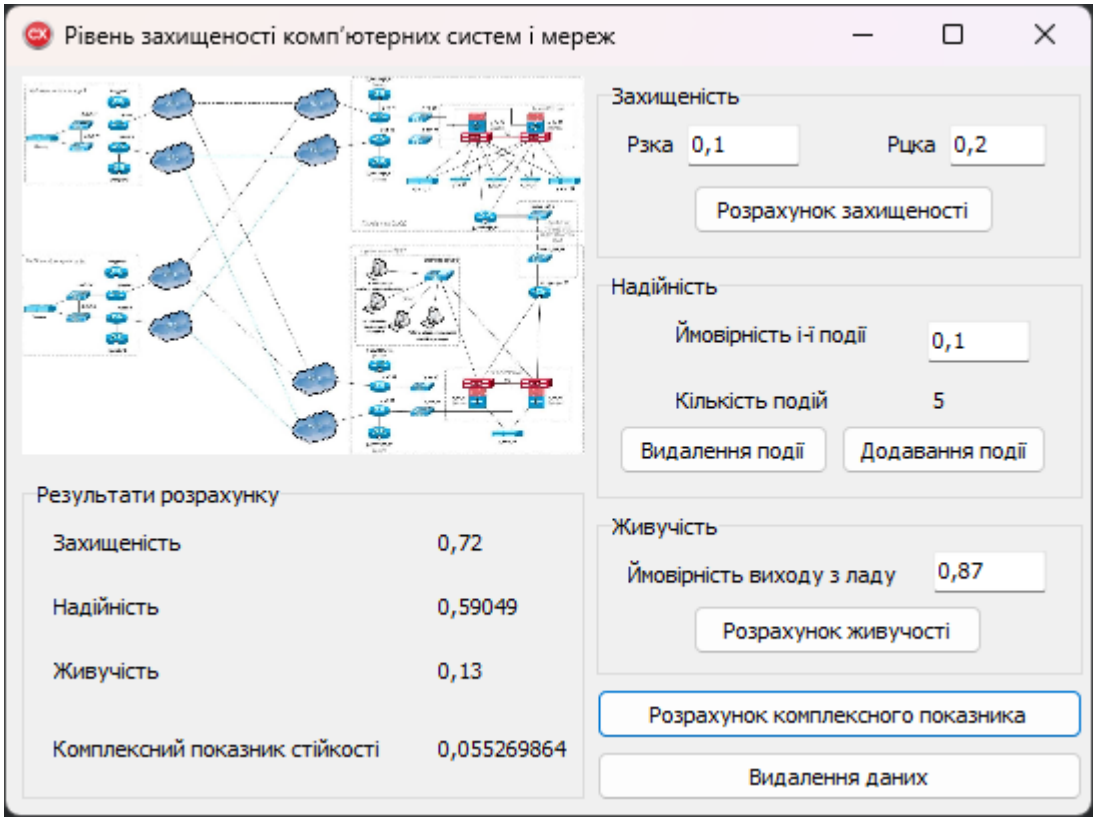


Рисунок 1.22. Розрахунок комплексного показника стійкості об'єктів КСМ

2 ЕКОНОМІЧНИЙ РОЗДІЛ

2.1 Резюме

У даному дипломному дослідженні розроблено програмну модель для визначення рівня стійкості, що охоплює створення алгоритмів, розробку програмного застосунку на базі Embarcadero RAD Studio із використанням мови C++ та оцінку стійкості комп'ютерних систем і мереж. Отримані результати обчислень підтвердили ефективність впровадженої методики, спрямованої на забезпечення захищеності об'єктів.

Ефективність програмного забезпечення залежить не лише від його внутрішньої якості, але й від успішності процесу його створення. Якість ПЗ оцінюють за кількома критеріями: з позиції користувача, з точки зору ефективного використання ресурсів та відповідності встановленим вимогам. З погляду користувача, якість програмного продукту включає аналіз витрат, пов'язаних з його розробкою, зокрема – оцінку трудомісткості та вартості виробництва. У цьому розділі проведено розрахунок собівартості створеного програмного забезпечення.

2.2 Визначення трудомісткості розробки програмного забезпечення

Тривалість створення програмного продукту визначається його масштабом, рівнем трудомісткості, кваліфікацією виконавців та встановленими ринковими термінами. Використовуючи метод структурної аналогії та аналіз відповідних каталогів аналогічного ПЗ, можна встановити обсяг програмного засобу, що виражається у тисячах умовних машинних команд для аналога

Таблиця 2.1. Каталог аналогів

Найменування ПП	**Обсяг функції ПП – V_o, усл. машинних командах.**
1. ПП автоматизації засобів по каталогу	680 – 7000
2. ПП автоматизованих розрахунків	1300 – 8600
3. ПП оптимізації розрахунків	1300 – 4200

У таблиці 2.1 представлені аналоги програмного забезпечення, функції яких, у більшому або меншому ступені, виконує розроблений програмний продукт. Для нашого варіанта виділено сірим кольором.

Вибравши аналог ПЗ, що містить Vo в умовних машинних командах, трудомісткості визначати на основі табл.2.2

Таблиця.2.2. Норма часу

Обсяг ПЗ, тис.умов.машинних команд	**Норма часу, люд/год**
1.00	229
2.00	244
3.00	262

На підставі отриманого значення, по довіднику, визначається укрупнена норма часу на розробку аналога програмного забезпечення (коректується поправочним коефіцієнтом враховуючої умови розробки ПП, тобто в умовах комп'ютера, Кк=0,7÷0,8): $T^a = 244 \times 0,7 = 170,08$ (люд/годин).

Трудомісткість програмного продукту визначається окремо для кожного етапу розробки, виходячи з показників трудомісткості відповідного аналога. При цьому враховують рівень складності розробки, ступінь інноваційності та частку використання стандартних модулів. Розрахунки проводяться згідно з наступними формулами:

$$T_{ТЗ} = T^a p \times L_1 \times K_H \quad (2.1)$$

$$T_{ТП} = T^a p \times L_2 \times K_H \quad (2.2)$$

$$T_{РП} = T^a p \times L_3 \times K_H \times K_T \quad (2.3)$$

Для розрахунку необхідні наступні коефіцієнти:

Li – питома вага і-го етапу розробки (див. табл. 2.3.);

Кн – поправочний коефіцієнт, що враховує ступінь новизни (див. табл. 2.4.);

Кт – поправочний коефіцієнт, що враховує ступінь використання в розробці типових програм (див. табл. 2.5)

Таблиця 2.3. Значення питомих коефіцієнтів трудомісткості стадії в загальній трудомісткості розробки ПП

Код стадії	**Ступінь новизни**		
	А	Б	В
ТЗ (L_1)	0,15	0,12	0,12
ТП (L_2)	0,16	0,15	0,11
РП (L_3)	0,55	0,58	0,61

Для нашого варіанта виділено сірим кольором.

Таблиця 2.4. Значення поправочного коефіцієнта, що враховує ступінь новизни

Код ступеня новизни	**Ступінь новизни**	**Значення $К_н$**
А	Принципово нові ПП	1,75 – 1,2
Б	ПП – розвиток визначеного параметричного ряду	1,0 – 0,8
В	ПП маючий аналог	0,7

Для нашого варіанта виділено сірим кольором.

Таблиця 2.5. Значення коефіцієнта ступеня використання в розробці типових програм

Ступінь охоплення реалізованих функцій розроблювального ПП типовими програмами, %	**Значення $К_т$**
60 і вище	0,6
40-60	0,7
20-40	0,8
До 20	0,9

Для нашого варіанта виділено сірим кольором.

Тепер розраховуємо трудомісткість по кожному етапу окремо:

Трудомісткість технічного завдання

$$Т_{тз}=Т^а * L_1 * К_н = 183,2 * 0,12 * 0,7 = 15,38 \text{ (люд/годин)} \quad (2.4)$$

Трудомісткість розробки технічного проекту

$$Т_{тп}=Т^а * L_2 * К_н = 183,2 * 0,11 * 0,7 = 14,11 \text{ (люд/годин)} \quad (2.5)$$

Трудомісткість розробки робочого проекту

$$Т_{рп}=Т^а * L_3 * К_н * К_т = 183,2 * 0,61 * 0,7 * 0,6 = 46,94 \text{ (люд/годин)} \quad (2.6)$$

Для подальших розрахунків визначили кількість папера, витраченого на кожен етап: технічне завдання $N_{тз}$= 2 (стр), розробка ТП $N_{тп}$=26 (стр), розробка робочого проекту $N_{рп}$=6(стр), пояснювальна записка відповідно $N_{пз}$=22(стр) Розрахунок зведений у таблицю 2.6.

Таблиця 2.6. Розрахунок трудомісткості ПП

Найменування етапів	**Розрахунок, годин**		
1.ТЗ	$T_{Ртз}$=15,38	$T_{кк}=0,7*N_{тз}$= 0,7*2=1,4	$T_{нк}=0,15*N_{тз}$=0,15*2=0,3
2.Розробка ТП	$T_{Ртп}$=14,11	$T_{кк}=0,7*N_{тп}$=0,7*26=18,2	$T_{нк}=0,15*N_{тп}$=0,15*26=3,9
3.Розробка РП	$T_{Ррп}$= 46,94	$T_{кк}=0,7*N_{рп}$=0,7*6=4,2	$T_{нк}=0,15*N_{рп}$=0,15*6=0,9
4.Розробка ПЗ	$T_{пз}=1,5*N_{пз}$= 1,5*22=33	$T_{кк}=0,7*N_{тз}$=0,7*22=15,4	$T_{нк}=0,15*N_{пз}$=0,15*22 =3,3
Усього, в т.ч.:	157,03		
- на розробку	$\Sigma T_{р}$=109,43		
- контроль керівника		$\Sigma T_{кк}$=39,2	
- нормоконтроль			$\Sigma T_{нк}$=8,4

2.3 Розрахунок ціни програмного продукту

Для оцінки вартості програмного продукту розглядаються основна заробітна плата виконавців, матеріальні витрати та загальні витрати на розробку ПЗ. Детальний розрахунок основної заробітної плати наведено у таблиці 2.7. Згідно зі статтею 8 «Закону про Державний бюджет України на 2025» з 1 січня 2025 року встановлено мінімальну місячну заробітну плату у розмірі 8000 гривень, а також мінімальну погодинну тарифну ставку – 48,00 грн.

Таблиця 2.7. Розрахунок основної заробітної плати виконавців

Найменування робіт	**Трудомісткість робіт, години**	**Погодинна тарифна ставка, грн.**	**Розрахунок, грн.**
1.Розробка ПП	109,43	48,00	5252,64
2.Контроль керівника	39,2	110,00	4312,00
3.Нормоконтроль	8,4	105,00	882,00
Усього	-	-	$\Sigma З_{о}$= 10446,64

Зробимо розрахунок матеріальних витрат на розробку ПП. Розрахунок зведемо в таблицю 2.8.

Таблиця 2.8. Розрахунок матеріальних витрат на розробку ПЗ

Найменування матеріальних витрат	**Тип, модель**	**Кількість**	**Ціна одиниці, грн.**	**Вартість, грн.**
Папір	Лист А4	56	5.0	280,0
Разом	-	-	-	$В_{м\,і}$=280,0
Транспортно – заготівельні Витрати (10%)				$Втр\_з = 0{,}1 \times Вм1$= 0,1*280=28,0
Усього				$В_м=В_{мі}+В_{тр\ з=}$ 308,00

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому ПП за формою, приведеною в таблиці 2.9.

Таблиця 2.9. Розрахунок статей витрат планової собівартості

Стаття витрат	**Значення, грн.**	**Формула розрахунку**
1. Матеріали	308,00	$В_м$ (див. табл. 2.8.)
2. Основна заробітна плата	10446,64	$З_о$ (див. табл. 2.7.)
3.Додаткова заробітна плата	1044,66	$Зд = 0{,}1 \times Зо$ = 10446,64*0,1
4.Відрахування до єдиного фонду соціального внеску	2528,08	$Вє.с.в. = 0{,}22 \times (Зо + Зд)$ =0,22* (10446,64+1044,66)
5. Накладні витрати	4178,66	$Внак. = 0{,}4 \times Зо$ =0,4 * 10446,64
6. Повна собівартість	18506,04	$С_{пов}$= $В_м$ +$З_о$ + $З_д$ +Вє.с.в. + Внак.= 308,00+10446,64+1044,66+2528,08 +4178,66

Розмір прибутку, що включається в ціну, визначаємо по наступній формулі:

$$П=(С_{пов}*Р)/100=(18506,04*10)/100=1850,6 \text{ грн} \qquad (2.7)$$

Де р – плановий рівень рентабельності (10-15%).

Оптова ціна (кошторисна вартість) визначається по формулі:

$$Ц_о = С_{пов}+П = 18506,04+1850,6 = 20356,64 \text{ грн;} \qquad (2.8)$$

Виходячи з отриманих даних, ціна реалізації розробленого програмного забезпечення становитиме:

$$Ц_р=Ц_о+ПДВ = 20356,64+20356,64 *0.2 = 24427,97 \text{ грн;} \qquad (2.9)$$

3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Сучасне впровадження комп'ютерної техніки дає змогу автоматизувати безліч рутинних процесів, оптимізувати обробку даних і забезпечити оперативний доступ до численних інформаційних ресурсів, а також виконання необхідних розрахунків. Ці можливості сприяють значному підвищенню продуктивності праці та ефективності роботи організацій. Втім, з широковживанням персональних комп'ютерів у професійній діяльності зростають і певні негативні наслідки, зокрема – підвищене навантаження на здоров'я співробітників через тривалий час роботи за комп'ютером.

В контексті даного дипломного проєкту під розробку програмної моделі оцінки рівня стійкості комп'ютерних систем і мереж розуміється створення аналітичного інструмента, який базується на сучасних підходах до аналізу робочих місць. Робоче місце користувача включає системний блок із встановленим програмним забезпеченням, розробленим спеціально для оцінки життєздатності, надійності та захищеності систем і мереж. При цьому стандартні вимоги безпеки праці для користувача ПК залишаються актуальними, оскільки забезпечують комфорт і мінімізацію ризиків для здоров'я в умовах підвищеної інтенсивності роботи.

Отже, створення такої моделі дозволяє не лише автоматизувати аналіз комп'ютерних систем і мереж, але й врахувати комплекс факторів, що впливають на їх стійкість у реальних умовах експлуатації.

3.1 Аналіз небезпечних і шкідливих факторів, що впливають на користувача ПК

До основних критеріїв забезпечення гігієни робочого середовища належать інтенсивність освітлення, температура повітря, вологість, рівень шумового забруднення, ступінь вібраційного впливу, токсичність, загазованість, а також обмеження загальної м'язової активності (гіподинамія). Крім цього, враховується дія електростатичного поля та вплив як неіонізуючих, так і іонізуючих електромагнітних випромінювань.

3.2 Гігієнічні вимоги до виробничого середовища

Державні санітарні норми, зокрема ДСАНПіН 3.3.2.007-98 «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин», спрямовані на запобігання негативного впливу шкідливих чинників, що супроводжують роботу з візуальними дисплейними терміналами, на здоров’я працівників.

3.2.1 Вимоги до приміщення

Розміщення робочих місць із використанням ВДТ, ЕОМ і ПЕОМ заборонено у підвальних приміщеннях та на цокольних поверхах. Для кімнат, призначених для роботи з візуальними дисплейними терміналами, рекомендується орієнтувати вікна у напрямку півночі або північного сходу. На вікнах повинні бути встановлені регульовані жалюзі або штори, що дозволяють їх повністю закривати для забезпечення оптимальних умов освітлення.

Планувальні рішення будівель і приміщень, де розташовано відеодисплейні термінали, мають відповідати вимогам ДСАНПіН 3.3.2.007-98. Для робочого місця програміста передбачено мінімальну площу не менше 6 кв. м та об’єм приміщення не менше 20 куб. м. Крім того, стіни приміщень повинні бути пофарбовані матовою фарбою, а в приміщеннях з ВДТ обов’язково мають бути передбачені зони для відпочинку та психологічного розвантаження.

3.2.2 Освітлення

Для забезпечення належного освітлення приміщення, де працює програміст, застосовується комбінована система, що поєднує природне освітлення із додатковим штучним світлом. Загальне оздоблення простору виконується за допомогою газорозрядних ламп типу ЛД. Згідно з встановленими нормами, для робочого місця, на якому здійснюються високоточні операції (де мінімальний розмір об'єкта розрізнення становить 0,3–0,5 мм), необхідна освітленість рівномірно має досягати 300 лк. В цілому, ці вимоги щодо освітлення забезпечені.

3.2.3 Шум

У робочих приміщеннях основним джерелом шумового навантаження є звуки, що генеруються ПЕОМ. Крім того, значну частину шуму створюють джерела електромагнітного походження – це коливання компонентів електромеханічних пристроїв під впливом змінних магнітних полів. До того ж, в приміщеннях виникає структурний шум, який випромінюють поверхні конструктивних елементів (стіни, перекриття, перегородки) у звуковому спектрі частот. Для зниження або усунення негативного впливу шуму доцільно ізолювати робочі зони, розташовуючи їх у частинах будівлі, що знаходяться в глибині та ведуть своїми вікнами у двір – таким чином мінімізується вплив міського шуму. Крім цього, необхідно регулярно перевіряти герметичність корпусів комп'ютерної техніки та своєчасно здійснювати заміну вентиляторів охолодження.

3.3 Вимоги до організації робочого місця працівника

Конструкція робочого місця користувача комп'ютера, з урахуванням розташування сидіння, засобів керування та засобу відображення інформації, розроблена згідно з антропометричними, фізіологічними та психологічними вимогами, а також відповідно до специфіки виконуваної роботи. Робоче меблеве обладнання повинно бути оснащене можливістю індивідуального регулювання, що дозволить адаптувати його під зріст кожного користувача й підтримувати оптимальну, зручну поставу. Робочий стіл рекомендовано обробляти матовим покриттям, що сприяє зменшенню небажаних відблисків. > > Розміщення дисплея організовано таким чином, щоб його верхня межа відповідала рівню очей, а відстань до екрану становила приблизно 70 см – що повністю входить у допустимий інтервал від 60 до 90 см. Частота мерехтіння екрану fмер дорівнює 100 Гц, що значно перевищує мінімальне рекомендоване значення у 70 Гц. Крім цього, робоче місце розташовано перпендикулярно до віконних прорізів, що дозволяє уникнути прямого та відбитого світлового мерехтіння від вікон та джерел штучного освітлення.

3.4 Мікроклімат

Показники мікроклімату, складу іонів у повітрі, а також рівень шкідливих речовин у робочих зонах, де використовуються ПК, мають відповідати вимогам ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень».

Для підтримки нормативних значень мікроклімату та забезпечення оптимального співвідношення позитивних і негативних іонів слід передбачити установку пристроїв зволоження, штучної іонізації або кондиціювання повітря. Крім того, рівні інфрачервоного випромінювання не повинні перевищувати встановлених нормативних меж згідно з ГОСТ 12.1.005. Також вміст озону в робочій зоні не має перевищувати 0,1 мг/м³, оксидів азоту – 5 мг/м³, а концентрація пилу повинна залишатися в межах 4 мг/м³.

3.5 Електробезпека

Приміщення, де використовуються імпульсні джерела живлення згідно з ОНТП24-86 і ПУЕ-87, віднесено до категорії об'єктів, де ризик ураження персоналу електричним струмом не є підвищеним. Це пояснюється тим, що відносна вологість повітря не перевищує 75%, температура залишається нижчою за 35°С, а хімічно агресивні середовища відсутні. Електроживлення обладнання організовано від двофазної мережі з заземленою нейтраллю, при напрузі 220 В і частоті 50 Гц, із застосуванням автоматичних пристроїв токового захисту.

В приміщенні обов’язково має бути встановлена схема заземлення. Ураження електричним струмом може виникнути у випадках: 1) при контакті з відкритими струмоведучими елементами; 2) при торканні нестумоведучих частин обладнання, які, через порушення ізоляції або інші причини, опинилися під напругою.

Відповідно до вимог ГОСТ-12.2.007.0-75 устаткування (за винятком ЕОМ II класу) відноситься до I класу та оснащене робочою ізоляцією згідно з ГОСТ 12.1.009-76. Підключення обладнання здійснено згідно з нормативами ПБЕ та ПУЕ, тому додаткових заходів щодо електробезпеки не вимагається.

3.6 Пожежна безпека

Робоче приміщення, що відповідає вимогам ПБЕ та ОНТП 24–86 у сфері вибухово-пожежної безпеки, класифікується як об’єкт категорії «В».

Основними потенційними причинами виникнення пожежі в такому приміщенні є:

1. Коротке замикання електропроводки;

2. Використання побутових електрорадіоприладів;

3. Недотримання встановлених норм протипожежного захисту.

Відповідно до ПУЕ, для зниження ризику виникнення пожежі необхідно забезпечити комплекс заходів, зокрема: ретельну ізоляцію всіх струмоведучих проводів, що підключені до робочих місць, регулярний огляд та перевірку стану їх ізоляції, а також суворе дотримання норм безпечної експлуатації обладнання.

Для гасіння пожеж на робочому місці користувача ПК застосовують як вуглекислотні, так і порошкові вогнегасники.

– Вуглекислотні вогнегасники випускаються у варіанті ручних пристроїв (наприклад, ВВК-5);

– Порошкові вогнегасники представлені моделями ВП-2, ВП-5, ВП-10 та іншими

Рисунок 3.1. Засоби пожежогасіння

З метою своєчасного оповіщення, на дільниці необхідно встановити протипожежну сигналізацію. Проходи та запасні виходи повинні бути вільними. Пожежний щит повинен розміщуватись в доступному місці та містити первинні засоби пожежогасіння (вогнегасник, лопату, відро, простирадло, ящик з піском)

ВИСНОВКИ

У виконаному дипломному проекті розглянуто сучасні методи та засоби оцінки рівня стійкості комп'ютерних систем і мереж. Аналізувалися підходи щодо таксономії загроз інформаційній безпеці комп'ютерних систем і мереж, побудовано модель загроз інформаційним об'єктам у комп'ютерних системах і мережах, включаючи таксономію загроз, матрицю залежності об'єктів захисту від типу загроз і модель бази даних загроз інформаційним об'єктам. Передбачена система захисту інформації комп'ютерних систем і мереж включає методи розпізнавання загроз, структурну модель системи виявлення підозрілих впливів і методику оцінювання стійкості комп'ютерних систем і мереж.

Реалізовано програмну модель для оцінки рівня стійкості, що включає розробку алгоритмів, створення програмного застосунку у середовищі Embarcadero RAD Studio мовою C++ та визначення рівня стійкості комп'ютерних систем і мереж.

В ході роботи проаналізовано сучасні методи та засоби захисту інформації в комп'ютерних мережах та системах; побудовано таксономію кіберзагроз, яка враховує параметри системи, властивості порушника та структуру загрози; складено матрицю залежності інформаційних об'єктів захисту від типу загроз; розроблено модель бази даних загроз, яка дозволяє створити базу даних для інформаційної безпеки комп'ютерних мереж та систем; реалізовано комбінований метод розпізнавання загроз, який поєднує сигнатурний метод та метод виявлення аномалій; розглянуто методику оцінювання стійкості комп'ютерних систем та мереж, що забезпечує підтримку створення систем захисту інформації; побудовано структурну модель багаторівневої системи виявлення кібервпливів на основі комбінованого методу розпізнавання загроз; розроблено алгоритмічне забезпечення та програмний застосунок захисту інформації, який дозволяє автоматизовано розраховувати комплексний показник стійкості з урахуванням надійності, захищеності та живучості. Отримані результати розрахунку за допомогою створеного застосунку підтвердили ефективність реалізованої методики, орієнтованої на захист об'єктів комп'ютерних систем та мереж.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Балагура В. І., Андрущенко І. В. Інформаційна безпека: основи та методи захисту. Київ: Вид-во КНУ ім. Т. Шевченка, 2015. 320 с.
2. Литвиненко О. В., Литвиненко І. В. Кібербезпека: теорія та практика. Харків: Вид-во ХНУРЕ, 2018. 280 с.
3. Литвиненко В. М., Литвиненко О. В. Захист інформаційних систем: теорія та практика. Львів: Вид-во ЛПУ, 2017. 340 с.
4. Литвиненко І. В., Литвиненко О. В. Інформаційна безпека в умовах глобалізації. Одеса: Вид-во ОНУ ім. І. І. Мечникова, 2019. 360 с.
5. Балагура В. І., Андрущенко І. В. Кібербезпека та захист інформації. Київ: Вид-во КНУ ім. Т. Шевченка, 2020. 295 с.
6. Терейковський І. А., Гнатюк С. О. Захист інформації в комп'ютерних системах. Київ: Каравела, 2021. 310 с.
7. Лахно В. А., Гусєв Б. С., Касаткіна Д. Ю., Хорольська К. В. Захист інформації в комп'ютерних системах і кібербезпека. Харків: Основа, 2019. 290 с.
8. Бурдаєв В. П., Аксанов Н. Г., Кушнарьов М. В. Сучасні інформаційні технології і системи. Львів: Новий Світ, 2022. 400 с.
9. Network Programmability and Automation. Джейсон Едельман. 1-е видання. O'Райлі, 2022. 580 с.
10. Computer Networking: A Top-Down Approach. Джеймс Курос. 7th видання. Pearson, 2023. 800 с.
11. Каспер Крістофер. C++17 in Detail. Київ: Підручник, 2021. 400 с.
12. Мейерс Скотт. Effective Modern C++: 42 Specific Ways to Improve Your Use of C++11 and C++14. Київ: Підручник, 2019. 320 с.
13. Страуструп Бьєрн. The C++ Programming Language, 4th Edition. Київ: Підручник, 2018. 800 с.
14. Купер Тобіас. C++ Concurrency in Action: Practical Multithreading. Київ: Підручник, 2017. 350 с.
15. Стейн Ендрю. C++ Crash Course. Київ: Підручник, 2020. 200 с.

ДОДАТОК А. Коду модулю Unit1 мовою С++застосунку для оцінки рівня захищеності комп'ютерних систем і мереж

```
//---------------------------------------------------------------------------

#include <vcl.h>
#pragma hdrstop

#include "Unit1.h"
//---------------------------------------------------------------------------
#pragma package(smart_init)
#pragma resource "*.dfm"
TForm1 *Form1;
float Kgiv = 0;
float Kzah = 0;
float Rzka = 0;
float Rcka = 0;
float Knad = 1;
float KnadTemp = 1;
int KilkPodiy = 0;
//---------------------------------------------------------------------------
__fastcall TForm1::TForm1(TComponent* Owner)
        : TForm(Owner)
{
}
//---------------------------------------------------------------------------
void __fastcall TForm1::Button3Click(TObject *Sender)
{
try {
                if (StrToFloat(Edit1->Text) > 1) {
                        ShowMessage(L"Рзка не може бути більше 1");
                } else if (StrToFloat(Edit2->Text) > 1) {
                        ShowMessage(L"Рцка не може бути більше 1");
                } else {
                        Rzka = StrToFloat(Edit1->Text);
                        Rcka = StrToFloat(Edit2->Text);
                        Kzah = (1 - Rzka) * (1 - Rcka);
                        Label4->Caption = FloatToStrF(Kzah,ffFixed,6,2);
                }
        } catch (...) {
                ShowMessage(L"Помилка вводу даних");
        }
}
//---------------------------------------------------------------------------

void __fastcall TForm1::Button5Click(TObject *Sender)
{
try {
                if (StrToFloat(Edit3->Text) > 1) {
                        ShowMessage(L"Імовірність і-ої події не може бути більше 1");
                } else {
                        KilkPodiy += 1;
                        KnadTemp = Knad;
                        Knad = Knad * (1 - StrToFloat(Edit3->Text));
                        Label5->Caption = FloatToStrF(Knad,ffFixed,6,5);
                        Label13->Caption = IntToStr(KilkPodiy);
                        Button2->Enabled = true;
                }
        } catch (...) {
                ShowMessage(L"Помилка вводу даних");
        }
}
//---------------------------------------------------------------------------
```

```
void __fastcall TForm1::Button4Click(TObject *Sender)
{
        KilkPodiy -= 1;
        Label13->Caption = IntToStr(KilkPodiy);
        Knad = KnadTemp;
        Label5->Caption = FloatToStrF(Knad,ffFixed,6,5);
        Button2->Enabled = false;
}
//---------------------------------------------------------------------------

void __fastcall TForm1::FormCreate(TObject *Sender)
{
         Label4->Caption = "___";   // 10
        Label5->Caption = "___";    //  11
        Label6->Caption = "___";    // 12
        Label8->Caption = "___";    // 13
}
//---------------------------------------------------------------------------

void __fastcall TForm1::Button1Click(TObject *Sender)
{
  Kgiv = 0;
        Kzah = 0;
        Rzka = 0;
        Rcka = 0;
        Knad = 1;
        KnadTemp = 1;
        KilkPodiy = 0;

        Edit1->Text = "0,0";
        Edit2->Text = "0,0";
        Edit3->Text = "0,0";

        Label13->Caption = "0";
        Label4->Caption = "___";
        Label5->Caption = "___";
        Label6->Caption = "___";
        Label8->Caption = "___";
}
//---------------------------------------------------------------------------

void __fastcall TForm1::Button6Click(TObject *Sender)
{
try {
                if (StrToFloat(Edit4->Text) > 1) {
                        ShowMessage(L"Імовірність виходу з ладу не може бути більше 1");
                } else {
                        Kgiv = 1 - StrToFloat(Edit4->Text);
                        Label6->Caption = FloatToStrF(Kgiv,ffFixed,6,2);
                }
        } catch (...) {
                ShowMessage(L"Помилка вводу даних");
        }
}
//---------------------------------------------------------------------------

void __fastcall TForm1::Button2Click(TObject *Sender)
{
if (Label4->Caption == "___" || Label5->Caption == "___" || Label6->Caption == "___") {
                ShowMessage(L"Розрахуйте всі необхідні параметри");
        } else {
                Label8->Caption = FloatToStr(StrToFloat(Label4->Caption) * StrToFloat(Label5-
>Caption) * StrToFloat(Label6->Caption));
        }
}
//---------------------------------------------------------------------------
```

ДОДАТОК Б. Слайди мультимедійної презентації

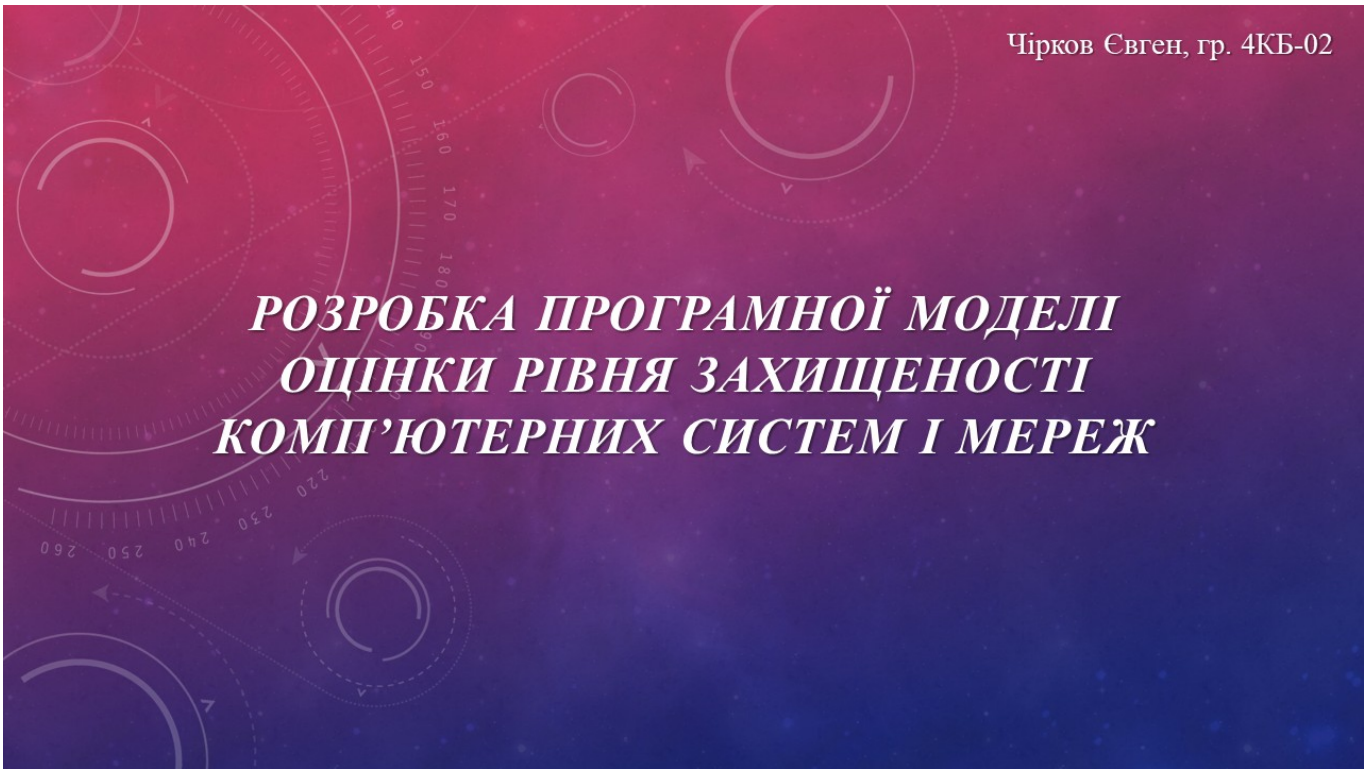
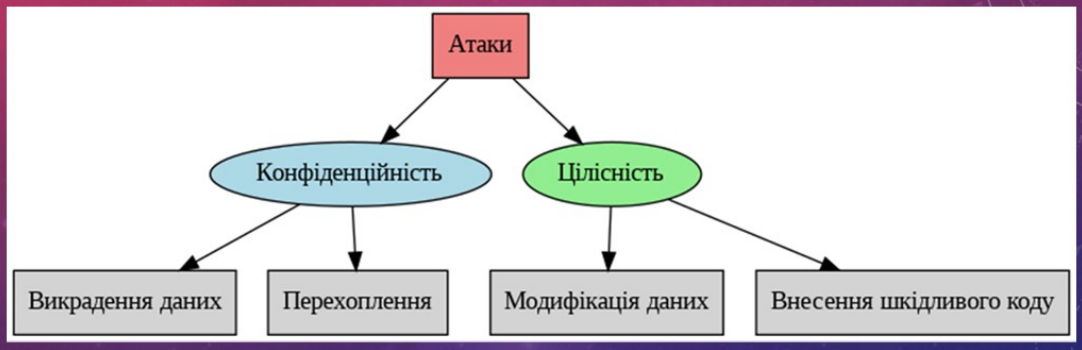
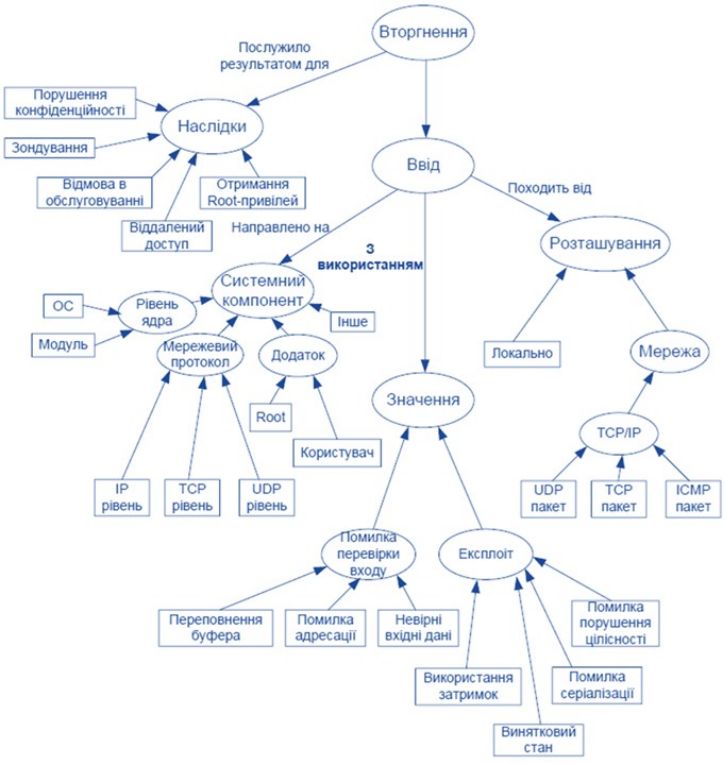


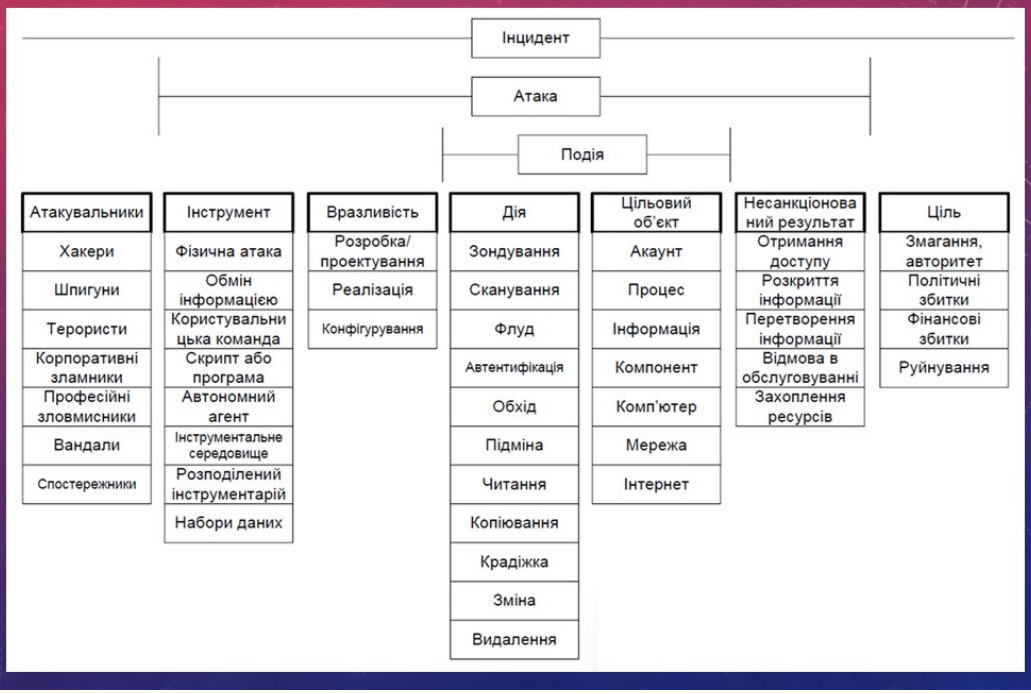
Схема класифікації атак





Таксономія загроз інформаційній безпеці на основі вторгнення

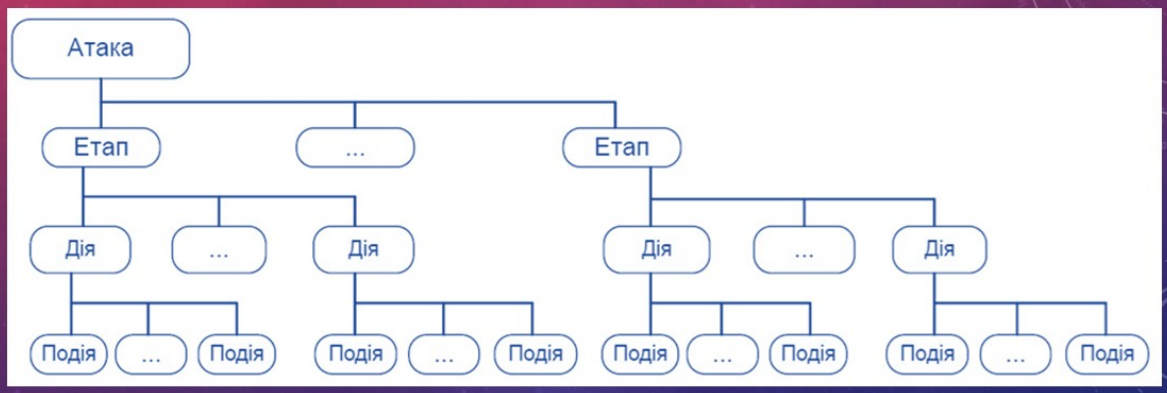
Таксономія загроз інформаційній безпеці на основі інцидентів



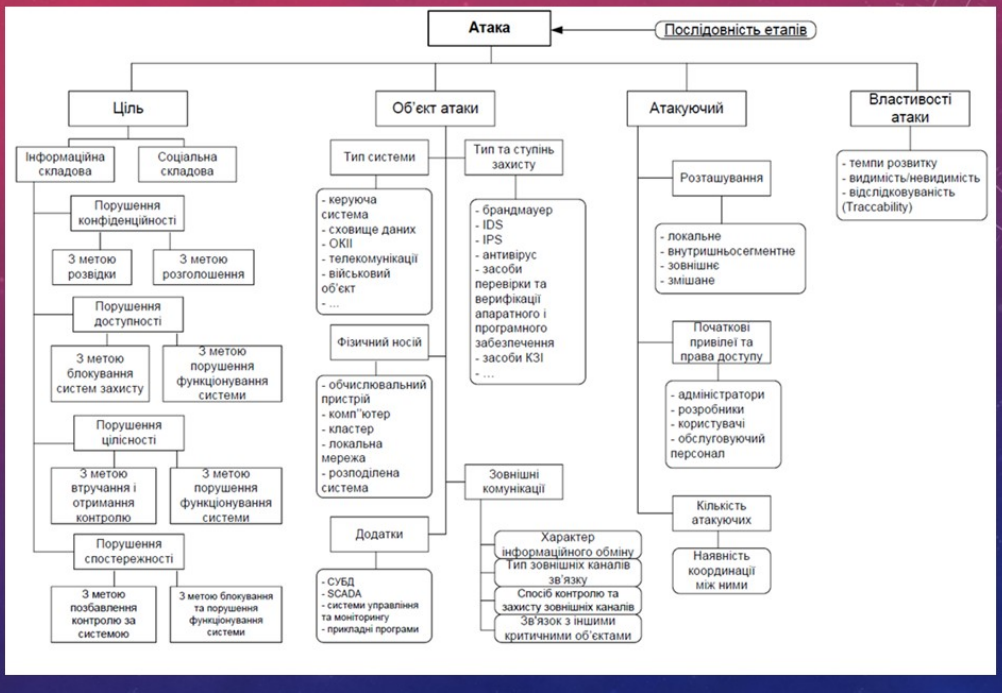
Аналіз ефективності різних підходів таксономій загроз ІБ

Властивості / підходи до класифікації	Застосовуваність (інформативність)	Повнота	Детермінованість	Взаємне виключення	Чіткість термінів	Об' єктивність	Зрозумілість	Однозначність	Узгодженість	Повторюваність результатів
За ефектом впливу на властивості інформації	-	+	+	-	-	+	-	-	+	-
Вразливості апаратного та програмного забезпечення	+	-	+	+	+	+	+	+	-	-
Загальний список атак	+	-	-	-	+	+	-	-	+	-
Комбінований підхід	+	+	+	+	+	+	+/-	+	+	+

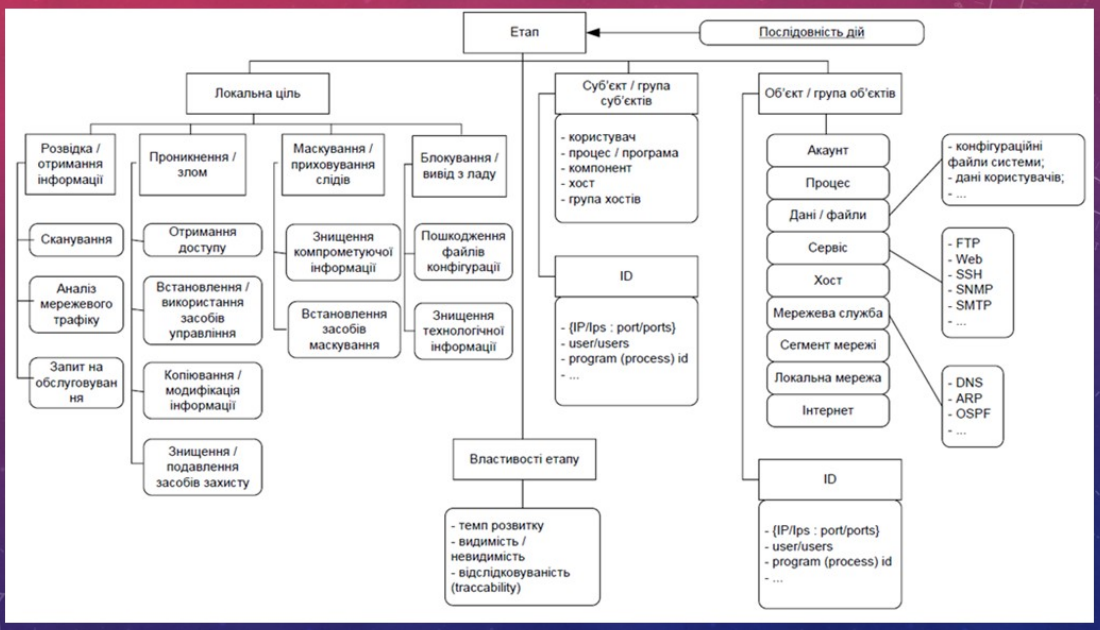
Ієрархічна структура атаки на інформаційну систему



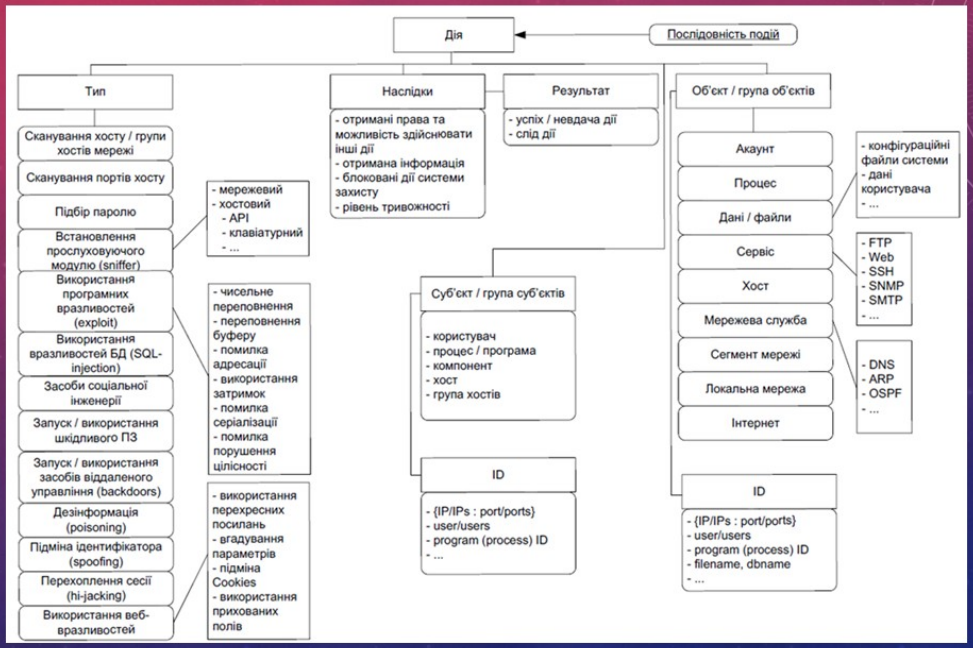
Функціональна схема атаки на інформаційну систему



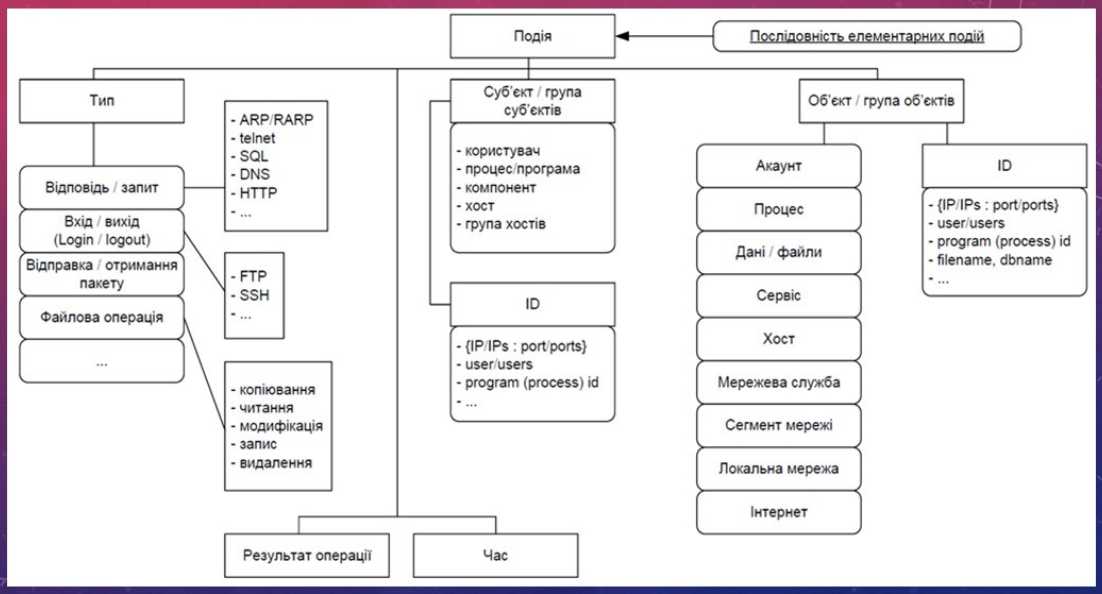
Функціональна схема етапу атаки на інформаційну систему



Функціональна схема дії при атаці на інформаційну систему



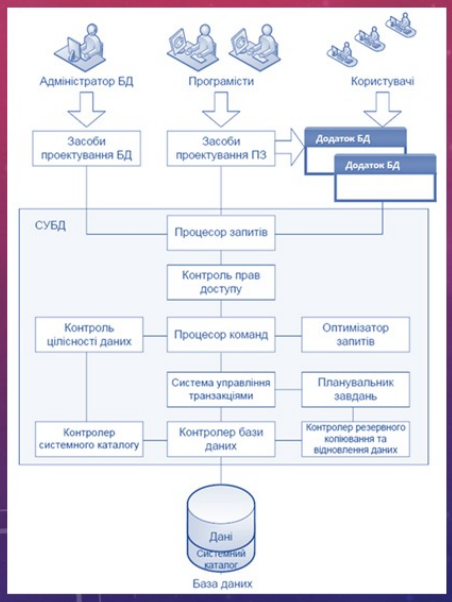
Функціональна схема події при атаці на інформаційну систему



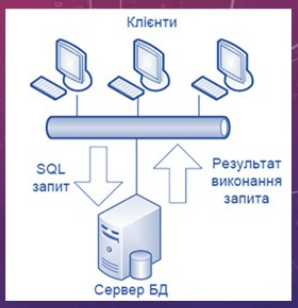
Матриця загроз для програмних та апаратних засобів КСМ

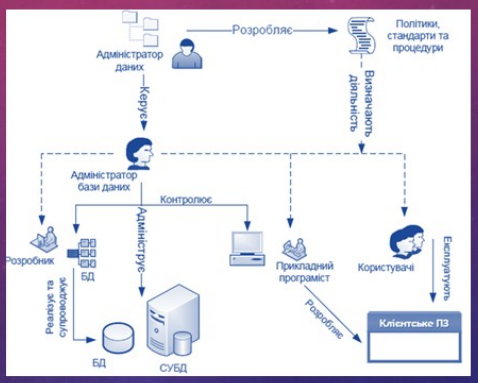
Об'єкти / загрози	*Кабельна система*	*Мережеве обладнання*	*Засоби мережевого захисту*	*Технологічна інф. захисту активного мереж. обладнання*	*Технологічна інформація захисту хостів*	*Дані, що передаються мережею*	*Програмне забезпечення*	*Файли*	*Записи баз даних*	*Обчислювальні ресурси*
Відсутність фізичного з'єднання	•	•								
Помилки та непрацездатність АМО		•	•							
Розголошення даних про мережу				•	•					
Перехоплення (сніффінг) пакетів				•	•	•				
Підміна отримувача (спуфінг пакетів)				•	•					
Відмова в обслуговуванні (DoS)				•	•		•			
Дзеркалювання трафіку					•	•				
Непрацездатність мережевих застосувань							•	•	•	
Бекдор		•	•	•			•	•		•
Віддалене захоплення (боти, ботнети)				•	•		•			
Сканування системи		•	•	•						
Фітинг, маскарад			•	•		•	•	•	•	•
Соціальна інженерія	•	•	•	•	•	•	•	•	•	•
Цільова кібератака (APT)		•	•	•	•	•				
Помилка, збій та відмова прикладного ПЗ							•	•	•	•
Виконання недокументованих функцій					•			•	•	
Розповсюдження вірусів та хробаків					•		•	•	•	•
Несумісність версій ПЗ							•			
Перехоплення інформації					•					
Підміна або дезорганізація							•			
Злам					•		•			
Використання вразливостей (експлоїт)					•		•	•	•	•
Кейлогер					•			•	•	
Атака під час реєстрації					•		•	•	•	
Захоплення облікового запису (АТО)					•		•	•	•	
Помилка системного ПЗ							•	•		•
Перехоплення технологічної інформації					•					
Пошкодження файлів ОС					•		•			
Збирання «сміття»					•			•		
Втручання в роботу ОС з мережі					•		•	•		
Руткіт (rootkit)					•		•	•	•	•
Атака нульового дня							•	•		•

Модель бази даних з розподілом ролей користувачів (СУБД)



Клієнт-серверна архітектура бази даних





Організація процесів адміністрування та розробки баз даних

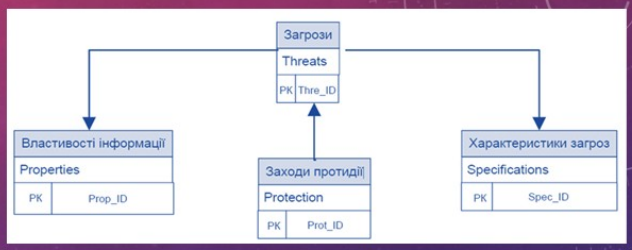
ID	Тип загрози	Опис загрози
1	Підробка (Spoofing)	Неправомірне використання IP-адреси для підробки особистості
2	Прослуховування (Sniffing)	Нелегальний перехоплення мережевих пакетів з метою збору даних
3	Відмова в обслуговуванні (DoS)	Атаки на сервер, що призводять до його перевантаження або недоступності

ID	Загроза	Специфікація
1	Підробка (Spoofing)	Кількість виявлених IP-адрес у спам-базах
2	Підробка (Spoofing)	Кількість спам-слів у темі повідомлення
3	Прослуховування (Sniffing)	Кількість пакетів з однаковими IP-адресами відправника та отримувача
4	DoS-атака	Кількість одночасних з'єднань до сервера
5	DoS-атака	Затримка між запитами від одного користувача

ID	Властивість	Опис
1	Цілісність	Забезпечення повноти та правильності даних
2	Конфіденційність	Обмежений доступ до інформації
3	Доступність	Гарантія доступу до сервісів у випадку загроз
4	Спостережність	Можливість моніторингу дій у системі.

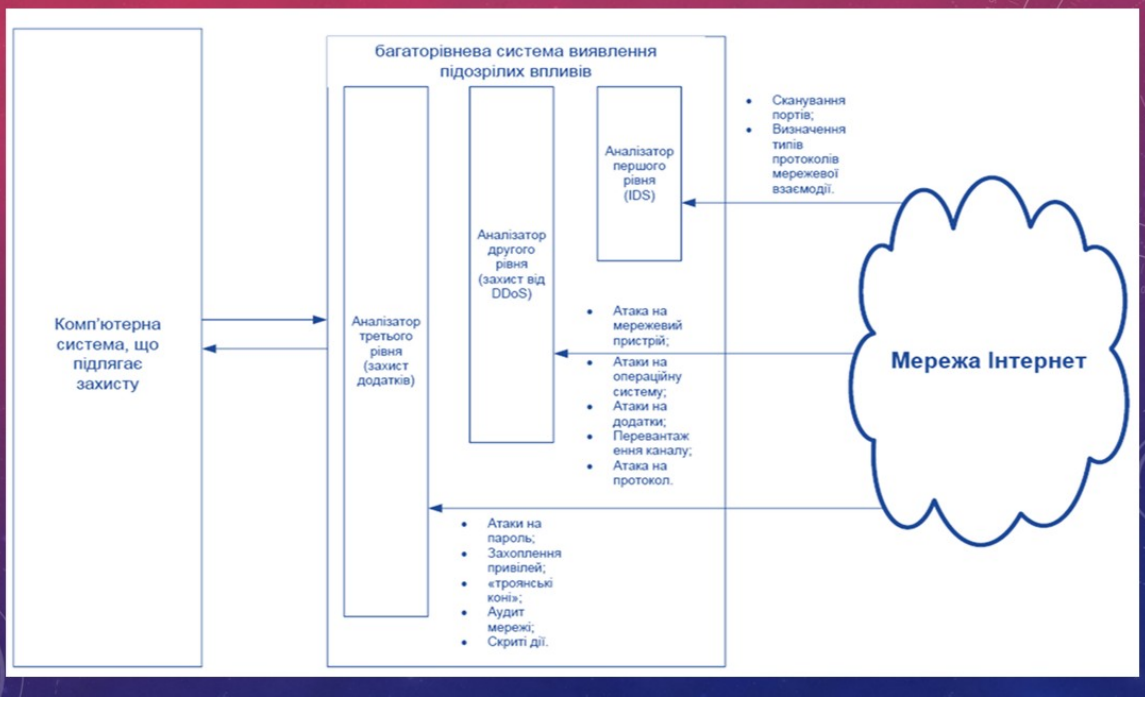
ID	Загроза	Захисний захід
1	Підробка (Spoofing)	Налаштування управління доступом.
2	Підробка (Spoofing)	Використання двофакторної автентифікації.
3	Прослуховування (Sniffing)	Впровадження криптографічного захисту даних.
4	Прослуховування (Sniffing)	Установлення систем для розпізнавання сниферів.
5	DoS-атака	Блокування шкідливих IP-адрес.
6	DoS-атака	Забезпечення високої пропускної здатності мережі.

Модель бази даних загроз інформаційним об'єктам

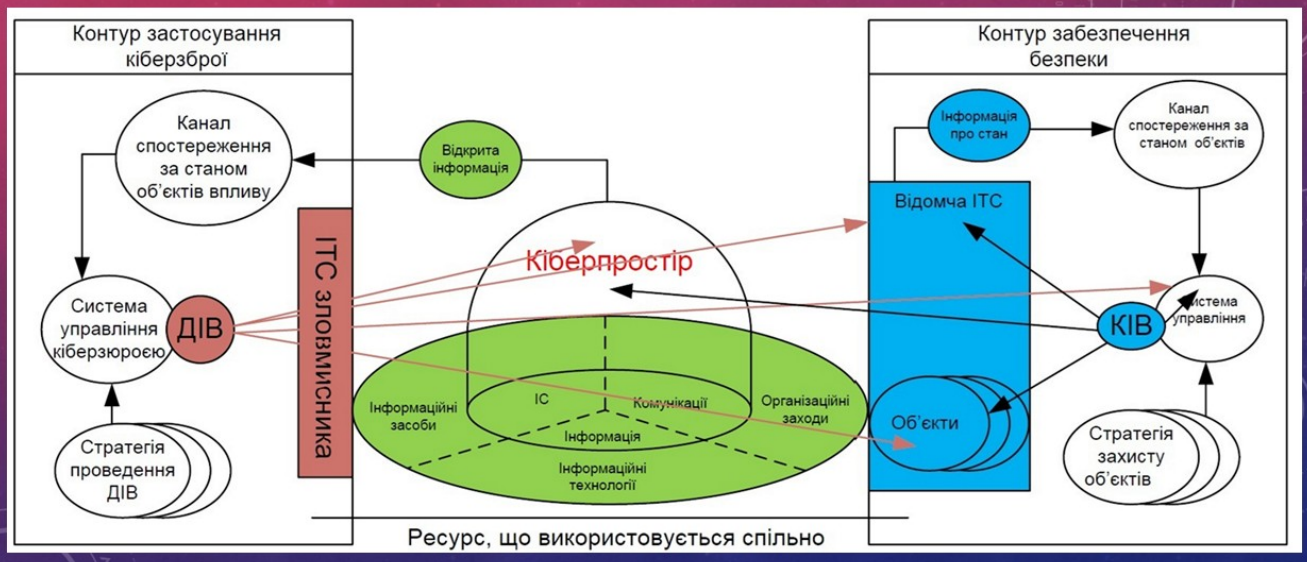


№	*Назва атрибуту*	*Фізичний формат*	*Опис*
1	Threats	TXT	Загрози
2	Properties	TXT	Характеристики інформації
3	Protection	TXT	Заходи захисту
4	Specifications	TXT	Тип документації
5	Thre_ID	BINARY	Унікальний ідентифікатор загрози
6	Prop_ID	BINARY	Унікальний ідентифікатор властивості
7	Prot_ID	BINARY	Ідентифікатор заходу захисту
8	Spec_ID	BINARY	Ідентифікатор характеристики загрози

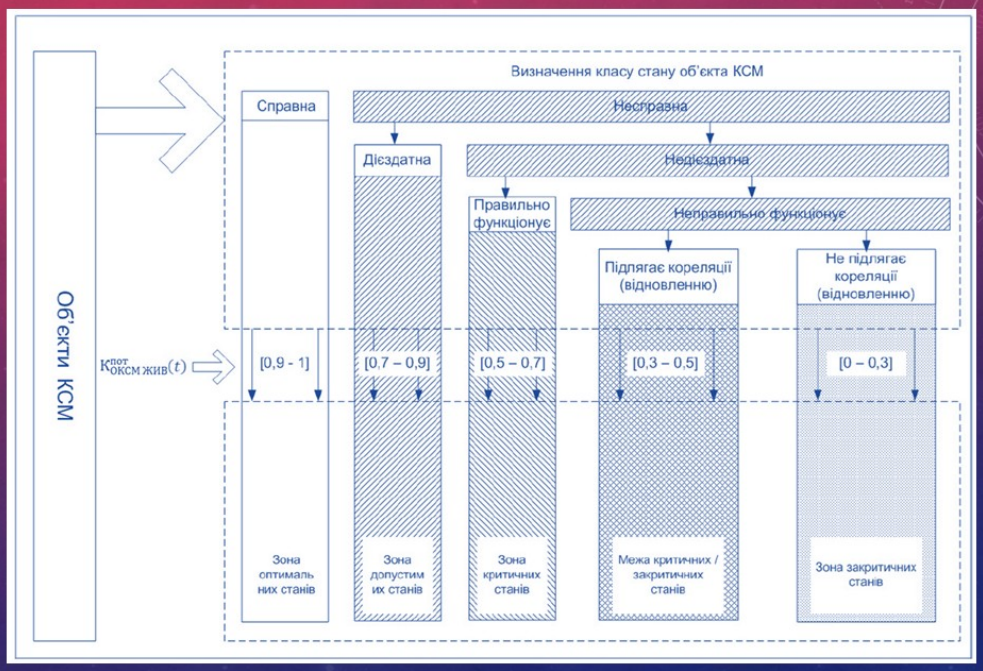
Структурна модель багаторівневої системи виявлення впливів

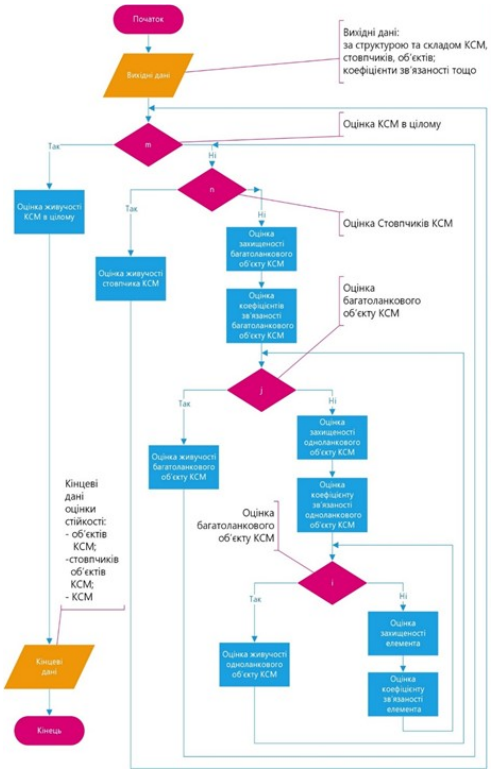


Контури забезпечення кібербезпеки та застосування кіберзброї



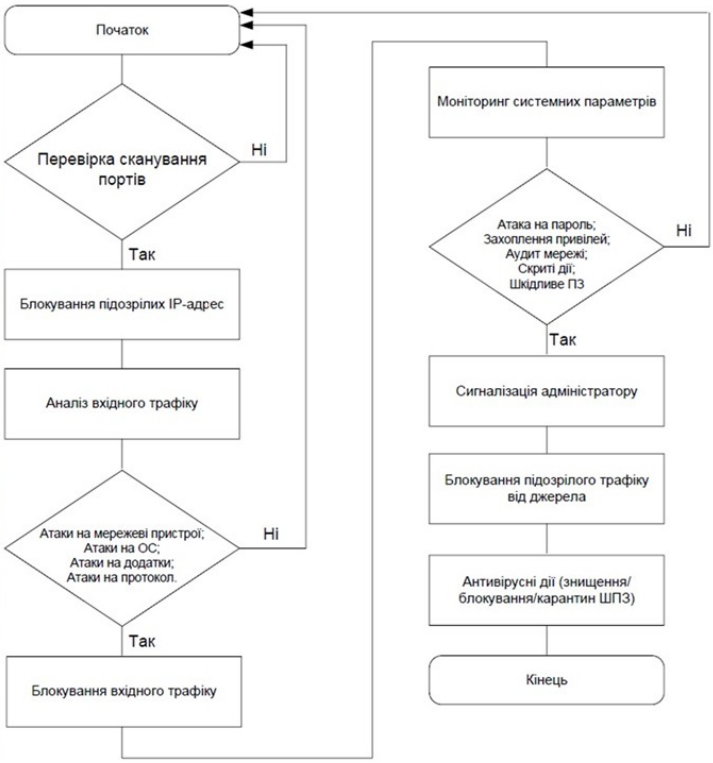
Класифікація стану об’єкта КСМ за рівнем живучості



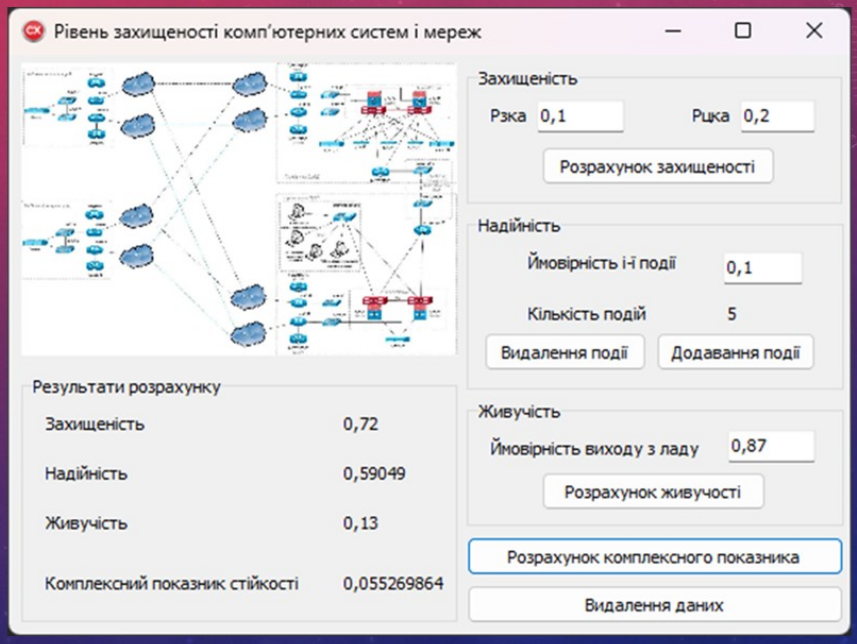


БСА методології оцінювання стійкості КСМ

БСА виявлення та нейтралізації кібератак на комп'ютерні системи та мережі



Розрахунок комплексного показника стійкості об’єктів КСМ



ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Чіркова Євгена Вікторовича

(прізвище, ім`я та по батькові)

Спеціальність *123 «Комп'ютерна інженерія»*

Освітньо-професійна програма *«Безпека комп'ютерних систем і мереж»*

Керівник дипломного проекту (роботи) *Кривченко Анастасія Анатоліївна*

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи) *Розробка програмної моделі оцінки рівня захищеності комп'ютерних систем і мереж*

Обсяг розрахунково-пояснювальної записки *76* сторінок

Обсяг графічної (презентаційної) частини *18* аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту завданню

Представлений дипломний проект відповідає затвердженій темі та виконаний відповідно технічному завданню. Дипломний проект присвячений створенню програмної моделі оцінки рівня стійкості комп'ютерних систем і мереж і складається з пояснювальної записки та мультимедійної презентації з відповідними схемами.

б) характеристика виконання кожного розділу дипломного проекту

Пояснювальна записка складається з основного розділу (Аналіз методів та засобів оцінки рівня стійкості комп'ютерних систем і мереж; Розробка моделі загроз інформаційним об'єктам у комп'ютерних системах і мережах; Розробка системи захисту інформації комп'ютерних систем і мереж; Розробка програмної моделі оцінки рівня стійкості комп'ютерних систем і мереж), економічного розділу, розділу охорони праці та додатків. Перелічені розділи поетапно охоплюють розробку, виконані докладно та обґрунтовано.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту

Графічна частина складається з 18 слайдів мультимедійної презентації, виконаної у програмному продукті MS PowerPoint, які містять структурні, принципові та функціональні схеми, структурні моделі, блок-схеми алгоритмів, передбачені технічним завданням. Пояснювальна записка виконана акуратно та у відповідності до норм. Якість виконання пояснювальної записки відмінна, розробку виконано у повному обсязі.

г) перелік позитивних якостей дипломного проекту *Реалізована програмна модель оцінки рівня стійкості КСМ виконує достатньо обгрунтований розрахунок надійності, захищеності та живучості. Передбачено події спуфінгу при визначенні показника надійності. Застосунок має зручний візуальний інтерфейс, дружній до користувача.*

д) основні недоліки дипломного проекту *Не передбачено масштабування зображення мережі у застосунку; Варто було б передбачити збереження результатів розрахунку у текстовий файл*

Оцінка розрахункової частини *Відмінно*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Відмінно*

Прізвище, ім'я, по батькові рецензента *к.т.н. Рудніченко Микола Дмитрович*

Місце роботи і посада рецензента *Національний університет «Одеська політехніка», доцент кафедри інформаційних технологій*

Підпис: _____

20 *червня* *2025 р.*

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Чіркова Євгена Вікторовича

(прізвище, ім`я та по батькові)

Спеціальність: *123 «Комп'ютерна інженерія»*

Освітня програма: *«Безпека комп'ютерних систем і мереж»*

Тема дипломного проекту: *Розробка програмної моделі оцінки рівня захищеності комп'ютерних систем і мереж*

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки) *Дипломний проект виконано відповідно технічному завданню. Пояснювальна записка до дипломного проекту містить 76 сторінок. У пояснювальній записці описано створення програмної моделі оцінки рівня стійкості комп'ютерних систем і мереж. Графічна частина складається з 18 слайдів, оформлених у вигляді презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та слайдів добра.*

б) самостійність роботи над проектом: *Протягом виконання дипломного проекту здобувач освіти Чірков Євген поступово та послідовно виконував всі етапи, проявив ініціативу в створенні загальної концепції та реалізації роботи. Всі роботи здобувач освіти виконував самостійно, з оглядом на рекомендації керівника.*

в) теоретична підготовка випускника (випускниці): *Здобувач освіти Чірков Євген під час роботи над дипломним проектом вивчив достатньо багато літературних та інтернет-джерел за даною тематикою.*

Вважаю, що теоретична підготовка дипломника достатня і він готовий до захисту проекту.

г) вміння розв'язувати виробничі та конструкторські питання *Під час виконання дипломного проекту здобувач освіти Чірков Євген показав вміння організовано працювати над поставленим завданням, застосовувати знання у сфері безпеки комп'ютерних систем і мереж, програмування, використовуючи сучасні комп'ютерні програмні засоби розробки, такі як Embarcadero RAD Studio.*

Оцінка розрахункової частини *Відмінно*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Відмінно*

Прізвище, ім'я, по батькові керівника дипломного проекту *Кривченко Анастасія Анатоліївна*

Місце роботи і посада керівника дипломного проекту *ВСП «Одеський технічний фаховий коледж ОНТУ», викладач спецдисциплін циклової комісії комп'ютерних технологій та програмної інженерії*

Підпис

«16» 06 2025 р.

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
(ДИПЛОМНОГО ПРОЕКТУ)
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Чірков Є.В.,
здобувач освіти гр. 4КБ-02, та

Кривченко А.А.,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до дипломного проекту фахового молодшого бакалавра на тему:

«Розробка програмної моделі оцінки рівня стійкості комп'ютерних систем і мереж» (автор роботи – Чірков Є.В., керівник роботи – Кривченко А.А.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2025 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи і даємо згоду на обробку персональних даних.

Виконавець _____ / Чірков Є.В. /

Керівник _____ / Кривченко А.А. /

«16» червня 2025 р.

ДОВІДКА

циклової комісії КТ та ПІ
про допуск до захисту дипломного проєкту
здобувача (здобувачки) освіти IV курсу
відділення комп'ютерних систем групи 4КБ-02

Чіркова Євгена Вікторовича

на тему *Розробка програмної моделі оцінки рівня стійкості комп'ютерних систем і мереж*

Висновок відповідальної особи за проведення нормоконтролю:
пояснювальна записка до дипломного проєкту виконана з несуттєвими порушеннями ДСТУ та оформлена відповідно до вимог Положення про дипломне проєктування

(підпис) *16.06.2025* (дата) *Петрашова В.І.* (П.І.Б.)

Висновок відповідальної особи за перевірку роботи на наявність академічного плагіату *згідно звіту про перевірку від 25.05.2025 р. значення коефіцієнту подібності в роботі становить 17,03%, коефіцієнт цитування – 1,39%.*

(підпис) *16.06.2025* (дата) *Краснокутська К.Г.* (П.І.Б.)

Попередня експертиза (малий захист) дипломного проєкту

здобувача (здобувачки) освіти *Чіркова Є.С.* (П.І.Б.)

проведена «*16*» *червня* 20*25* р.

Висновки *Пояснювальна записка до дипломного проєкту виконана у повному обсязі. Випускна кваліфікаційна робота (дипломний проєкт) відповідає вимогам Положення про дипломне проєктування та рекомендована до захисту.*

Голова ЦК КТ та ПІ (підпис) *Кривченко Ю.В.* (П.І.Б.)

StrikePlagiarism.com

Дата звіту 5/25/2025
Дата редагування 5/25/2025

Документ прийнятий

Звіт подібності

метадані

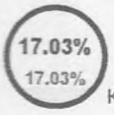
Назва організації
Odesa Technical Professional College of Odesa National University of Technology
Заголовок
Розробка програмної моделі оцінки рівня стійкості комп'ютерних систем і мереж

Автор
Чірков Євген Вікторович
Науковий керівник / Експерт
Кривченко Анастасія Анатоліївна

підрозділ
Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету"

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



КП 1

КЦ

25
Довжина фрази для коефіцієнта подібності 2

12728
Кількість слів

104421
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		42
Інтервали	A→	0
Мікропробіли	·	0
Білі знаки		0
Парафрази (SmartMarks)	a	70

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://card-file.ontu.edu.ua/server/api/core/bitstreams/ead3fa83-2e3d-4cd7-bfbd-1d5ed04c1ce4/content	103 0.81 %
2	https://card-file.ontu.edu.ua/bitstreams/53ed22ad-8700-4162-b97a-082a1ad472d6/download	86 0.68 %
3	https://card-file.ontu.edu.ua/server/api/core/bitstreams/ead3fa83-2e3d-4cd7-bfbd-1d5ed04c1ce4/content	67 0.53 %
4	https://card-file.ontu.edu.ua/server/api/core/bitstreams/ead3fa83-2e3d-4cd7-bfbd-1d5ed04c1ce4/content	57 0.45 %
5	https://card-file.ontu.edu.ua/bitstreams/b1c4b329-c3e8-4b5a-a1fc-ae232ec677bd/download	48 0.38 %

6	https://card-file.ontu.edu.ua/bitstreams/53ed22ad-8700-4162-b97a-082a1ad472d6/download	46 0.36 %
7	https://card-file.ontu.edu.ua/server/api/core/bitstreams/ead3fa83-2e3d-4cd7-bfbd-1d5ed04c1ce4/content	43 0.34 %
8	https://card-file.ontu.edu.ua/bitstreams/035f6436-20b4-4ee6-8e99-bede670e308b/download	42 0.33 %
9	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	38 0.30 %
10	https://card-file.ontu.edu.ua/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content	34 0.27 %

з домашньої бази даних (0.11 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Розробка оптоволоконної мережі для забезпечення надійного і високошвидкісного обміну даними між населеними пунктами [redacted] 5/22/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	14 (2) 0.11 %

з програми обміну базами даних (0.09 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Диплом Струк для проверкии.pdf [redacted] 12/22/2020 Odessa National Polytechnic University (УНІ, каф. підйомно-транспортного та робототехнічного обладнання)	7 (1) 0.05 %
2	2020_617200_Ryzhak_Andrii_Mykhailovych_87239 [redacted] 10/25/2024 National University "Lviv Politechnika" (National University Lviv Politechnika)	5 (1) 0.04 %

з Інтернету (16.82 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://card-file.ontu.edu.ua/bitstreams/1dff552d-7200-49b8-ae1d-ba76a1335685/download	**801 (69) 6.29 %**
2	https://card-file.ontu.edu.ua/server/api/core/bitstreams/ead3fa83-2e3d-4cd7-bfbd-1d5ed04c1ce4/content	**348 (10) 2.73 %**
3	https://card-file.ontu.edu.ua/bitstreams/53ed22ad-8700-4162-b97a-082a1ad472d6/download	**204 (10) 1.60 %**
4	https://card-file.ontu.edu.ua/bitstreams/b1c4b329-c3e8-4b5a-a1fc-ae232ec677bd/download	**79 (4) 0.62 %**
5	https://card-file.ontu.edu.ua/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content	**76 (6) 0.60 %**
6	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	**62 (4) 0.49 %**
7	https://card-file.ontu.edu.ua/bitstreams/035f6436-20b4-4ee6-8e99-bede670e308b/download	**56 (2) 0.44 %**
8	https://card-file.ontu.edu.ua/bitstreams/8999d5af-6274-44f4-ae78-d23e08048d38/download	50 (7) 0.39 %
9	https://card-file.ontu.edu.ua/bitstreams/82a6d375-2b69-4233-b80f-fbfd149b7747/download	**44 (3) 0.35 %**
10	http://cpsm.kpi.ua/stud/bak/DP_BAK_KARAULOVA_LU.pdf	**40 (2) 0.31 %**
11	https://card-file.ontu.edu.ua/server/api/core/bitstreams/995bdcec-4e4d-4321-8070-4d6badcb8e49/content	**39 (2) 0.31 %**

12	https://card-file.ontu.edu.ua/bitstreams/c58b0ff5-46e0-49f8-8cbe-65c32256665d/download	36 (3) 0.28 %
13	https://card-file.ontu.edu.ua/bitstreams/f292747f-f875-4858-906b-e14629f6ec57/download	34 (2) 0.27 %
14	https://card-file.ontu.edu.ua/bitstreams/bbed74c8-2ea7-44c5-8d00-0fe3fd9790ee/download	31 (3) 0.24 %
15	**https://card-file.ontu.edu.ua/bitstreams/5240e379-7721-49f0-8ee8-27140b0b473a/download**	**29 (1) 0.23 %**
16	https://card-file.ontu.edu.ua/server/api/core/bitstreams/4bb7255e-46d4-4349-9726-9698476da02d/content	27 (4) 0.21 %
17	https://card-file.ontu.edu.ua/bitstreams/21173711-5b67-4b87-b17f-6302c25e7a31/download	27 (4) 0.21 %
18	http://mumk-oop.narod.ru/Images/posobie/glava10.htm	26 (3) 0.20 %
19	https://card-file.ontu.edu.ua/server/api/core/bitstreams/a141b658-5fa7-4f90-b0bd-7f0ccaed21e5/content	25 (2) 0.20 %
20	https://www.amazon.com/Designing-Audio-Effect-Plug-Ins-Processing/dp/0240825152?tag=askcomdelta-20	23 (2) 0.18 %
21	https://card-file.ontu.edu.ua/bitstreams/29489599-0581-4ce6-8890-c3b13d9f2e0e/download	20 (1) 0.16 %
22	http://www.100balov.com/data23/ukr/Materialij_po_navchannu_pakynok_12/Zavdannyana_1_lijst.php	15 (3) 0.12 %
23	https://card-file.ontu.edu.ua/bitstreams/62baa43e-b968-4993-bb54-8cf8761a89b2/download	12 (1) 0.09 %
24	https://card-file.ontu.edu.ua/bitstreams/bbaf3f38-16a8-4070-bead-5562769b7c71/download	10 (2) 0.08 %
25	https://card-file.ontu.edu.ua/bitstreams/34a6756b-592f-4b77-a805-183aa03a6a26/download	9 (1) 0.07 %
26	https://card-file.ontu.edu.ua/bitstreams/e4afae26-0a7e-4a4d-afc2-94341838de2a/download	8 (1) 0.06 %
27	https://ohoronapraci.com.ua/articles/666201-vydy-medychnykh-ohlyadiv-pratsivnykiv	5 (1) 0.04 %
28	https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download	5 (1) 0.04 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: «Безпека комп'ютерних систем і мереж»
Група: 4КБ- 02

Дипломний проект
здобувача освіти денної форми навчання
КБ.02.23.000.ДП

ЧІРКОВА
ЄВГЕНА ВІКТОРОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: «Безпека комп'ютерних систем і мереж»