Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Коваля Олександра В'ячеславовича

на здобуття ступеня вищої освіти Бакалавра

Штучна імуна система для захисту інформаційно-комунікаційної мережі.

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ. 220240.22.02.27 ПЗ

Виконав студент 4 курсу група КБ-22-2 Олександр КОВАЛЬ
Керівник канд. техн. наук, доцент Віра ТІТОВА
Нормоконтролер д-р філософії Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

8 06 2026 р.

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

09 лютого 2026 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ковалю Олександру В'ячеславовичу

1 Тема роботи Штучна імуна система для захисту інформаційно-комунікаційної мережі.

Керівник роботи к.т.н. доцент Віра Тітова

Затверджено наказом ректора університету від 9 лютого 2026 № 19

2 Строк подання студентом кваліфікаційної роботи на кафедру 25 травня 2026

3 Вихідні дані до роботи Проаналізувати сучасний стан кібербезпеки в гетерогенних мережевих середовищах. Дослідити класифікацію мережевих загроз та проаналізувати обмеження традиційних систем виявлення вторгнень. Сформулювати концептуальні засади застосування імунологічної парадигми та здійснити постановку задачі. Визначити функціональні та архітектурні вимоги до системи виявлення мережевих аномалій. Змоделювати архітектуру розподіленої мережі інтелектуальних агентів-детекторівПровести порівняльний аналіз та теоретичну оцінку ефективності запропонованої концептуальної моделі.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз сучасного стану кібербезпеки в гетерогенних мережевих середовищах. Опис логіки процесів ідентифікації та нейтралізації DDoS-атак і мережевих аномалій. Архітектурна взаємодія імунної системи з класичними засобами моніторингу безпеки (SIEM, Firewall). Порівняльний аналіз та теоретична оцінка ефективності запропонованої моделі. Загальні висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Схема архітектури розподіленої мультигеної системи. Блок-схема логіки роботи негативного відбору (NSA) та логічна модель обробки конкретних сигналів агентом-координатором. Архітектура програмного прототипу імунної системи.

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 09 лютого 2026 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Травень	
Захист КР	Червень	

Студент _____ Олександр КОВАЛЬ

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

АНОТАЦІЯ

Тема кваліфікаційної роботи: Штучна імуна система для захисту інформаційно-комунікаційної мережі.

Автор роботи: Коваль Олександр В'ячеславович.

Керівник роботи: Тітова Віра Юріївна.

Пояснювальна записка: 70 с., 1 додатків, 9 рисунків, 48 джерел.

Графічна частина: 3 плакати.

Ключові слова: кібербезпека, штучна імунна система, мультиагентна система, виявлення аномалій, теорія небезпеки, алгоритм негативного відбору, ddos-атака.

Кваліфікаційна робота бакалавра присвячена розробці та теоретичному обґрунтуванню концептуальної архітектури розподіленої штучної імунної системи для підвищення ефективності моніторингу трафіку та виявлення аномалій у гетерогенних мережевих середовищах.

У роботі проведено комплексний аналіз обмежень традиційних сигнатурних та статистичних систем виявлення вторгнень, розглянуто основні мережеві загрози в гетерогенних середовищах. Досліджено концептуальні засади застосування імунологічної парадигми в кіберзахисті. Розроблено концептуальну модель розподіленої мультиагентної системи моніторингу, сформовано алгоритмічні основи генерації детекторів та розроблено сценарії адаптації системи на основі теорії небезпеки для мінімізації рівня хибних спрацювань. Описано схему архітектурної взаємодії розробленої імунної моделі з класичними засобами безпеки (Firewall, SIEM). Запропоноване рішення може бути використане архітекторами з кібербезпеки та системними адміністраторами для побудови проактивних контурів захисту, здатних ефективно протистояти невідомим атакам нульового дня та динамічно адаптуватися до змін інфраструктури.

28.05.2026 _____

ABSTRACT

Theme of the qualification work: Artificial immune system for protecting information and communication networks.

Author of the work: Koval Oleksandr Vyacheslavovych.

Advisor: Titova Vira Yurievna.

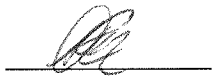
Explanatory note: 70 p., 1 appendices, 9 figures, 48 references.

Graphic part: 3 posters.

Keywords: cybersecurity, artificial immune system, multi-agent system, anomaly detection, danger theory, negative selection algorithm, ddos attack.

The bachelor's qualification work is dedicated to the development and theoretical justification of the conceptual architecture of a distributed artificial immune system to improve the efficiency of traffic monitoring and anomaly detection in heterogeneous network environments.

The work provides a comprehensive analysis of the limitations of traditional signature-based and anomaly-based intrusion detection systems and reviews the main network threats in heterogeneous environments. The conceptual foundations of applying the immunological paradigm in cyber defense have been investigated. A conceptual model of a distributed multi-agent monitoring system has been developed, the algorithmic foundations of detector generation have been formed, and system adaptation scenarios based on danger theory have been developed to minimize the false positive rate. The scheme of architectural interaction of the developed immune model with classical security tools (Firewall, SIEM) is described. The proposed solution can be used by cybersecurity architects and system administrators to build proactive defense perimeters capable of effectively resisting unknown zero-day attacks and dynamically adapting to infrastructure changes.

28.05.2026 

ЗМІСТ

ВСТУП

Актуальність теми зумовлена тим, що сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням масштабу та складності корпоративних мереж. Перехід до гетерогенних середовищ, використання хмарних сервісів, технологій віртуалізації та віддаленого доступу призвели до розмиття класичного мережевого периметра. Разом із цим безперервно еволюціонують і методи кібератак: зловмисники активно використовують поліморфне шкідливе програмне забезпечення, інтелектуальні ботнети та розподілені атаки на відмову в обслуговуванні (DDoS), здатні обходити традиційні засоби захисту.

Класичні системи виявлення вторгнень (IDS), що базуються на сигнатурному аналізі, ефективно блокують лише відомі загрози, залишаючись вразливими до атак нульового дня (Zero-Day). Альтернативні статистичні системи, які шукають відхилення від норми, генерують надмірну кількість хибних спрацювань (False Positives) в умовах мінливого легітимного трафіку, що критично перевантажує адміністраторів безпеки. У зв'язку з цим виникає гостра практична потреба у впровадженні нових, адаптивних методів моніторингу. Одним із найбільш перспективних напрямів розв'язання цієї прикладної задачі є використання імунологічної парадигми — перенесення принципів роботи біологічної імунної системи (розподіленість, самонавчання, здатність відрізняти своє від чужого) у сферу кібербезпеки. Розробка прикладної системи моніторингу на основі програмних агентів-детекторів дозволяє створити гнучкий контур захисту, який масштабується разом з інфраструктурою підприємства.

Метою роботи є розробка та обґрунтування концептуальної архітектури й програмно-технологічних рішень розподіленої штучної імунної системи для підвищення ефективності моніторингу трафіку та виявлення аномалій у сучасних гетерогенних мережах.

Для досягнення поставленої мети були сформульовані наступні завдання роботи:

– проаналізувати принципи функціонування мультиагентних систем та існуючі методи виявлення мережевих аномалій;

– дослідити класифікацію мережевих загроз та визначити обмеження традиційних засобів виявлення вторгнень;

– сформувати вимоги та спроєктувати архітектуру розподіленої імунної системи моніторингу трафіку;

– адаптувати логіку алгоритмів негативного відбору, клональної селекції та теорії небезпеки для практичного розпізнавання шкідливого трафіку і зниження рівня хибних тривог;

– запропонувати програмно-технологічну реалізацію прототипу системи та описати механізми її інтеграції з класичними засобами безпеки (Firewall, SIEM);

– провести теоретичну оцінку та порівняльний аналіз розробленої системи з існуючими рішеннями.

Об’єктом дослідження є процеси виявлення та нейтралізації кіберзагроз у сучасних гетерогенних інформаційно-комунікаційних мережах.

Предметом дослідження виступають методи, алгоритми та архітектурні рішення штучних імунних систем для моніторингу мережевого трафіку.

Практичне значення одержаних результатів полягає у формуванні готового базису для розгортання адаптивних систем кіберзахисту в реальних корпоративних мережах на основі запропонованої архітектурної моделі та програмно-технологічної реалізації прототипу. Застосування розробленої системи дозволяє адміністраторам безпеки автоматизувати процес виявлення невідомих атак, мінімізувати час реакції на інциденти завдяки взаємодії з міжмережевими екранами, а також значно знизити навантаження на аналітиків SOC (Security Operations Center) за рахунок попередньої фільтрації хибних спрацювань перед передачею даних до SIEM-систем.

1 ДОСЛІДЖЕННЯ МЕТОДІВ ШТУЧНОГО ІМУНІТЕТУ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ

1.1 Теоретичні основи побудови та функціонування мультиагентних систем

Розвиток сучасних інформаційних технологій та ускладнення обчислювальних мереж вимагають переходу від централізованих монолітних програмних рішень до гнучких, розподілених та інтелектуальних архітектур. Однією з найбільш ефективних парадигм для вирішення складних розподілених задач є концепція мультиагентних систем (Multi-Agent Systems, MAS), яка базується на використанні автономних програмних сутностей — агентів [1].

З точки зору штучного інтелекту та програмної інженерії, програмний агент — це обчислювальна система, що знаходиться в певному середовищі та здатна до автономних дій у ньому для досягнення поставлених цілей [2]. На відміну від звичайних програм (об'єктів), які пасивно очікують виклику своїх методів, агенти володіють власним потоком управління і самостійно приймають рішення щодо ініціації тих чи інших дій.

Для того щоб програмний модуль класифікувався як інтелектуальний агент, він повинен володіти наступними базовими властивостями [3]:

- автономність (Autonomy): здатність функціонувати без постійного прямого втручання людини або інших систем, маючи контроль над власним внутрішнім станом і поведінкою;
- реактивність (Reactivity): здатність сприймати стан навколишнього середовища (через віртуальні сенсори) та своєчасно реагувати на його зміни (через ефектори);
- проактивність (Proactiveness): здатність не лише реагувати на зовнішні події, але й генерувати цілеспрямовану поведінку, проявляючи ініціативу для виконання закладеної логіки;
- соціальна здатність (Social ability): можливість взаємодіяти, обмінюватися даними та координувати свої дії з іншими агентами (або людьми) за допомогою спеціалізованих мов спілкування агентів (наприклад, ACL — Agent

Communication Language) [4].

Окремий програмний агент має обмежені обчислювальні ресурси та локальне бачення середовища. Тому для розв'язання глобальних задач (таких як моніторинг великої корпоративної мережі) створюються мультиагентні системи. MAS являє собою сукупність кількох взаємодіючих інтелектуальних агентів, які об'єднують свої зусилля для досягнення спільної мети, що виходить за межі можливостей кожного окремого агента [5].

Головною перевагою MAS є емерджентність: глобальна інтелектуальна поведінка системи формується як результат локальних взаємодій множини простих агентів. Коли кілька агентів працюють разом, вони формують кооперативну мережу. Процес їхньої спільної роботи включає [6]:

– розподіл задач: глобальне завдання розбивається на підзадачі (наприклад, кожен локальний агент моніторить лише свій сегмент мережі або свій вузол);

– обмін даними: агенти транслюють інформацію про виявлені події (наприклад, знайдена аномалія або зміна конфігурації) своїм сусідам або спеціалізованим вузлам;

– координацію рішень: узгодження дій для уникнення конфліктів та формування консолідованої відповіді (наприклад, агрегація даних з кількох вузлів для підтвердження розподіленої DDoS-атаки).

У контексті забезпечення кібербезпеки та моніторингу мереж застосування MAS є концептуально виправданим. Сучасні комп'ютерні мережі за своєю природою є розподіленими системами. Використання єдиного централізованого аналізатора трафіку створює "пляшкове горло" (bottleneck) для продуктивності та єдину точку відмови (Single Point of Failure) [7]. Натомість, впровадження ієрархічної мультиагентної моделі дозволяє розмістити локальні агенти безпосередньо на кінцевих вузлах для первинного збору даних, агенти пам'яті — для зберігання сигнатур, а агенти-координатори — для контекстного аналізу та прийняття глобальних рішень [8].

Така розподілена взаємодія гарантує високу живучість: навіть якщо частина агентів буде скомпрометована або знищена зловмисником, решта системи

продовжить функціонувати, обмінюватися даними та ізолювати загрозу. Загальну логіку взаємодії агентів у середовищі наведено на рис. 1.1.

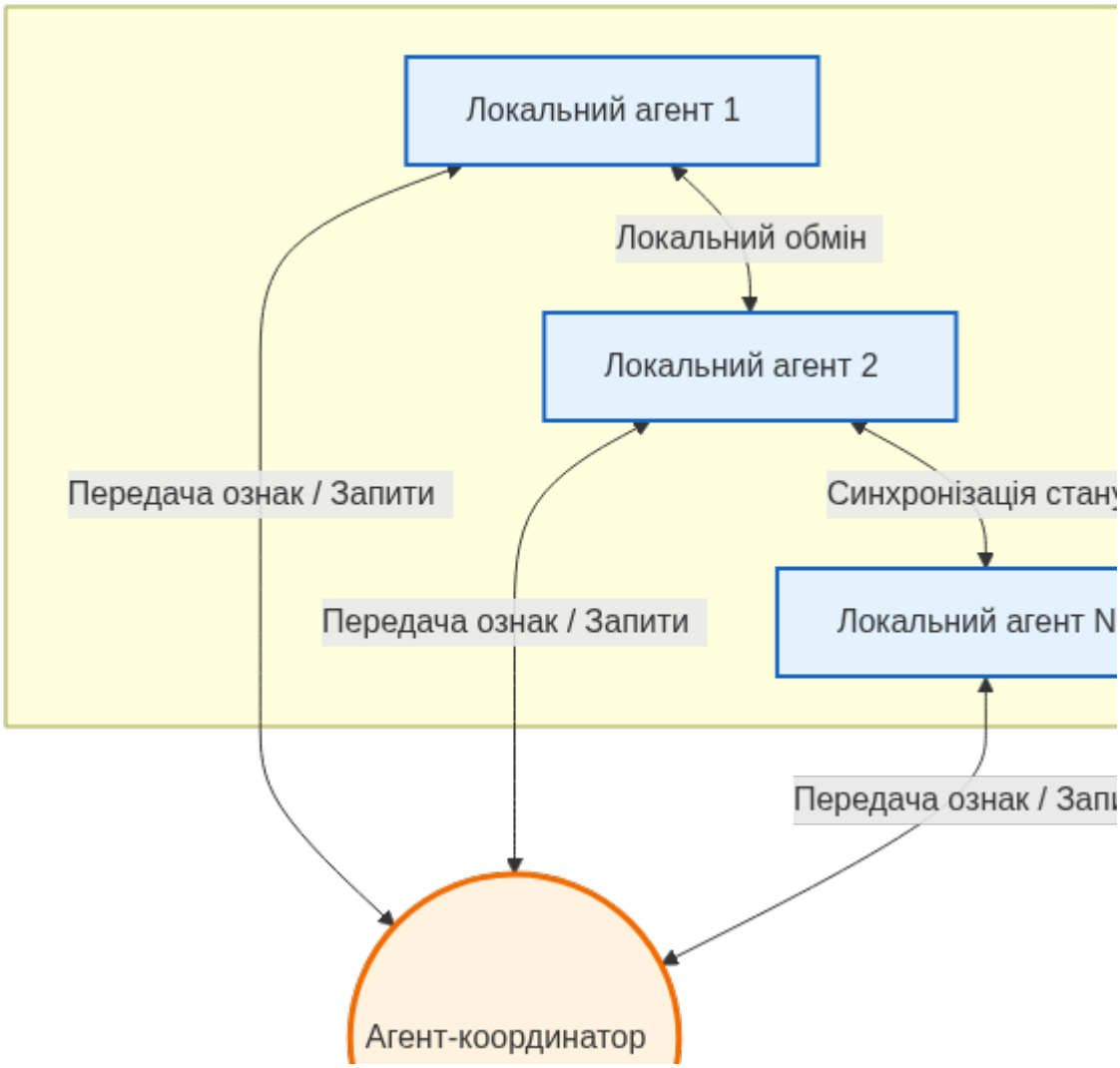


Рисунок 1.1 — Загальна логічна структура взаємодії в мультиагентній системі

Для повноцінного розуміння механізмів роботи мультиагентних систем необхідно детальніше розглянути внутрішню структуру самих інтелектуальних агентів. У сучасній теорії штучного інтелекту виділяють три основні архітектурні моделі побудови агентів, кожна з яких має свої переваги при вирішенні специфічних завдань у сфері кібербезпеки:

1. Реактивні архітектури (Reactive architectures). Такі агенти не мають складної внутрішньої моделі навколишнього середовища та не зберігають довгострокову історію станів. Їхня поведінка базується на принципі «стимул-

реакція» (stimulus-response), тобто на наборі продукційних правил виду «ЯКЩО виявлено умову X, ТОДІ виконати дію Y». У контексті мережевого захисту реактивні агенти ідеально підходять для ролі локальних сенсорів або ефекторів на кінцевих вузлах, де вимагається мінімальна затримка реагування (наприклад, миттєве блокування порту при виявленні специфічного TCP-флуду). Основна перевага — швидкодія та низькі вимоги до обчислювальних ресурсів.

2. Деліберативні архітектури (Deliberative architectures). На відміну від реактивних, ці агенти володіють внутрішньою моделлю світу і здатні до логічного висновку та цілеспрямованого планування. Найбільш відомою моделлю цього типу є BDI-архітектура (Belief-Desire-Intention — Переконання-Бажання-Наміри). «Переконання» відображають знання агента про поточний стан мережі; «Бажання» — глобальні цілі (наприклад, підтримка доступності сервера); «Наміри» — конкретні плани дій, вибрані для реалізації бажань. Такі агенти виконують роль координаторів: вони здатні аналізувати складні багатоетапні атаки (APT), корелювати події від різних реактивних агентів і формувати стратегію захисту.

3. Гібридні архітектури (Hybrid architectures). Поєднують у собі реактивний та деліберативний компоненти. Гібридний агент має нижній (реактивний) рівень для швидкого реагування на критичні загрози та верхній (деліберативний) рівень для довгострокового аналізу та адаптації. Саме гібридна архітектура є найдоцільнішою для розробки повноцінних агентів-детекторів у складі штучних імунних систем.

Надзвичайно важливим аспектом функціонування MAS є забезпечення інтероперабельності — здатності агентів коректно розуміти один одного. Оскільки гетерогенна мережа може включати агентів, написаних різними мовами програмування або розгорнутих на різних платформах, їхня взаємодія повинна базуватися на загальноприйнятих стандартах. Найбільш поширеним стандартом є специфікація FIPA (Foundation for Intelligent Physical Agents), яка визначає мову комунікації агентів ACL (Agent Communication Language).

Повідомлення у форматі FIPA-ACL складається з комунікативного акту

(наприклад, INFORM — передача інформації про аномалію, REQUEST — запит на зміну конфігурації фаєрвола, PROPOSE — пропозиція ізолювати підмережу) та безпосереднього вмісту. Для того щоб вміст повідомлення трактувався всіма агентами однаково, мультиагентна система використовує спільні онтології — формалізовані словники понять предметної області (наприклад, чітке визначення атрибутів мережевого пакета, типів загроз, рівнів критичності). Онтологічний підхід дозволяє агенту-координатору безпомилково агрегувати дані від сенсорів різних типів (IDS, Firewall, антивірусних агентів).

Окрім архітектури самих агентів, ефективність MAS критично залежить від обраної топології їхньої організації в мережі. За принципом розподілу управління виділяють три базові топології:

– Централізована (Зіркоподібна): Усі локальні агенти (сенсори) передають зібрану інформацію єдиному центральному агенту-аналітику. Недоліком є створення єдиної точки відмови та перевантаження центрального вузла при зростанні обсягів трафіку.

– Децентралізована (Peer-to-Peer): Кожен агент рівноправно спілкується з іншими агентами-сусідами. Система має максимальну живучість, оскільки вихід з ладу будь-якого вузла не зупиняє роботу системи. Однак досягнення глобального консенсусу (наприклад, визначення факту розподіленої атаки) у такій топології потребує складних алгоритмів синхронізації та генерує значний службовий трафік.

– Ієрархічна (Кластерна): Компромісний варіант, що найчастіше застосовується у корпоративному сегменті. Локальні агенти об'єднуються в кластери (наприклад, за географічним принципом або в межах одного VLAN). Кожен кластер має свого локального координатора, який агрегує дані та передає їх на вищий рівень — головному агенту-координатору. Це дозволяє ефективно масштабувати систему та мінімізувати навантаження на канали зв'язку.

Ще однією інноваційною характеристикою, яку дозволяють реалізувати мультиагентні технології, є мобільність коду. Мобільні агенти (Mobile Agents) — це спеціалізовані програмні процеси, які здатні призупиняти своє виконання на

одному мережевому вузлі, переміщувати свій код і збережений стан на інший вузол, і продовжувати роботу там. У парадигмі класичного клієнт-серверного моніторингу дані пересилаються до аналітичного центру (Data to Code). У парадигмі мобільних агентів код переміщується безпосередньо до джерела даних (Code to Data). Якщо система фіксує підозрілу активність на віддаленому сервері з низькою пропускною здатністю каналу зв'язку, агент-координатор може відправити туди мобільного агента-детектора. Мобільний агент проведе глибокий локальний аналіз логів та процесів, не завантажуючи мережу передачею терабайтів сирих даних, і повернеться лише з готовим висновком (наприклад, підтвердженням зараження).

Підсумовуючи, мультиагентні системи надають гнучкий, масштабований та інтелектуальний базис для створення сучасних засобів кіберзахисту. Використання реактивно-деліберативних архітектур, ієрархічних топологій управління та стандартизованих протоколів комунікації дозволяє перетворити статичну систему моніторингу на динамічне та адаптивне середовище. Саме ці властивості роблять MAS ідеальним архітектурним фундаментом для реалізації алгоритмів штучних імунних систем, розгляд яких є наступним логічним кроком у побудові комплексної моделі виявлення аномалій.

1.2 Базові принципи та методи виявлення аномалій у мережевому трафіку

Фундаментальною задачею будь-якої системи моніторингу інформаційної безпеки є поділ мережевих подій на легітимні (безпечні) та шкідливі. У контексті систем виявлення вторгнень (Intrusion Detection Systems, IDS) цей процес найчастіше реалізується через дві основні парадигми: сигнатурний аналіз (виявлення відомих загроз) та аналіз аномалій (пошук відхилень від норми) [9]. Оскільки сучасні кібератаки стають все більш поліморфними та цілеспрямованими, саме методи виявлення аномалій (Anomaly-based IDS, AIDS) набувають критичного значення.

Для розуміння принципів роботи таких систем необхідно чітко розмежувати базові поняття:

– нормальний (легітимний) трафік — це сукупність мережевих пакетів та з'єднань, що генеруються в результаті штатного функціонування інформаційної інфраструктури, дій авторизованих користувачів та легального програмного забезпечення;

– аномальний трафік — це будь-яка мережева активність, параметри якої (обсяг, частота, структура пакетів, послідовність звернень до портів) суттєво відхиляються від встановленого профілю нормальної поведінки [10].

Процес виявлення аномалій зазвичай складається з двох етапів. На першому етапі (фаза навчання) система протягом певного часу збирає статистику та будує еталонний профіль нормальної поведінки мережі (Baseline). Аналізуються такі метрики, як середня пропускна здатність, типові IP-адреси призначення, співвідношення протоколів (TCP/UDP/ICMP) та час активності користувачів [11]. На другому етапі (фаза моніторингу) поточний трафік у реальному часі порівнюється з еталонним профілем за допомогою статистичних методів, алгоритмів машинного навчання або евристичних правил. Якщо рівень відхилення перевищує заданий поріг, система генерує сигнал тривоги.

Головною проблемою традиційних систем виявлення аномалій є високий рівень хибних спрацювань (False Positives). Це пов'язано з тим, що "нормальний" стан корпоративної мережі не є статичним; він постійно еволюціонує. Виникнення хибних тривог найчастіше провокується такими легітимними подіями [12]:

– встановлення нового програмного забезпечення або оновлення операційних систем (що викликає нетиповий сплеск трафіку);

– зміна мережевої архітектури або додавання нових підмереж;

– легітимні пікові навантаження (наприклад, масове підключення користувачів на початку робочого дня або створення резервних копій баз даних).

Система, що не володіє контекстним розумінням ситуації (Context Awareness), класифікує будь-яке значне відхилення як атаку, що призводить до

інформаційного перевантаження адміністраторів (Alert Fatigue) та знижує загальну ефективність захисту [13].

Для об'єктивної оцінки ефективності систем виявлення аномалій у теорії кібербезпеки використовується матриця помилок (Confusion Matrix), яка оперує чотирма базовими станами [14]:

- TP (True Positive) — Істинно позитивні: система правильно ідентифікувала реальну атаку.
- TN (True Negative) — Істинно негативні: система правильно проігнорувала нормальний трафік.
- FP (False Positive) — Хибно позитивні (Хибна тривога): система класифікувала легітимний трафік як атаку.
- FN (False Negative) — Хибно негативні (Пропуск атаки): система не помітила реальну загрозу, вважаючи її нормальним трафіком.

На основі цих базових показників розраховуються ключові метрики оцінки роботи системи [15]:

– Точність (Accuracy): Частка правильно класифікованих подій (як нормальних, так і аномальних) відносно загальної кількості подій і обчислюється за формулою (1.1):

$$Accurancy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1.1}$$

– Рівень виявлення (Detection Rate / True Positive Rate) показує, яку частку реальних атак система здатна виявити, тобто відображає чутливість системи згідно з виразом (1.2):

$$DR = \frac{TP}{TP + FN} \tag{1.2}$$

– Рівень хибних тривог (False Positive Rate) відображає відсоток легітимного трафіку, який був помилково заблокований або ідентифікований як загроза, і розраховується за формулою (1.3):

$$FPR = \frac{FP}{FP + TN} \tag{1.3}$$

Ідеальна система захисту повинна максимізувати рівень виявлення (DR →1) та мінімізувати рівень хибних тривог (FPR → 0). Однак на практиці між цими метриками існує зворотна залежність: підвищення чутливості системи для виявлення прихованих атак неминуче призводить до зростання кількості хибних спрацювань. Подолання цього фундаментального обмеження є головним мотиваційним чинником для дослідження та розробки інтелектуальних біоінспірованих алгоритмів захисту, зокрема штучних імунних систем.

1.3 Аналіз сучасного стану кібербезпеки в гетерогенних мережевих середовищах

Сучасний етап розвитку інформаційних технологій характеризується тотальною конвергенцією різнорідних обчислювальних ресурсів у межах єдиної інформаційно-комунікаційної інфраструктури. Гетерогенні мережеві середовища, що поєднують у собі різне апаратне забезпечення (маршрутизатори, комутатори, сервери), різноманітні операційні системи (Windows, Linux, мобільні платформи, такі як iOS та Android) та велику кількість кінцевих пристроїв (від робочих станцій до засобів інтернету речей — IoT), стали стандартом для сучасних підприємств та організацій [16].

Ключовою особливістю таких середовищ є їхня структурна складність та висока динамічність. Використання обладнання від різних виробників та впровадження хмарних сервісів значно розширює ландшафт потенційних кіберзагроз. Кожен тип пристрою або мережевого протоколу може мати власні специфічні вразливості, що робить процес централізованого управління безпекою надзвичайно складним завданням. Крім того, активне використання концепцій віддаленої роботи та власних пристроїв співробітників (BYOD) призвело до розмивання традиційного периметра мережі, надаючи зловмисникам нові вектори

для несанкціонованого проникнення [17].

Гіперконнективність сучасних інформаційно-комунікаційних систем зумовила фундаментальний зсув у парадигмі побудови мережевої архітектури. Класична периметральна модель захисту, яку можна порівняти із «замком та ровом» (Castle-and-Moat), де довіра автоматично надавалася всім суб'єктам всередині корпоративної мережі, остаточно втратила свою релевантність. Замість неї домінуючою стає концепція архітектури нульової довіри (Zero Trust Architecture, ZTA). У гетерогенному середовищі, де користувач може автентифікуватися з особистого смартфона через публічну Wi-Fi мережу для доступу до корпоративної бази даних у публічній хмарі, принцип «ніколи не довіряй, завжди перевіряй» стає єдиним ефективним механізмом забезпечення конфіденційності. Zero Trust вимагає безперервної автентифікації та мікросегментації мережі, що, у свою чергу, генерує колосальні обсяги телеметричних даних та службового трафіку, які потребують постійного моніторингу в режимі реального часу.

Важливим фактором ускладнення гетерогенних середовищ є масова інтеграція пристроїв Інтернету речей (Internet of Things, IoT) та Промислового Інтернету речей (Industrial IoT, IIoT). На відміну від традиційних робочих станцій, IoT-пристрої часто характеризуються обмеженими обчислювальними потужностями, що унеможливлює встановлення на них повноцінних криптографічних засобів захисту чи локальних антивірусних агентів. Крім того, виробники такого обладнання нерідко ігнорують принципи "Security by Design", залишаючи вбудовані вразливості, дефолтні паролі та відкриті порти. У результаті IoT-сегмент стає найслабшою ланкою інфраструктури, перетворюючись на ідеальний плацдарм для формування масштабних ботнетів та проведення транзитних атак на критичні вузли корпоративної мережі.

Зміна ландшафту також тісно пов'язана з еволюцією підходів до розробки та розгортання програмного забезпечення. Перехід від монолітних додатків до мікросервісної архітектури та контейнеризації (наприклад, використання Docker та систем оркестрації Kubernetes) радикально змінив топологію мережевого

трафіку. Якщо раніше основний потік даних рухався за вектором «північ-південь» (від клієнта до сервера через граничний маршрутизатор), то сьогодні до 80% трафіку в центрах обробки даних є трафіком типу «схід-захід» (обмін даними між внутрішніми мікросервісами, віртуальними машинами та контейнерами). Традиційні апаратні міжмережеві екрани, встановлені на межі мережі, фізично не здатні інспектувати цей внутрішній трафік, що створює великі «сліпі зони» (blind spots) для адміністраторів безпеки. Зловмисник, якому вдалося скомпрометувати хоча б один низькопривілейований контейнер, отримує можливість безперешкодно переміщуватися всередині інформаційного середовища (Lateral Movement), оминаючи зовнішні контури захисту.

Технологічною відповіддю на потребу гнучкого управління такими складними середовищами стала поява програмно-конфігурованих мереж (Software-Defined Networking, SDN) та віртуалізації мережевих функцій (Network Function Virtualization, NFV). SDN відокремлює площину управління (Control Plane) від площини передачі даних (Data Plane), централізуючи логіку маршрутизації в єдиному програмному контролері. Хоча це значно спрощує адміністрування та дозволяє динамічно перерозподіляти ресурси, централізований контролер стає єдиною точкою відмови (Single Point of Failure) та високопріоритетною ціллю для кібератак. Компрометація SDN-контролера означає повну втрату контролю над усією мережевою інфраструктурою підприємства.

Не менш критичним аспектом є криптографічне затінення загроз. Згідно зі статистикою провідних аналітичних центрів, понад 90% сучасного інтернет-трафіку є зашифрованим (з використанням протоколів TLS 1.3, HTTPS тощо). З одного боку, наскрізне шифрування (End-to-End Encryption) є базовою вимогою для захисту даних від перехоплення. З іншого боку, шифрування стає ідеальним інструментом для зловмисників. Шкідливе програмне забезпечення використовує зашифровані канали для зв'язку з командними серверами (C&C), ексфільтрації викрадених даних та завантаження додаткових модулів (payloads). Класичні системи виявлення вторгнень (IDS), що базуються на глибокому інспектуванні

пакетів (Deep Packet Inspection, DPI), виявляються безсилими перед зашифрованим корисним навантаженням. Процес примусового дешифрування трафіку «на льоту» (SSL/TLS Inspection) вимагає колосальних обчислювальних ресурсів, порушує принципи конфіденційності та вносить критичні затримки в роботу мережі.

Окрім технічних викликів, функціонування гетерогенних мережевих середовищ обтяжується суворими регуляторними вимогами. Національні та міжнародні стандарти інформаційної безпеки вимагають від організацій забезпечення комплексної системи захисту інформації. У таких умовах мережева інфраструктура повинна не лише відбивати атаки, але й забезпечувати безперервний збір доказової бази (логування), гарантувати цілісність даних та надавати механізми для проведення ретроспективного форензик-аналізу (Forensic Analysis) у разі виникнення інцидентів безпеки.

Враховуючи вищезазначені фактори — розмиття периметра, домінування внутрішнього «схід-захід» трафіку, масове впровадження вразливих IoT-пристроїв, централізацію управління через SDN та повсюдне шифрування даних — стає очевидним, що гетерогенні інформаційно-комунікаційні середовища є надзвичайно крихкими екосистемами. Забезпечення їхньої безпеки вимагає принципово нових підходів, орієнтованих не на побудову непробивних стін, а на безперервний, глибоко контекстний аналіз поведінки кожного окремого вузла мережі.

Концептуальну схему типового гетерогенного мережевого середовища наведено на рис. 1.2.

Аналіз поточної ситуації у сфері кібербезпеки свідчить про зміну парадигми нападів: від масових вірусних епідемій фокус змістився на складні цілеспрямовані атаки та програми-вимагачі (Ransomware). Такі атаки часто використовують експлойти нульового дня (zero-day), які не мають відомих сигнатур у вірусних базах. Згідно з аналітичними звітами Європейського агентства з кібербезпеки (ENISA) щодо ландшафту загроз, класичні антивіруси та системи виявлення вторгнень (IDS), які покладаються виключно на базу відомих сигнатур,

виявляються малоефективними проти мутуючих та новітніх загроз [18, 19].

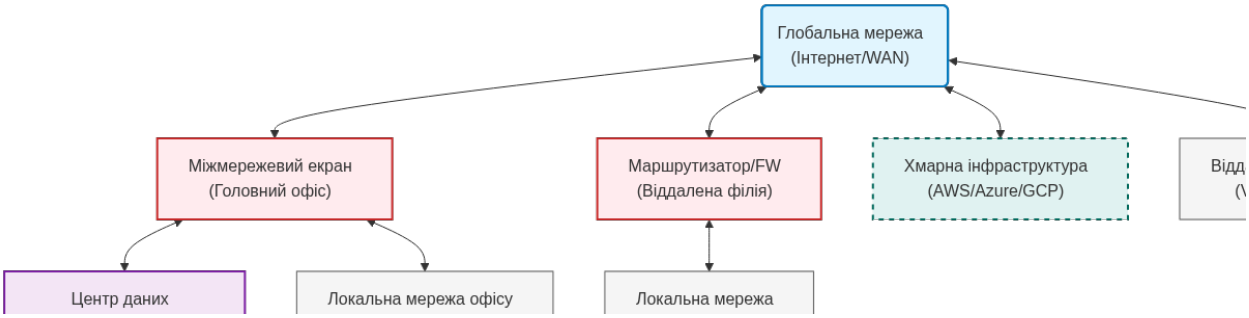


Рисунок 1.2 — Концептуальна схема гетерогенного інформаційно-комунікаційного середовища

Додатковим фактором ризику є використання поліморфного шкідливого коду, який змінює свою структуру під час кожного нового зараження, залишаючи при цьому свій основний деструктивний функціонал незмінним. У поєднанні з обмеженими можливостями класичного статичного аналізу це створює критичні розриви в системі захисту інформації [20]. Відтак, на перший план виходить необхідність впровадження інтелектуальних систем моніторингу, які здатні не просто порівнювати дані зі списками хешів відомих вірусів, а аналізувати поведінку системи в цілому, виявляючи найменші відхилення від нормального стану мережевого трафіку [21].

Саме імунологічний підхід, що базується на моделюванні штучних імунних систем (ШІС), пропонує ефективний вихід із цієї ситуації. Цей підхід розглядає корпоративну мережу як живий організм, де кожен вузол є клітиною, а будь-яка аномалія в трафіку або нетипова поведінка процесу сприймається як антиген (чужорідний елемент), що потребує негайної ідентифікації [22, 23]. ШІС дозволяє системі захисту адаптуватися та виявляти нові загрози на основі фундаментальної концепції розпізнавання «свій-чужий», що робить її стійкою до невідомих раніше атак [24].

1.4 Класифікація мережевих загроз та аналіз обмежень традиційних систем виявлення вторгнень

Побудова надійної комплексної системи захисту для сучасної інформаційно-комунікаційної мережі вимагає глибокого розуміння природи та еволюції деструктивних впливів. У гетерогенних середовищах, де взаємодіють сотні різнотипних пристроїв та протоколів, мережеві загрози доцільно класифікувати за вектором їхнього проникнення та рівнем скритності. Згідно з актуальними дослідженнями ландшафту кіберзагроз, найбільш критичну небезпеку для корпоративного сегмента становлять три основні класи атак [18, 19, 20]:

– об'ємні атаки на відмову в обслуговуванні (DDoS): спрямовані на критичне перевантаження пропускної здатності каналів зв'язку або апаратних ресурсів серверного обладнання. Сучасні розподілені ботнети здатні генерувати терабітні потоки сміттєвого трафіку, імітуючи при цьому поведінку легітимних користувачів [21];

– цілеспрямовані атаки та експлойти нульового дня (Zero-Day): експлуатація раніше невідомих вразливостей в операційних системах та прикладному програмному забезпеченні. До цієї категорії також входять складні персистентні загрози (APT), головною метою яких є тривале, приховане та несанкціоноване перебування зловмисника у внутрішній інфраструктурі організації [22, 23];

– поліморфне та метаморфне шкідливе програмне забезпечення: комп'ютерні віруси, мережеві черв'яки та програми-вимагачі (Ransomware), які здатні динамічно модифікувати свій вихідний код при кожному новому циклі розповсюдження. Це робить їхній двійковий підпис унікальним і унеможливлює виявлення класичними статичними методами [24].

Крім зазначених основних класів, сучасна таксономія мережевих загроз виділяє ще кілька специфічних векторів, які становлять особливу небезпеку для гетерогенних мереж. Зокрема, це атаки типу «людина посередині» (Man-in-the-

Middle, MitM), які в умовах бездротових та хмарних середовищ набули нових форм, таких як ARP-spoofing, DNS-hijacking та SSL-stripping. Зловмисник, перехоплюючи транзитний трафік, може не лише здійснювати пасивний сніфінг конфіденційних даних, але й активно модифікувати пакети "на льоту".

Ще однією критичною категорією є інсайдерські загрози (Insider Threats). Згідно зі статистикою, значний відсоток успішних зламів відбувається за участі легітимних користувачів мережі — як через їхню халатність (ненавмисні інсайдери, що стають жертвами соціальної інженерії чи фішингу), так і через зловмисні дії скомпрометованих співробітників. Виявлення інсайдерської активності є надскладним завданням для традиційних систем безпеки, оскільки такі дії виконуються з використанням авторизованих облікових записів і не містять класичних сигнатур шкідливого коду.

Особливої уваги заслуговує еволюція складних персистентних загроз (APT). Життєвий цикл APT-атаки складається з багатьох етапів: початкової розвідки (Reconnaissance), доставки (Delivery), експлуатації (Exploitation), встановлення бекдору (Installation), зв'язку з командним центром (Command and Control, C2) та ексфільтрації даних. Кожен з цих етапів ретельно маскується під легітимний мережевий трафік. APT-угруповання часто використовують техніки "Living off the Land" (LotL) — застосування вбудованих системних утиліт (наприклад, PowerShell, WMI) для виконання шкідливих дій, що дозволяє їм залишатися непоміченими для антивірусних рішень протягом тривалого часу.

Традиційні підходи до протидії зазначеним загрозам спираються на використання міжмережевих екранів (Firewalls) та систем виявлення/запобігання вторгненням (IDS/IPS). За базовим алгоритмом функціонування класичні системи моніторингу поділяються на дві категорії: сигнатурні (Signature-based IDS, SIDS) та статистичні (аномальні, Anomaly-based IDS, AIDS) [25]. Проте обидва ці підходи демонструють суттєві архітектурні обмеження.

Сигнатурні системи (SIDS) здійснюють верифікацію вхідного трафіку шляхом його порівняння з базою даних уже відомих загроз (хеш-сум або специфічних байтових послідовностей). Фундаментальним недоліком цього

методу є його "сліпота" до новітніх атак. Поліморфний вірус, код якого зазнав мінімальних мутацій, безперешкодно обходить такий захист. Крім того, безперервне збільшення обсягів баз даних сигнатур створює значне обчислювальне навантаження на мережеве обладнання, що призводить до неприпустимих затримок (latency) під час обробки високошвидкісного трафіку [25].

Системи на основі виявлення аномалій (AIDS) функціонують шляхом попередньої побудови математичної моделі "нормального" стану мережі. Будь-яке суттєве відхилення трафіку від цієї базової лінії класифікується як потенційна атака. Теоретично такий підхід здатний виявляти атаки нульового дня, однак на практиці він стикається з проблемою критично високого рівня хибних спрацювань (False Positives). Оскільки легітимний трафік у гетерогенних мережах є вкрай нелінійним (наприклад, через масове оновлення ПЗ або сплески активності віддалених працівників), статистичні IDS генерують тисячі хибних тривог. Це призводить до ефекту "втоми від сповіщень" (alert fatigue), через що адміністратори безпеки можуть пропустити реальний інцидент [26].

Результати порівняльного аналізу традиційних методів виявлення вторгнень узагальнено в таблиці 1.1.

Таблиця 1.1 — Порівняльний аналіз традиційних методів виявлення вторгнень

Метод виявлення	Основні переваги	Критичні недоліки
Сигнатурний аналіз (SIDS)	Висока точність виявлення відомих загроз; мінімальний рівень хибних спрацювань (False Positives).	Нездатність виявляти загрози «нульового дня» та поліморфні віруси; високі вимоги до обчислювальних ресурсів для пошуку по великих базах.
Статистичний аналіз аномалій (AIDS)	Здатність ідентифікувати невідомі раніше атаки (Zero-Day); незалежність від баз даних антивірусних компаній.	Високий відсоток хибних тривог; складність та тривалість етапу "навчання" системи (побудови профілю нормальної поведінки).

Детальний аналіз оперативної ефективності цих систем виявляє ще глибші архітектурні проблеми. Зі свого боку, зловмисники постійно вдосконалюють методи обходу (Evasion Techniques) традиційних засобів захисту. Класичні IDS виявляються вразливими до методів обфускації на рівні мережевих протоколів. Серед найпоширеніших технік обходу слід виділити фрагментацію IP-пакетів. Зловмисник штучно розбиває шкідливе корисне навантаження на надзвичайно малі фрагменти або навмисно перекриває зміщення фрагментів (overlapping fragments). Якщо механізм збирання пакетів (reassembly) в IDS відрізняється від того, який використовує цільова операційна система, система захисту збирає хибну послідовність байтів, яка не співпадає із сигнатурою.

Ще однією технікою є маніпуляція полем TTL (Time-To-Live). Атакуючий генерує пакети з різними значеннями TTL, створюючи ситуацію, коли частина шкідливого коду досягає IDS (і успішно проходить інспекцію), але відкидається маршрутизатором до того, як досягне цілі. Експлуатація протоколів прикладного рівня також зазнала значних змін. Сучасні атаки часто використовують тунелювання (Tunneling) для приховування шкідливого трафіку всередині легітимних протоколів, таких як DNS, ICMP або HTTP. DNS-тунелювання дозволяє інкапсулювати вкрадені дані у звичайні DNS-запити, які більшість міжмережевих екранів пропускають без глибокої перевірки.

Крім того, критичним операційним обмеженням традиційних систем є проблема масштабованості. Механізми глибокого інспектування пакетів (Deep Packet Inspection, DPI), які є основою роботи SIDS, вимагають значних потужностей CPU. Під час об'ємних DDoS-атак системи виявлення вторгнень самі можуть стати вузьким місцем (bottleneck), що призводить до відмови в обслуговуванні самої системи захисту. Зловмисники часто використовують цей ефект, запускаючи "шумову" DDoS-атаку для відвернення уваги (Smokescreen Attack), під прикриттям якої реалізується цілеспрямоване викрадення даних.

У контексті статистичного аналізу аномалій (AIDS) головною перешкодою для практичного впровадження залишається феномен "базової помилки" (Base-rate fallacy). В умовах реальної корпоративної мережі, де мільйони легітимних

подій відбуваються щохвилини, а реальні атаки є відносно рідкісними явищами, навіть система з точністю виявлення 99% генеруватиме величезну кількість хибних спрацювань. Це явище неминуче призводить до ефекту "втоми від сповіщень" (Alert Fatigue) серед аналітиків Центру операцій з кібербезпеки (SOC). Зіштовхуючись із сотнями хибних тривог щодня, оператори фізично не встигають проводити якісне розслідування інцидентів, що значно підвищує ризик пропуску критичної атаки (False Negative).

Окремим аспектом, що ускладнює роботу традиційних засобів виявлення, є тенденція до інтелектуалізації кібератак. Зародження нового класу загроз — Adversarial Machine Learning (змагальне машинне навчання) — кардинально змінює правила гри. Зловмисники використовують алгоритми штучного інтелекту для автоматичного пошуку «сліпих зон» у статистичних моделях IDS. Генеруючи спеціально підібраний трафік з мінімальними пертурбаціями, змагальні алгоритми здатні "отруїти" етап навчання моделі (Data Poisoning) або обдурити вже навчену систему, змушуючи її класифікувати шкідливі дії як нормальну поведінку [27]. У таких умовах статичні правила та навіть прості статистичні моделі стають повністю нерелевантними.

Аналіз наведених недоліків доводить вичерпаність традиційної парадигми захисту. Сучасна інфраструктура потребує переходу до систем, які поєднують здатність ідентифікувати невідомі атаки з низьким рівнем хибних тривог, забезпечуючи при цьому властивість самоадаптації. Найбільш релевантним рішенням цієї проблеми є впровадження біоінспірованого імунологічного підходу (ШІС). Використовуючи адаптивні алгоритми та теорію небезпеки, штучні імунні системи здатні безпомилково відрізняти деструктивні аномалії від легітимних змін у мережевому середовищі.

1.5 Концептуальні засади застосування імунологічної парадигми в кіберзахисті

Штучна імунна система (ШІС) — це інтелектуальна обчислювальна парадигма, натхненна принципами та процесами біологічної імунної системи людини. Основною метою ШІС у контексті кібербезпеки є розробка адаптивних механізмів, здатних підтримувати стабільне функціонування інформаційно-комунікаційної мережі в умовах постійно мінливих зовнішніх та внутрішніх загроз [28]. Дослідження ефективності імунологічних алгоритмів доводять їхню високу життєздатність як у локальних, так і в розподілених мережевих архітектурах [29].

Фундаментальною концепцією, на якій базується імунологічний підхід, є розпізнавання «свій-чужий» (Self-Nonself discrimination). У біологічному сенсі імунітет повинен ідентифікувати та знищити антигени (віруси, бактерії), не пошкоджуючи при цьому здорові клітини організму. У цифровому просторі під «своїм» (Self) розуміють легітимні мережеві пакети, санкціоновані запити користувачів та нормальну поведінку системних процесів. Відповідно, «чуже» (Nonself) — це будь-яка активність, що свідчить про спробу зламу, розповсюдження шкідливого коду або проведення DDoS-атаки [30]. Детальний взаємозв’язок між компонентами біологічної системи та їх технічними аналогами у сфері захисту мереж представлено на рис. 1.3.

Для повного розуміння потужності імунологічної парадигми варто зазначити, що біологічний захист організму базується на двох взаємопов'язаних підсистемах: вродженому (Innate) та набутому (Adaptive) імунітеті. Вроджений імунітет є першою лінією оборони (шкіра, слизові оболонки, макрофаги), яка реагує на відомі, базові патерни загроз миттєво, але не має пам'яті. У термінах кібербезпеки аналогом вродженого імунітету є традиційні міжмережеві екрани, списки контролю доступу (ACL) та базові антивірусні сигнатури (SIDS). Натомість набутий імунітет (В-клітини та Т-клітини) формується протягом усього життя, розпізнає нові, раніше невідомі мутації вірусів і створює клітини пам'яті.

Саме імітація набутого імунітету є головним завданням ШІС, що дозволяє вирішити проблему виявлення атак нульового дня.

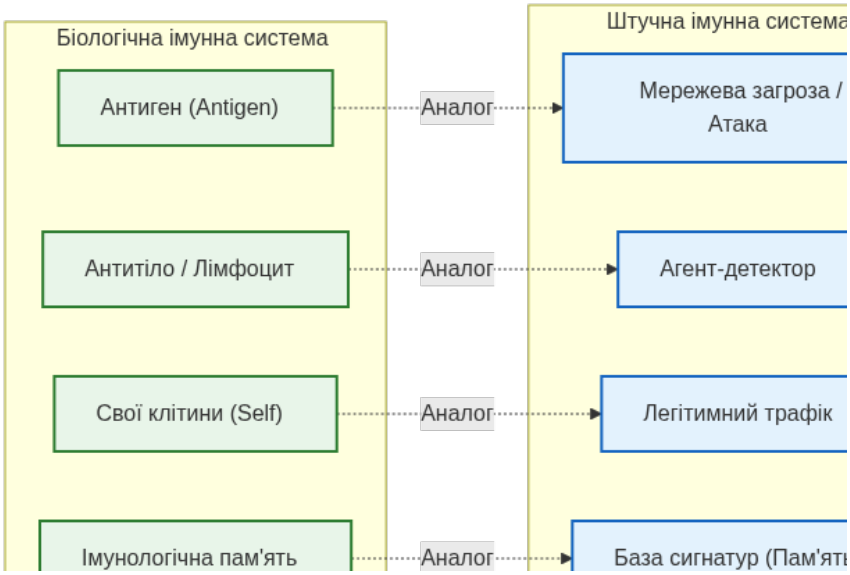


Рисунок 1.3 — Компаративний аналіз компонентів біологічної та штучної імунних систем

Для забезпечення ефективного захисту гетерогенних мереж імунологічна парадигма використовує кілька ключових механізмів, які суттєво відрізняють її від класичних засобів безпеки [31, 32]:

– розподіленість та децентралізація: імунна система не має єдиного центру управління; мільйони імунних клітин (детекторів) циркулюють по всьому організму, приймаючи локальні рішення. У комп'ютерній мережі це реалізується через систему автономних програмних агентів, що моніторять трафік на різних вузлах;

– різноманітність (Diversity): кожен організм має унікальний набір антитіл. Це гарантує, що якщо одна система захисту буде скомпрометована, інші вузли мережі залишаться захищеними через відмінність своїх детекторів;

– адаптивність та навчання: система здатна «запам'ятовувати» характеристики раніше зустрінутих загроз. Це дозволяє при повторному інциденті реагувати миттєво, значно швидше, ніж при первинному контакті;

– стійкість до збоїв (Robustness): завдяки відсутності централізованого контролера, вихід з ладу навіть значної частини агентів-детекторів не призводить

до краху всієї системи захисту. Деградація функціональності відбувається плавно, зберігаючи базовий рівень безпеки.

Основними алгоритмічними стовпами ШІС, що застосовуються для захисту мереж, є алгоритм негативного відбору (Negative Selection Algorithm, NSA) та алгоритм клональної селекції (Clonal Selection Algorithm, CSA) [33]. Обидва алгоритми оперують концепцією «простору форм» (Shape Space). У цьому просторі кожна подія (мережевий пакет, системний виклик) представляється у вигляді вектора ознак x = {x1, x2, ..., xn}. Ступінь відповідності між антигеном (трафіком) та антитілом (детектором) називається афінністю (Affinity) і обчислюється за допомогою метрик відстані, таких як відстань Геммінга для бінарних рядків або евклідова відстань для дійсних чисел.

Алгоритм негативного відбору (NSA) моделює процес дозрівання Т-лімфоцитів у вилочковій залозі (тимусі). Його мета — згенерувати набір детекторів, які гарантовано не реагуватимуть на легітимний трафік. Процес складається з двох фаз:

1. Фаза генерації (Цензурування): Система випадковим чином генерує кандидати в детектори. Кожен кандидат порівнюється з множиною відомого нормального трафіку (Self-профілем). Якщо афінність кандидата до будь-якого елемента Self перевищує заданий поріг чутливості ϵ (тобто детектор реагує на норму), такий кандидат знищується. Ті детектори, що не зреагували на "своє", стають зрілими і переходять у робочу фазу.

2. Фаза моніторингу: Зрілі детектори порівнюються з новим, невідомим вхідним трафіком. Якщо відбувається збіг (афінність перевищує поріг), система фіксує аномалію (Nonself).

Перевагою NSA є те, що він навчається виключно на нормальних даних, усуваючи необхідність збору величезних баз вірусних сигнатур.

Алгоритм клональної селекції (CSA) формалізує механізм реакції В-клітин на антиген і використовується для оптимізації та адаптації системи. Якщо детектор успішно ідентифікує загрозу, він активується і починає процес клональної експансії — створення власних копій. Ключовою особливістю є

соматична гіпермутація: під час клонування детектори піддаються випадковим змінам. Рівень мутації є обернено пропорційним до афінності: чим краще детектор розпізнав ціль, тим менше він мутує; чим слабшим було розпізнавання, тим радикальнішими будуть зміни. Це забезпечує як локальний пошук оптимального рішення (точну підгонку під виявлений вірус), так і глобальний пошук у просторі загроз (створення детекторів для майбутніх мутацій вірусу) [34]. Найефективніші мутанти перетворюються на «клітини пам'яті», інтегруючись у базу знань для миттєвого блокування аналогічних атак у майбутньому. Окремі дослідження підтверджують високу ефективність цих імунологічних обчислень навіть у промислових мережах та системах Інтернету речей (IoT) [35, 36].

Незважаючи на ефективність класичних моделей "свій-чужий", у гетерогенних мережах з високою динамікою легітимного трафіку NSA та CSA можуть стикатися з проблемою масштабованості та генерації хибних спрацювань (False Positives). Вирішенням цієї фундаментальної проблеми став розвиток імунологічного підходу через призму «теорії небезпеки» (Danger Theory), формалізованої у вигляді алгоритму дендритних клітин (Dendritic Cell Algorithm, DCA) [37].

Теорія небезпеки, запропонована імунологом Поллі Матцінгер, стверджує, що біологічна імунна відповідь ініціюється не фактом присутності чужорідного елемента, а наявністю реальної шкоди для організму. У біології дендритні клітини збирають сигнали з навколишнього середовища тканин. У контексті кібербезпеки програмні дендритні клітини агрегують контекстні сигнали від операційної системи та мережевого обладнання.

Математична модель DCA оперує трьома основними типами вхідних сигналів:

1. PAMP (Pathogen-Associated Molecular Patterns) — Сигнали патогенів: Індикатори явної, беззаперечної загрози (наприклад, збіг із чорним списком IP-адрес або виявлення відомої сигнатури).

2. Danger Signals — Сигнали небезпеки: Індикатори ймовірного

пошкодження або аномалії поведінки (наприклад, різкий стрибок використання CPU до 100%, масова кількість спроб авторизації або нетипово велика кількість з'єднань на один порт).

3. Safe Signals — Сигнали безпеки: Індикатори нормального функціонування (наприклад, успішна авторизація через двофакторну аутентифікацію, стабільна робота системних процесів без відхилень).

Дендритна клітина збирає антигени (IP-адреси, ID процесів) і паралельно накопичує зазначені сигнали. Алгоритм розраховує кумулятивні значення концентрації костимуляторних молекул (CSM) та маркерів стану (Semi-mature або Mature) за допомогою матриці ваг , що формалізується у вигляді виразу (1.4):

$$Ccsm = WP * PAMP + WD * Danger + WS * Safe \tag{1.4}$$

Якщо загальна концентрація сигналів перевищує поріг життєздатності, клітина припиняє збір даних і аналізує свій стан. Якщо домінували сигнали безпеки, клітина стає "напівзрілою" (Semi-mature) і маркує зібрані антигени як легітимні (навіть якщо вони виглядали аномально, як у випадку масового оновлення Windows). Якщо ж домінували сигнали небезпеки та PAMP, клітина стає "зрілою" (Mature) і передає інформацію агенту-координатору для ініціації імунної відповіді (блокування).

Впровадження цієї теорії в системи моніторингу мережі дозволяє радикально знизити кількість хибних спрацювань. Система більше не блокує трафік лише тому, що він "не схожий на норму". Вона вимагає підтвердження — кореляції аномалії з деградацією продуктивності або іншими метриками небезпеки [38, 39]. Цей контекстно-залежний механізм ідеально підходить для розгортання в умовах складних гетерогенних архітектур, де межа між нормальним та шкідливим є розмитою.

Таким чином, застосування імунологічної парадигми дозволяє створити багаторубежеву, адаптивну систему захисту. Інтеграція реактивних алгоритмів (NSA), механізмів довгострокової пам'яті (CSA) та контекстного аналізу небезпеки (DCA) у мультиагентне середовище створює архітектуру, яка здатна до

самоорганізації та ефективного функціонування в умовах високої невизначеності сучасного кіберпростору.

1.6 Постановка задачі на дослідження та моделювання імунної системи моніторингу

Проведений у попередніх підрозділах аналіз свідчить про наявність глибокої системної кризи в галузі традиційних засобів захисту інформації. Гетерогенні інформаційно-комунікаційні мережі, характеризуючись високим рівнем масштабованості та динамічності, залишаються критично вразливими до цілеспрямованих атак нульового дня, поліморфного шкідливого коду та розподілених атак на відмову в обслуговуванні (DDoS) [40]. Існуючі сигнатурні та статистичні системи виявлення вторгнень (IDS) не здатні забезпечити необхідний рівень проактивного захисту через фундаментальні архітектурні обмеження: неможливість детектування невідомих загроз та критично високий відсоток хибних тривог [41].

Вирішення цієї комплексної проблеми вимагає переходу від жорстких детермінованих алгоритмів до адаптивних біоінспірованих моделей. Використання концепції штучних імунних систем (ШІС), яка інтегрує алгоритми негативного відбору, клональної селекції та положення теорії небезпеки, дозволяє створити розподілену систему моніторингу, здатну до самоорганізації, розпізнавання складних патернів та навчання в режимі реального часу [42, 43]. Однак безпосереднє впровадження імунологічних алгоритмів у корпоративну мережу вимагає попереднього теоретичного обґрунтування, формування чітких архітектурних вимог та детального моделювання поведінки системи.

З огляду на вищезазначене, головною задачею даної кваліфікаційної роботи є проведення теоретичного дослідження та розробка концептуальної моделі розподіленої імунної системи моніторингу трафіку для захисту інформаційно-комунікаційних мереж.

Для розв'язання цієї глобальної задачі в межах проєктування та аналітичної оцінки необхідно виконати наступні кроки:

– сформувати комплекс функціональних та архітектурних вимог до системи виявлення мережевих аномалій на основі імунологічного підходу;

– розробити теоретичну модель розподіленої мережі інтелектуальних програмних агентів-детекторів, адаптовану для роботи в гетерогенному середовищі;

– визначити та обґрунтувати алгоритмічні основи застосування методів негативного відбору та клональної селекції для аналізу мережевого трафіку;

– змоделювати логіку адаптації системи та мінімізації хибних спрацювань шляхом імплементації механізмів теорії небезпеки (Danger Theory);

– описати архітектурні сценарії взаємодії розробленої імунної моделі з класичними засобами моніторингу безпеки (міжмережевими екранами, SIEM-системами) для нейтралізації виявлених DDoS-атак [44, 45];

– провести порівняльний аналіз та теоретичну оцінку ефективності запропонованої концептуальної моделі [46, 47].

Розв'язання поставленої задачі дозволить сформувати обґрунтоване підґрунтя для проєктування адаптивних систем кіберзахисту нового покоління, здатних ефективно протистояти сучасним кіберзагрозам в умовах високої невизначеності.

Важливою умовою успішної реалізації поставлених завдань є перехід від абстрактного теоретичного опису до формалізованого архітектурного моделювання. Саме тому наступним логічним кроком дослідження стане проєктування структурних компонентів системи та детальний опис життєвого циклу програмних агентів. Такий підхід дозволить не лише концептуально описати систему захисту, але й створити надійне інженерне підґрунтя для її подальшої практичної програмної реалізації та верифікації в умовах імітації реальних мережевих атак [48].

Для забезпечення високої репрезентативності та обґрунтованості результатів майбутнього моделювання, необхідно чітко окреслити межі

дослідження (Scope of Research) та сформулювати базові припущення, в умовах яких функціонуватиме розроблюваний прототип штучної імунної системи. Оскільки повномасштабне розгортання експериментальних систем безпеки в діючих (production) інфраструктурах несе неприпустимі ризики для бізнес-процесів, перевірка концептуальної моделі вимагає створення ізольованого, але структурно адекватного імітаційного середовища (Testbed).

Проєктована система орієнтована на захист корпоративного сегмента гетерогенної мережі. У межах даної роботи передбачається, що об'єктом захисту виступає віртуалізована мережева інфраструктура, яка включає маршрутизуюче обладнання (на рівні ядра та доступу), сервери застосунків, бази даних та пул кінцевих робочих станцій.

До імітаційного середовища висуваються наступні суворі вимоги: – Репрезентативність фонового трафіку: Для коректного навчання алгоритму негативного відбору (формування профілю «Self») мережа повинна генерувати стабільний потік легітимного трафіку, що імітує реальну поведінку користувачів. Це включає HTTP/HTTPS-запити до вебсерверів, DNS-розділення, ICMP-пінгування для перевірки доступності вузлів та службовий трафік локальної мережі (наприклад, ARP). – Можливість генерації контрольованих аномалій: Середовище повинно дозволяти інжекцію шкідливого трафіку різної інтенсивності з фіксованими часовими мітками (timestamps). Це є критично важливим для подальшого розрахунку матриці помилок (Confusion Matrix) та визначення того, наскільки швидко імунна система реагує на подразник. – Ізоляція та безпека: Усі експерименти з імітацією цілеспрямованих атак та впливу шкідливого програмного забезпечення повинні проводитися в закритому віртуальному контурі (Sandboxed Environment) для унеможливлення витоку деструктивного коду в глобальну мережу.

Зважаючи на те, що спектр сучасних кіберзагроз є надзвичайно широким, для верифікації ефективності розробленої імунної системи доцільно сфокусуватися на класах атак, які найважче піддаються виявленню традиційними сигнатурними методами. В рамках дослідження моделюватимуться наступні

деструктивні сценарії:

– агресивні розподілені атаки на відмову в обслуговуванні (Volumetric DDoS): Моделювання SYN-флуду та UDP-флуду з підміною вихідних IP-адрес (IP Spoofing). Завдання імунної системи в цьому сценарії — не просто зафіксувати зростання обсягу трафіку, а за допомогою алгоритму дендритних клітин скорелювати цю аномалію з деградацією продуктивності цільового сервера (сигналом небезпеки) та виокремити шкідливі пакети з-поміж легітимних запитів;

– атаки прикладного рівня (Application-Layer (L7) DDoS): Генерація високочастотних HTTP GET/POST запитів (наприклад, атака типу HTTP Flood). На відміну від транспортного рівня, такі атаки виглядають як абсолютно легітимні з'єднання, що вимагає від агентів-детекторів глибокого аналізу контексту та поведінкових патернів джерела запиту;

– мережеве сканування та розвідка (Reconnaissance): Моделювання прихованого (Stealth) сканування портів з використанням змінених прапорців протоколу TCP (наприклад, FIN, NULL або XMAS сканування). Здатність імунної системи ідентифікувати такі повільні, розтягнуті в часі аномалії продемонструє ефективність механізмів довгострокової імунологічної пам'яті (клональної селекції).

Процес розробки та валідації системи вимагає чіткої метризації. Концептуальний підхід «працює / не працює» є неприйнятним для інженерного дослідження. Оцінка ефективності запропонованої мультиагентної імунної моделі здійснюватиметься за комплексом кількісних та якісних критеріїв:

– точність класифікації (Classification Accuracy): Базовий параметр, що визначатиметься співвідношенням істинно позитивних (TP) та істинно негативних (TN) спрацювань до загальної кількості проаналізованих мережевих подій;

– рівень хибних тривог (False Positive Rate, FPR): Найбільш критичний показник для систем виявлення аномалій. Успішність імплементації «теорії небезпеки» оцінюватиметься саме за здатністю системи утримувати цей показник на мінімальному рівні навіть під час стрибків легітимного навантаження;

– ступінь адаптивності системи: Здатність системи автоматично генерувати

нові детектори для невідомих варіацій атак без необхідності ручного оновлення баз даних адміністратором. Цей параметр перевірятиметься шляхом подачі на вхід системи мутованих векторів атак, які раніше не зустрічалися в процесі навчання (імітація Zero-Day загроз);

– продуктивність та ресурсоємність: Оскільки локальні агенти планується розміщувати безпосередньо на кінцевих вузлах гетерогенної мережі (зокрема на пристроях з обмеженими обчислювальними можливостями), важливим критерієм є споживання ресурсів центрального процесора (CPU) та оперативної пам'яті (RAM) під час роботи скриптів детектування;

– час реакції (Response Latency): Інтервал часу між фактичним початком мережевої атаки та моментом генерації відповідного керуючого впливу (наприклад, передачі команди агентом-координатором на міжмережевий екран для блокування шкідливого IP-адреси).

Реалізація окреслених у постановці задачі етапів — від теоретичного обґрунтування мультиагентної архітектури до безпосереднього написання коду алгоритмів та їх тестування — становить структуру наступних розділів роботи. Перехід до розділу проєктування базуватиметься на вже доведеній неспроможності монолітних та суто сигнатурних систем, і буде повністю присвячений синтезу архітектурних рішень, здатних задовольнити висунуті вище функціональні вимоги до систем кіберзахисту нового покоління.

Очікується, що впровадження розробленої концептуальної моделі дозволить не лише підвищити загальний рівень стійкості мережевої інфраструктури, але й суттєво оптимізувати операційну діяльність підрозділів безпеки. Зниження рівня хибних тривог завдяки застосуванню алгоритму дендритних клітин (DCA) та теорії небезпеки безпосередньо вплине на зменшення інформаційного перевантаження аналітиків Центрів операцій з кібербезпеки (SOC). Автоматизація процесів виявлення аномалій та первинного реагування, повністю делегована розподіленій мережі програмних агентів, вивільнить критично важливі людські ресурси для виконання складніших аналітичних завдань, розслідування інцидентів та проактивного пошуку прихованих загроз (Threat Hunting).

2 ПРОЄКТУВАННЯ ТА ТЕОРЕТИЧНЕ МОДЕЛЮВАННЯ СИСТЕМИ ІМУННОГО МОНІТОРИНГУ ТРАФІКУ

2.1 Формування вимог до архітектури системи виявлення мережевих аномалій

Перехід від теоретичної концепції штучних імунних систем (ШІС) до побудови практичної моделі захисту інформаційно-комунікаційної мережі вимагає чіткого визначення набору функціональних та архітектурних вимог. Оскільки цільовим середовищем розгортання є гетерогенна корпоративна мережа з високою динамікою трафіку, архітектура системи повинна забезпечувати не лише високу точність виявлення загроз, але й стійкість до збоїв, масштабованість та мінімальний вплив на пропускну здатність каналів зв'язку.

Процес формування вимог базується на принципі декомпозиції складної задачі кіберзахисту на окремі ізольовані підпроцеси, які імітують поведінку біологічних клітин. Усю сукупність вимог до проєктованої моделі доцільно розділити на дві великі категорії: функціональні (що система повинна робити) та архітектурні (якими властивостями вона повинна наділятися).

Функціональні вимоги визначають базову логіку роботи імунної системи моніторингу:

– здійснення безперервного пасивного аналізу мережевого трафіку на рівнях L3-L7 (мережевий, транспортний та прикладний рівні моделі OSI) без внесення затримок у процес маршрутизації;

– здатність до динамічної генерації набору програмних детекторів (на основі алгоритму негативного відбору), які не реагують на профіль «нормального» трафіку конкретної мережі;

– ідентифікація мережевих аномалій шляхом кореляції нетипової поведінки з наявністю «сигналів небезпеки» (Danger Signals), таких як масове сканування портів, раптове зростання кількості помилок авторизації або перевантаження процесора на кінцевому вузлі;

– формування «імунологічної пам’яті» — механізму збереження інформації

про структуру виявленого та нейтралізованого шкідливого впливу для миттєвого блокування аналогічних атак у майбутньому;

– генерація структурованих сповіщень про інциденти інформаційної безпеки у форматі, придатному для автоматизованої обробки зовнішніми SIEM-системами.

Архітектурні (нефункціональні) вимоги визначають принципи побудови інфраструктури ШІС для забезпечення її життєздатності в реальних умовах:

– децентралізованість: система не повинна мати єдиної точки відмови (Single Point of Failure). Обчислювальне навантаження має бути розподілене між множиною автономних агентів, розташованих на різних сегментах мережі;

– масштабованість: архітектура повинна підтримувати можливість безшовного додавання нових сенсорів та агентів-детекторів при розширенні меж корпоративної мережі або інтеграції сегментів Інтернету речей (IoT);

– адаптивність та самоорганізація: агенти повинні мати здатність до обміну інформацією про нові загрози між собою (аналог локальної імунної реакції), самостійно оновлюючи свої бази детекторів без обов'язкового втручання адміністратора безпеки;

– відмовостійкість: у разі компрометації або відключення одного мережевого вузла з агентом-детектором, інші елементи системи повинні продовжувати функціонувати, компенсуючи втрату за рахунок надмірності (аналог величезної кількості лімфоцитів в організмі).

Сформульовані вимоги виключають можливість використання монолітних систем захисту інформації. Відповідно, оптимальним архітектурним рішенням для реалізації поставлених завдань є мультиагентна система, де кожен агент виконує роль окремого імунологічного елемента. Це створює надійне підґрунтя для подальшого теоретичного моделювання логічної структури системи.

2.2 Моделювання розподіленої мережі інтелектуальних агентів-детекторів

Реалізація імунологічного підходу в складних гетерогенних мережах вимагає використання концепції мультиагентних систем. У межах даного дослідження пропонується модель розподіленої мережі, що складається з автономних програмних агентів-детекторів, які функціонують як цифрові аналоги лімфоцитів біологічної імунної системи. Така архітектура дозволяє забезпечити децентралізований моніторинг трафіку без створення надмірного навантаження на магістральні канали зв'язку.

Кожен інтелектуальний агент у проєктованій системі є автономною одиницею, яка розміщується на критичних вузлах мережі (серверах, робочих станціях, маршрутизаторах). Логічна структура окремого агента-детектора включає наступні функціональні блоки:

- модуль перцепції (захоплення даних): відповідає за пасивне перехоплення мережевих пакетів та вилучення ключових ознак трафіку (IP-адреси, порти, прапори TCP, обсяг корисного навантаження);
- аналітичне ядро (модуль розпізнавання): містить набір сформованих детекторів, які перевіряють вилучені ознаки на відповідність профілю «чужого» за допомогою алгоритму негативного відбору;
- модуль адаптації: відповідає за динамічне оновлення локальної бази детекторів та взаємодію з іншими агентами для обміну інформацією про нові загрози;
- ефекторний модуль: ініціює захисну реакцію (генерує сигнал тривоги або передає команду на блокування трафіку зовнішнім засобам захисту) у разі підтвердження атаки.

Загальну логічну архітектуру взаємодії внутрішніх модулів агента-детектора та його зв'язок із глобальною мережею наведено на рис. 2.1.

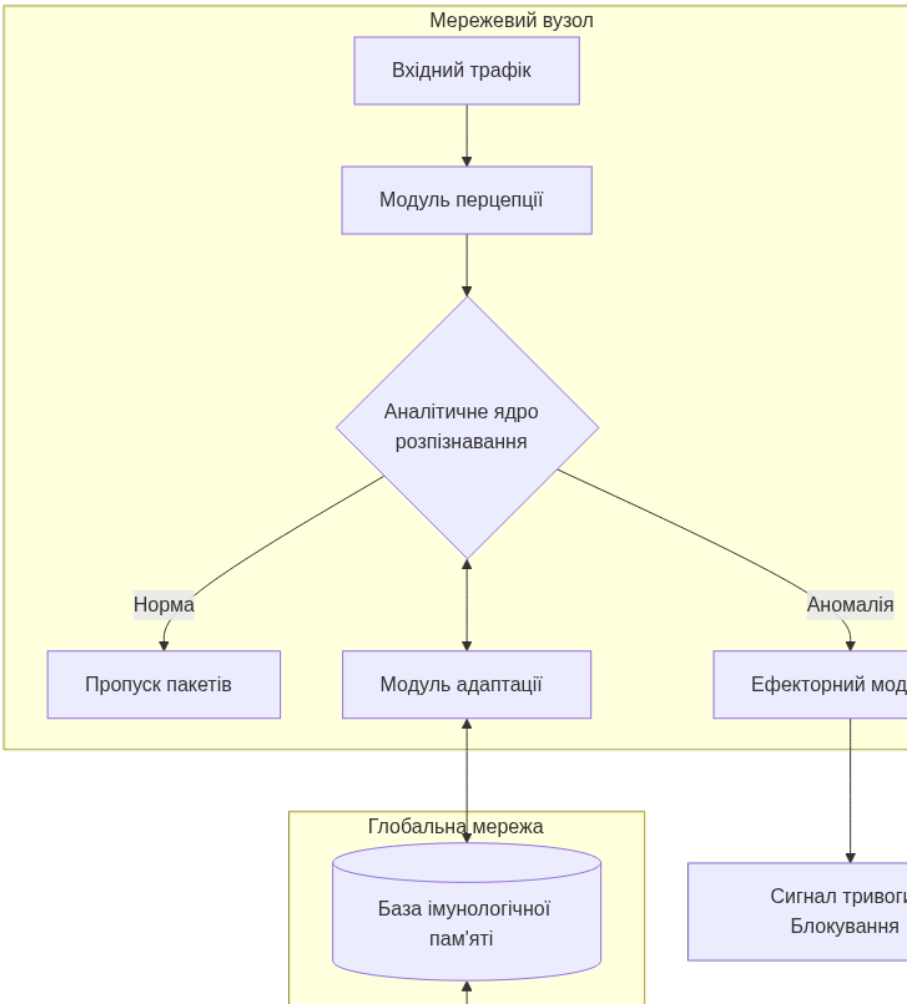


Рисунок 2.1 — Схема архітектури розподіленої мультиагентної імунної системи

Розподілена природа системи моделюється через ієрархічну взаємодію трьох типів агентів, що утворюють цілісний захисний контур:

– локальні агенти-детектори (L-agents): виконують первинний моніторинг на кінцевих пристроях, фокусуючись на специфічних для даного вузла аномаліях;

– агенти імунологічної пам'яті (M-agents): накопичують та розповсюджують сигнатури підтверджених аномалій по всій мережі, забезпечуючи швидку вторинну імунну відповідь;

– агенти-координатори (C-agents): здійснюють агрегацію даних від локальних агентів для виявлення розподілених атак, таких як масоване сканування мережі або координовані DDoS-атаки.

Взаємодія між агентами базується на принципах емерджентної поведінки: кожен агент діє локально, але їхня сукупна активність формує глобальний рівень

безпеки мережі. Це моделюється як процес постійної циркуляції та мутації «цифрових антитіл» (детекторів) у мережевому середовищі. Якщо локальний агент виявляє аномалію, він не лише реагує самостійно, але й транслює «сигнал небезпеки» сусіднім вузлам, що дозволяє системі превентивно підготуватися до поширення загрози.

Така модель забезпечує високу живучість системи: навіть при виході з ладу частини агентів або компрометації окремих вузлів, решта мережі зберігає здатність до ідентифікації загроз завдяки різноманітності детекторів та децентралізованому управлінню.

2.3 Алгоритмічні основи застосування методів негативного відбору та клональної селекції

Функціонування аналітичного ядра розроблених інтелектуальних агентів-детекторів базується на математичній формалізації двох фундаментальних імунологічних процесів: алгоритмі негативного відбору (Negative Selection Algorithm, NSA) та алгоритмі клональної селекції (Clonal Selection Algorithm, CSA). Сумісне використання цих алгоритмів забезпечує як первинне виявлення невідомих аномалій, так і формування адаптивної бази знань (імунологічної пам’яті) мережі.

Для алгоритмічного опису введемо поняття простору станів мережі U (Universe), який представляє всі можливі варіанти мережевого трафіку. Цей простір розділяється на дві множини, що не перетинаються: множину нормальної поведінки S (Self) та множину аномалій N (Nonself), тобто U = S U N. Мережевий трафік подається системі у вигляді векторів ознак (IP-адреси, порти, прапори пакетів, розмір корисного навантаження), які система має класифікувати.

Алгоритм негативного відбору (NSA) застосовується на етапі генерації детекторів (навчання системи). Його головна мета — створити множину детекторів R (Receptors), які здатні розпізнавати будь-який вектор з множини N,

але при цьому ігнорувати вектори з множини S (щоб уникнути хибних спрацювань). Процес відбувається у три етапи:

1. Генерація: система випадковим чином або за допомогою евристичних правил генерує кандидати в детектори R0.

2. Цензурування (відбір): кожен кандидат порівнюється з профілем нормального трафіку S. Якщо кандидат збігається з нормальним патерном (рівень спорідненості перевищує заданий поріг толерантності), він знищується.

3. Дозрівання: кандидати, які не зреагували на S, стають зрілими детекторами множини R і розгортаються на мережевих вузлах для моніторингу вхідного трафіку.

Математично умова успішного детектування аномалії x Є U детектором d Є R визначається через функцію афінності (спорідненості) Affinity(x, d) ≥ Tr, де Tr — поріг реакції.

Алгоритм клональної селекції (CSA) активується в момент, коли зрілий детектор успішно ідентифікує аномалію (атаку). Цей алгоритм імітує процес розмноження та мутації найуспішніших імунних клітин для створення потужної вторинної відповіді. Його логіка описується наступними кроками:

1. Активація та клонування: детектор, що виявив атаку, починає створювати свої копії (клони). Кількість клонів прямо пропорційна ступеню загрози (сигналу небезпеки) та афінності.

2. Соматична гіпермутація: клони піддаються структурним змінам (змінюються параметри їхніх векторів ознак). При цьому діє правило зворотної пропорційності: чим вища афінність батьківського детектора до аномалії, тим нижчий рівень мутації застосовується до його клонів. Це дозволяє здійснювати тонке налаштування (Affinity Maturation) навколо виявленої загрози.

3. Формування пам'яті: клони, які після мутації найкраще розпізнають дану атаку, отримують статус «клітин пам'яті» і зберігаються в глобальній базі імунологічної пам’яті системи з необмеженим терміном життя.

Блок-схему, що ілюструє логіку прийняття рішень та послідовність проходження етапів генерації детекторів за алгоритмом негативного відбору,

наведено на рис. 2.2.

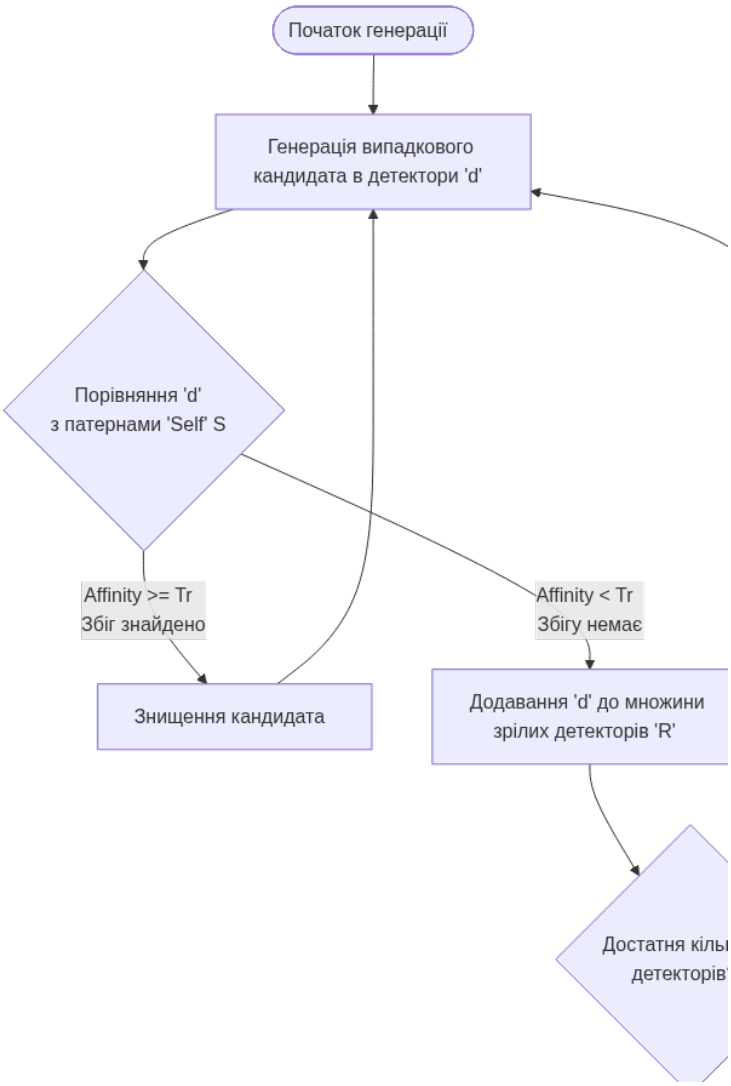


Рисунок 2.2 — Блок-схема логіки роботи алгоритму негативного відбору (NSA)

Інтеграція NSA та CSA у рамках єдиного програмного агента дозволяє вирішити ключову проблему традиційних IDS: система не потребує регулярного завантаження сторонніх баз сигнатур. Вона самостійно вивчає профіль нормальної поведінки корпоративної мережі, генерує унікальний набір детекторів та динамічно адаптується до нових модифікацій поліморфного ПЗ і zero-day атак шляхом спрямованих мутацій.

2.4 Висновки

У другому розділі було проведено теоретичне проєктування та моделювання архітектури розподіленої імунної системи моніторингу трафіку. Результати дослідження дозволяють зробити наступні висновки:

– сформовано комплекс функціональних та архітектурних вимог до системи, серед яких ключовими визначено децентралізованість, масштабованість, адаптивність та здатність до виявлення аномалій у режимі реального часу без внесення затримок у роботу мережі;

– розроблено концептуальну модель розподіленої мультиагентної системи, де кожен агент функціонує як автономний програмний «лімфоцит». Виділено три рівні ієрархії агентів (локальні, агенти пам'яті та координатори), що забезпечує відсутність єдиної точки відмови та високу живучість всієї системи кіберзахисту;

– обґрунтовано та математично формалізовано використання алгоритму негативного відбору (NSA) для процесу «дозрівання» детекторів. Це дозволяє системі самостійно вивчати профіль нормального трафіку та генерувати унікальний набір сигнатур для ідентифікації раніше невідомих аномалій;

– описано логіку застосування алгоритму клональної селекції (CSA), який забезпечує формування імунологічної пам’яті мережі. Завдяки механізмам соматичної гіпермутації система здатна динамічно адаптуватися до нових модифікацій атак, підвищуючи афінність (точність розпізнавання) детекторів з часом;

– доведено, що поєднання запропонованих алгоритмів у межах єдиної імунної парадигми дозволяє створити проактивний контур захисту, який, на відміну від традиційних IDS, здатний до самостійного навчання та ефективного функціонування в умовах високої невизначеності гетерогенного мережевого середовища.

Синтез функціональних та архітектурних вимог дозволив обґрунтувати перехід від класичних монолітних периметральних засобів захисту до розподіленої парадигми імунного моніторингу. Орієнтація на принципи

децентралізації та масштабованості забезпечує адаптивне розгортання системи в сучасних гетерогенних корпоративних мережах, де межі традиційного безпекового периметра є повністю розмитими. Застосування мультиагентної моделі дозволяє перенести основне обчислювальне навантаження безпосередньо на кінцеві вузли інфраструктури, виключаючи виникнення критичних точок відмови та мінімізуючи вплив процесів інспектування пакетів на загальну пропускну здатність каналів зв'язку.

Важливим аспектом змодельованого алгоритмічного забезпечення є автоматизація процесів адаптації через механізми оцінки афінності у просторі форм (Shape Space). Спільне застосування алгоритмів негативного відбору та клональної селекції дозволяє реалізувати концепцію безперервного проактивного навчання без залучення зовнішнього оператора або громіздких централізованих сигнатурних баз. Завдяки впровадженню операторів соматичної гіпермутації, штучні імунні компоненти набувають здатності до гнучкого розширення меж розпізнавання, що забезпечує точне детектування навіть незначно модифікованих або повністю нових векторів атак (Zero-day) при збереженні високої швидкості обробки трафіку на кожному окремому вузлі.

Таким чином, розроблена в межах розділу теоретична модель перетворює пасивний моніторинг трафіку на динамічне захисне середовище, здатне проактивно реагувати на деструктивні впливи в умовах високої апріорної невизначеності. Математична та архітектурна структуризація імунних компонентів доводить інженерну спроможність запропонованого підходу та ліквідує функціональні розриви, притаманні сигнатурним і статистичним системам виявлення вторгнень.

Проєктована модель закладає підґрунтя для подальшої аналітичної оцінки ефективності запропонованих рішень та опису сценаріїв їх взаємодії з існуючою інфраструктурою безпеки.

3 АНАЛІТИЧНА ОЦІНКА ТА АСПЕКТИ ВПРОВАДЖЕННЯ СИСТЕМИ ІМУННОГО МОНІТОРИНГУ

3.1 Моделювання сценаріїв адаптації системи на основі теорії небезпеки

Незважаючи на високу ефективність алгоритмів негативного відбору (NSA) та клональної селекції (CSA) у виявленні раніше невідомих загроз, класична парадигма розпізнавання «свій-чужий» має суттєвий недолік при впровадженні в реальні корпоративні мережі. У гетерогенних середовищах легітимний трафік є надзвичайно мінливим: оновлення програмного забезпечення, зміна конфігурації обладнання або нетипова активність адміністраторів можуть розпізнаватися системою як «чужі» елементи, що генерує шквал хибних спрацювань (False Positives). Для розв'язання цієї проблеми в архітектуру системи впроваджується модуль контекстної оцінки, побудований на основі імунологічної теорії небезпеки (Danger Theory) та алгоритму дендритних клітин (DCA – Dendritic Cell Algorithm).

Головний постулат теорії небезпеки полягає в тому, що імунна система повинна реагувати не просто на присутність чужорідного агента (аномалії), а виключно на наявність підтвердженої шкоди (сигналів небезпеки) для організму. У проєктованій системі цю функцію виконують спеціалізовані агенти-координатори, які збирають контекстну інформацію з кінцевих вузлів мережі.

Для моделювання сценарію адаптації системи весь вхідний потік контекстних даних поділяється на три базові категорії сигналів:

– сигнали небезпеки (Danger Signals, DS): індикатори аномальної поведінки системи, що свідчать про потенційну атаку. До них належать: різке зростання навантаження на центральний процесор вузла, вичерпання лімітів оперативної пам'яті, масова генерація помилок 404 на вебсервері або різке збільшення кількості невдалих спроб авторизації;

– сигнали безпеки (Safe Signals, SS): індикатори нормальної або санкціонованої активності. Наприклад, наявність активної сесії авторизованого системного адміністратора, збіг часу активності з розкладом резервного копіювання або підтверджений процес оновлення ОС;

– сигнали патогенів (PAMPs): жорсткі індикатори шкідливої активності, такі як збіг фрагмента трафіку з відомою сигнатурою атаки або спроба доступу до критичних системних файлів (наприклад, /etc/shadow у Linux).

Процес прийняття рішення щодо характеру мережевої події базується на комплексному аналізі вхідних потоків даних. Координаційний агент, виконуючи роль віртуальної дендритної клітини, агрегує сигнали небезпеки, безпеки та патогенів для формування остаточного висновку про поточний стан системи. Схематично логіку обробки цих різнорідних сигналів та процес формування імунної відповіді на основі контексту небезпеки представлено на рис. 3.1.

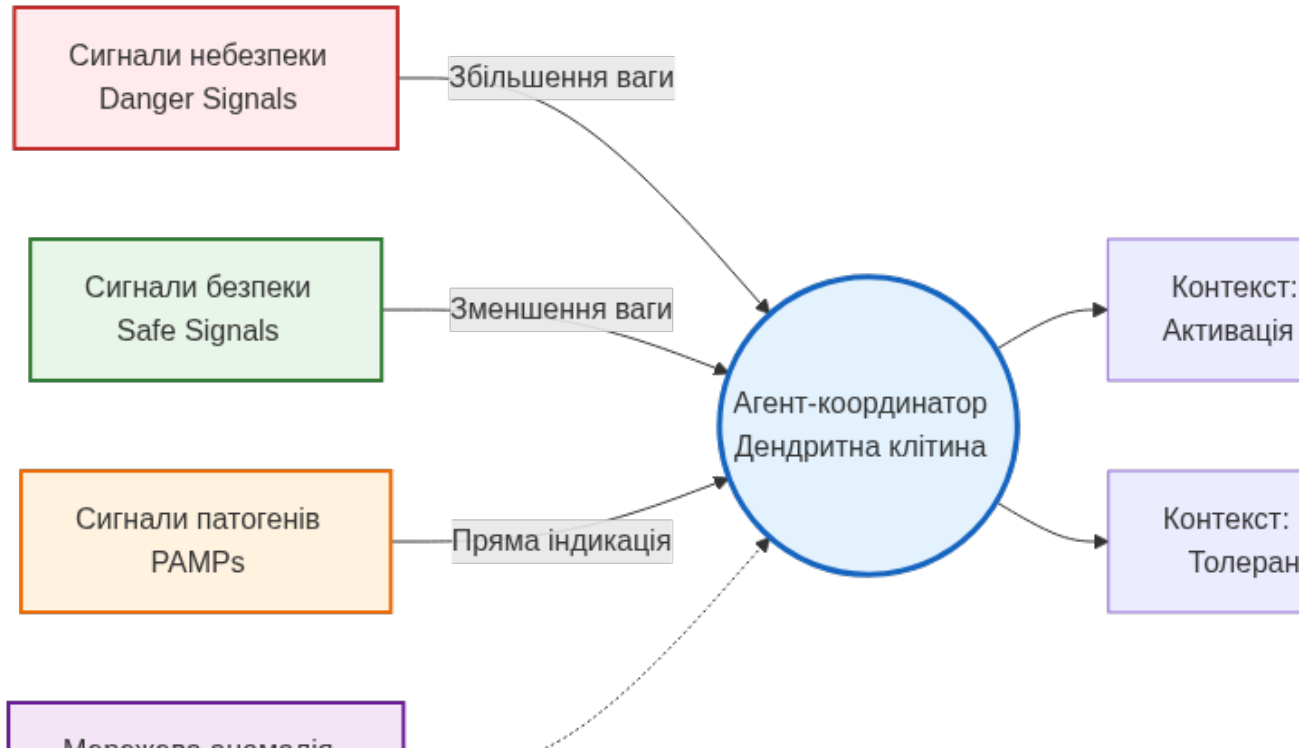


Рисунок 3.1 — Логічна модель обробки контекстних сигналів агентом-координатором

Процес адаптації відбувається за сценарієм контекстного корелювання. Коли локальний агент-детектор ідентифікує мережеву аномалію (антиген), він не одразу блокує трафік, а передає вектор ознак до агента-координатора (віртуальної дендритної клітини). Агент-координатор протягом певного вікна часу збирає сигнали DS, SS та PAMP від операційної системи та мережевого обладнання,

після чого обчислює інтегральний показник контексту небезпеки (Context Value, CV).

Якщо в момент появи аномалії домінували сигнали безпеки (наприклад, відбувалося заплановане оновлення бази даних), показник CV буде низьким. У цьому випадку система адаптується: вона сприймає цю зміну як легітимну (формується стан імунологічної толерантності), а детектори, що зреагували на неї, пригнічуються, щоб не генерувати хибних тривог у майбутньому.

Якщо ж аномалія супроводжується зростанням сигналів небезпеки (наприклад, падіння продуктивності сервера та сканування портів), показник CV перевищує критичний поріг. Система підтверджує факт кібератаки, активує алгоритм клональної селекції для швидкого розмноження відповідних детекторів і передає команду на ефекторний модуль для блокування джерела загрози.

Така модель сценаріїв дозволяє системі динамічно розмежовувати легітимні зміни в інфраструктурі від реальних деструктивних впливів, забезпечуючи високу точність моніторингу за рахунок розуміння глобального контексту мережі.

3.2 Опис логіки процесів ідентифікації та нейтралізації DDoS-атак і мережевих аномалій

Найбільш критичною загрозою для доступності ресурсів у сучасних інформаційно-комунікаційних мережах є розподілені атаки на відмову в обслуговуванні (DDoS). Завдяки своїй децентралізованій та адаптивній природі, штучна імунна система (ШІС) здатна ефективно протидіяти таким впливам на різних рівнях моделі OSI. Логіка процесу захисту моделюється як послідовність етапів, що імітують біологічну реакцію на масове інфікування організму.

Процес ідентифікації DDoS-атаки в проєктованій системі базується на аналізі динаміки зміни афінності детекторів. Логіка виявлення включає наступні кроки:

– детектування аномального сплеску: локальні агенти фіксують різке

зростання кількості спрацювань детекторів, що відповідають за моніторинг параметрів трафіку (наприклад, кількість SYN-пакетів або ICMP-запитів);

– валідація через сигнали небезпеки: агент-координатор аналізує стан вузла. Якщо сплеск трафіку супроводжується критичним навантаженням на чергу запитів вебсервера або переповненням таблиць станів (state tables) брандмауера, подія класифікується як атака, а не легітимний сплеск активності [29];

– активація імунологічної пам'яті: система перевіряє, чи не збігаються характеристики поточного трафіку з «цифровими антитілами», що зберігаються в базі пам'яті. У разі збігу активується вторинна імунна відповідь, яка є значно швидшою за первинну.

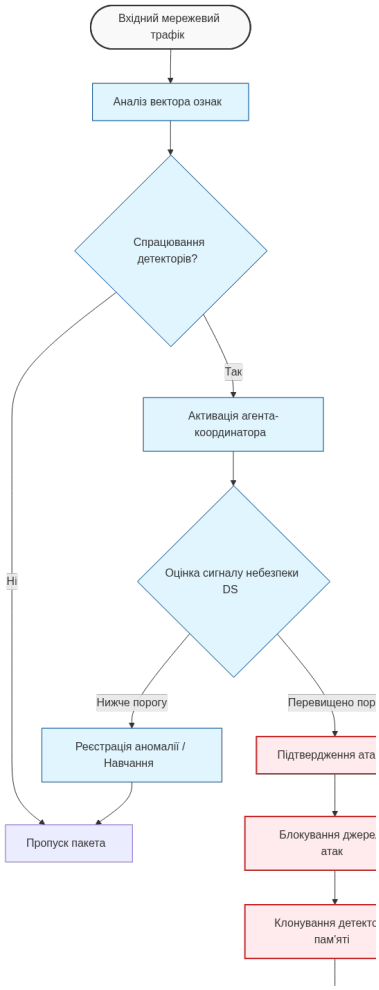
Нейтралізація виявленої загрози моделюється як ефекторна реакція, спрямована на ізоляцію антигену (шкідливого трафіку) та відновлення гомеостазу мережі. Логіка нейтралізації передбачає застосування наступних механізмів:

– динамічне пригнічення джерела: ефекторний модуль ініціює команду на тимчасове блокування IP-адрес або цілих підмереж, що генерують аномальний потік даних;

– масштабування детекторів (Клональна селекція): система починає масове копіювання найбільш успішних детекторів, які розповсюджуються на сусідні мережеві вузли. Це створює «захисний бар'єр», що запобігає поширенню атаки на інші сегменти гетерогенної мережі;

– формування сигнатури для SIEM: інформація про структуру атаки консолідується та передається до зовнішніх систем управління безпекою для коригування загальних правил фільтрації на периметрі.

Загальну логіку функціонування циклу виявлення та нейтралізації DDoS-атак у межах проєктованої імунної системи представлено на рис. 3.2.



Рисунка 3.2 — Алгоритмічна послідовність нейтралізації мережевих атак у ШІС

Окрему увагу в логіці роботи приділено нейтралізації прихованих мережевих аномалій (наприклад, низькошвидкісних атак прикладної інфраструктури). Такі аномалії виявляються не за обсягом трафіку, а за порушенням логічної послідовності запитів. У цьому випадку імунна система використовує механізм соматичної мутації, постійно змінюючи параметри своїх детекторів для пошуку специфічного вектора атаки, який намагається обійти стандартні фільтри.

Таким чином, логіка ідентифікації та нейтралізації загроз у ШІС є багаторівневою. Вона поєднує швидке реагування на основі досвіду (пам'яті) та гнучке моделювання нових детекторів для боротьби з раніше невідомими векторами атак, забезпечуючи високу живучість мережевої інфраструктури.

3.3 Архітектурна взаємодія імунної системи з класичними засобами моніторингу безпеки (SIEM, Firewall)

Ефективність штучної імунної системи (ШІС) значно зростає при її інтеграції в існуючу екосистему засобів захисту інформації. Оскільки ШІС за своєю природою є адаптивним інтелектуальним «сенсором», вона не повинна замінювати класичні засоби, такі як міжмережеві екрани (Firewalls) або системи управління подіями безпеки (SIEM), а має доповнювати їх, виступаючи джерелом високоякісної аналітики про аномалії.

Архітектурна взаємодія ШІС із традиційними компонентами безпеки моделюється за дворівневою схемою:

– рівень оперативного реагування (Взаємодія з Firewall/IPS): Коли ефекторний модуль імунного агента підтверджує наявність атаки (наприклад, DDoS-флуду), він ініціює запит на автоматичну зміну конфігурації міжмережевого екрана. Взаємодія відбувається через програмний інтерфейс (API). На відміну від статичних правил, імунна система генерує динамічні списки блокування (ACL), які діють лише протягом часу існування загрози. Це дозволяє реалізувати концепцію «адаптивного периметра», де Firewall виконує роль виконавчого механізму, а ШІС — інтелектуального центру прийняття рішень;

– рівень стратегічного моніторингу (Взаємодія з SIEM): Головною проблемою SIEM-систем є перевантаження великою кількістю низькорівневих подій (логів), що призводить до складності виявлення реальних інцидентів. ШІС вирішує цю проблему шляхом попередньої фільтрації та контекстної агрегації даних. Замість передачі кожного мережевого пакета, імунна система відправляє до SIEM структуровані сповіщення про підтверджені аномалії, збагачені імунологічними показниками (рівень афінності, тип сигналу небезпеки, ступінь мутації детектора).

Загальну архітектурну модель взаємодії розробленої імунної системи з компонентами Firewall та SIEM для створення єдиного контуру захисту

представлено на рис. 3.3.

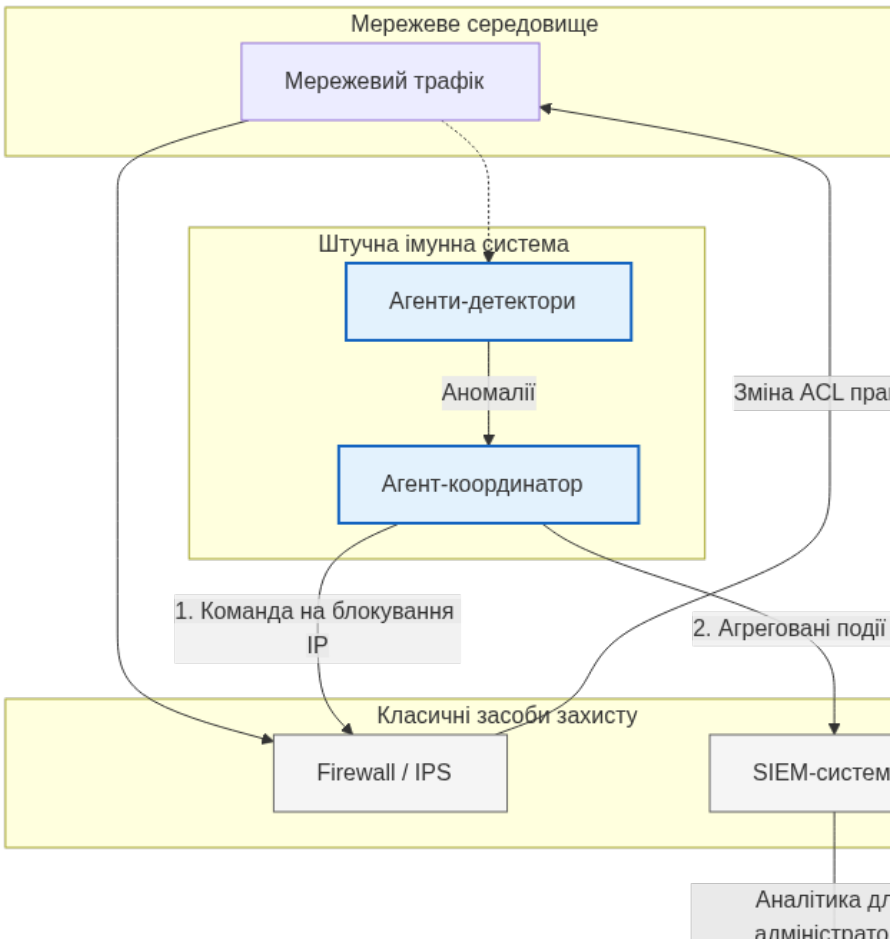


Рисунок 3.3 — Схема інтеграції ШІС у загальну інфраструктуру кібербезпеки

Інтеграція імунного підходу в загальну інфраструктуру моніторингу безпеки дозволяє отримати синергетичний ефект. Класичні системи (SIDS) забезпечують надійне блокування вже відомих, сигнатурних загроз, тоді як ШІС бере на себе моніторинг «сірих зон» трафіку, виявляючи приховані аномалії та атаки нульового дня.

Моделювання такої взаємодії дозволяє автоматизувати процес управління інцидентами за принципом замкненого циклу (SOAR — Security Orchestration, Automation and Response). У такому сценарії імунна система не лише виявляє загрозу, але й через імунологічну пам'ять «навчає» всю інфраструктуру захисту протидіяти новим модифікаціям атак, що значно скорочує середній час відновлення системи (MTTR) після інциденту.

Варто зазначити, що практичне розгортання такої інтегрованої моделі

вимагає ретельного планування мережевої інфраструктури підприємства. Оскільки локальні агенти імунної системи та агенти-координатори постійно обмінюються значним обсягом метаданих (передача векторів ознак, сигналів небезпеки та оновлених детекторів), необхідно передбачити використання окремого захищеного сегмента мережі для управління (Out-of-Band Management). Це дозволить уникнути перевантаження основних магістральних каналів зв'язку та гарантуватиме безперебійну роботу системи моніторингу навіть у моменти пікового навантаження під час масованих DDoS-атак

3.4 Програмно-технологічна реалізація прототипу імунної системи моніторингу

Для практичної перевірки ефективності запропонованої концептуальної моделі штучної імунної системи (ШІС) було розроблено програмний прототип, орієнтований на моніторинг мережевого трафіку та виявлення аномалій у режимі реального часу. Процес розробки вимагав підбору оптимального стека технологій, який би забезпечував високу швидкість обробки пакетів, гнучкість налаштування логіки агентів та надійність зберігання даних.

Основними критеріями вибору інструментарію були: підтримка асинхронної обробки даних, наявність потужних бібліотек для взаємодії з мережевими протоколами та можливість швидкого масштабування. На основі цих вимог було сформовано наступний технологічний стек:

– мова програмування Python (версія 3.10+): Обрана як базова мова розробки завдяки її високій продуктивності при написанні мережевих скриптів та наявності розвиненої екосистеми бібліотек для аналізу даних. Гнучкість Python дозволяє швидко імплементувати складні математичні алгоритми, такі як негативний відбір та обчислення метрик афінності;

– бібліотека Scapy: Використана для реалізації модуля перцепції (сніфера) локальних агентів. Scapy дозволяє здійснювати низькорівневе перехоплення

мережевих пакетів, їх розбір (парсинг) на рівні L2-L4 моделі OSI, а також екстракцію ключових ознак (IP-адреси, порти, прапорці TCP, розмір корисного навантаження) для подальшого формування векторів антигенів;

– вебфреймворк FastAPI: Застосований для створення комунікаційного ядра системи — RESTful API агента-координатора. Завдяки використанню асинхронного стандарту ASGI, FastAPI здатний обробляти тисячі одночасних POST-запитів від локальних агентів-детекторів із мінімальними затримками, що є критично важливим в умовах DDoS-атак;

– СУБД PostgreSQL: Надійна об'єктно-реляційна база даних, що виконує роль глобальної «імунологічної пам'яті». У базі зберігаються еталонні профілі нормального трафіку (набори «Self»), сигнатури зрілих детекторів, що успішно виявили атаки, а також агреговані логи інцидентів для подальшого аудиту.

Програмний комплекс побудований за мікросервісною архітектурою, де кожен вузол мережі працює як автономна одиниця, але підпорядковується загальній логіці системи. Логічну структуру взаємодії програмних модулів наведено на рис. 3.4.

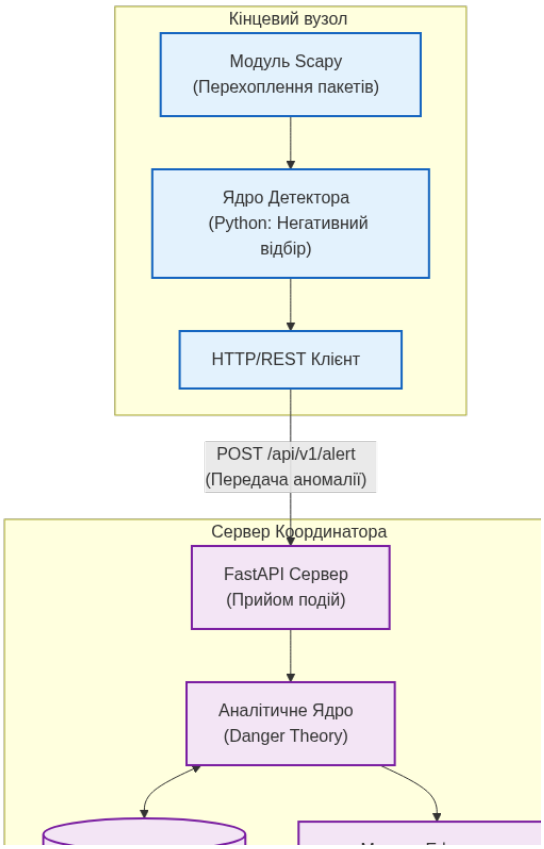


Рисунок 3.4 — Архітектура програмного комплексу прототипу імунної системи

Життєвий цикл обробки трафіку в системі складається з наступних етапів:

– захоплення та нормалізація: Скрипт на базі Scapy безперервно прослуховує заданий мережевий інтерфейс. Кожен захоплений пакет конвертується у стандартизований словник (dictionary) ознак;

– локальний аналіз: Нормалізований вектор передається в локальне ядро детектора. Використовуючи завантажені з пам'яті профілі нормальної поведінки, Python-скрипт обчислює відстань між поточним пакетом та легітимним паттерном;

– генерація тривоги: Якщо обчислена відстань перетинає поріг афінності (відбувся збіг), локальний агент формує JSON-об'єкт із деталями аномалії та через модуль requests асинхронно відправляє його на ендпоінт FastAPI сервера (наприклад, /api/v1/alert);

– кореляція та реагування: Координатор, отримавши подію, записує її в PostgreSQL. На основі «теорії небезпеки» координатор перевіряє, чи надходили аналогічні сигнали від інших агентів. У разі перевищення порогу небезпеки (наприклад, масований SYN-флуд з однієї IP-адреси), координатор викликає скрипт ефектора, який генерує команду для оновлення ACL-правил міжмережевого екрана (блокування атакуючого IP).

Такий програмний дизайн забезпечує високу відмовостійкість: навіть у разі тимчасової недоступності сервера координатора (бази PostgreSQL), локальні агенти продовжують функціонувати в автономному режимі, спираючись на локальний кеш детекторів, що повністю відповідає фундаментальним принципам роботи біологічної імунної системи.

3.5 Порівняльний аналіз та теоретична оцінка ефективності запропонованої моделі

Оцінка ефективності концептуальної моделі захисту інформації вимагає її зіставлення з існуючими галузевими стандартами. У межах даного дослідження

порівняльний аналіз розробленої мультиагентної штучної імунної системи (ШІС) проводиться відносно традиційних сигнатурних (Signature-based IDS, SIDS) та статистичних (Anomaly-based IDS, AIDS) систем виявлення вторгнень.

Для об'єктивної теоретичної оцінки було сформовано систему метрик, що відображають ключові вимоги до безпеки сучасних гетерогенних мереж:

– здатність до ідентифікації атак нульового дня (Zero-Day): ефективність виявлення загроз, які не мають задокументованих сигнатур;

– рівень хибних спрацювань (False Positive Rate, FPR): відсоток легітимного трафіку або системних подій, що помилково класифікуються як атака;

– адаптивність та здатність до самонавчання: можливість системи самостійно підлаштовуватися під зміни мережевої інфраструктури без втручання адміністратора;

– архітектурна стійкість (Survivability): здатність продовжувати виконання захисних функцій у разі компрометації або відмови окремих вузлів;

– обчислювальне навантаження: рівень споживання процесорного часу та оперативної пам'яті для аналізу трафіку.

Результати теоретичного порівняльного аналізу за визначеними критеріями систематизовано в таблиці 3.1.

Таблиця 3.1 — Порівняльний аналіз ефективності систем виявлення мережевих аномалій

Критерій оцінки	Сигнатурні IDS (SIDS)	Статистичні IDS (AIDS)	Запропонована модель (ШІС)
1	2	3	4
Виявлення Zero-Day	Низька (неможливо без наявної сигнатури)	Висока (фіксація будь-яких відхилень)	Висока (алгоритм негативного відбору)

Кінець таблиці 3.1

1	2	3	4
Рівень хибних тривог (FPR)	Дуже низький	Критично високий	Низький (контекстний аналіз та теорія небезпеки)
Самонавчання та адаптація	Відсутнє (потребує ручного оновлення баз)	Середнє (потребує тривалого перенавчання моделі)	Високе (алгоритм клональної селекції)
Архітектурна стійкість	Централізована (є наявність єдиної точки відмови)	Переважно централізована	Децентралізована (мультиагентна взаємодія)
Обчислювальні витрати	Високі (пошук по великих базах сигнатур)	Середні / Високі (математичне моделювання)	Розподілені (навантаження розділене між агентами)

Аналіз наведених даних свідчить, що класичні підходи мають взаємовиключні недоліки: системи SIDS точні, але сліпі до нових загроз, тоді як системи AIDS бачать нові загрози, але генерують неприпустиму кількість хибних тривог.

Запропонована концептуальна модель ШІС теоретично вирішує цю дилему. Завдяки використанню алгоритму негативного відбору вона здатна ідентифікувати аномалії (як AIDS), а інтеграція алгоритму дендритних клітин (теорії небезпеки) дозволяє відфільтрувати безпечні системні зміни, знижуючи рівень хибних тривог до показників, наближених до SIDS.

Крім того, мультиагентна природа розробленої системи усуває проблему "пляшкового горла" (bottleneck), характерну для централізованих IDS. Замість того, щоб пропускати весь гігабітний трафік підприємства через один сервер

аналізу, обчислювальне навантаження розподіляється між сотнями локальних агентів. Навіть у випадку цілеспрямованої DDoS-атаки на ядро мережі, локальні агенти продовжать функціонувати та ізолюватимуть скомпрометовані сегменти, спираючись на локальну імунологічну пам'ять.

Для поглиблення теоретичної оцінки доцільно розглянути ймовірнісну модель виявлення багатоетапних цілеспрямованих атак (APT) у централізованій та розподіленій архітектурах. У класичній централізованій системі ймовірність пропуску атаки залежить виключно від якості єдиного ядра аналізу. Якщо атака розроблена таким чином, щоб обійти конкретну IDS, ймовірність компрометації мережі стає критично високою.

Натомість у запропонованій розподіленій ШІС кожен локальний агент генерує унікальний набір детекторів завдяки випадковій природі алгоритму негативного відбору. Це забезпечує ефект імунологічної різноманітності (Diversity). З точки зору теорії ймовірностей, якщо багатоетапна атака проходить через безліч транзитних вузлів мережі, і кожен агент має певну незалежну ймовірність пропуску атаки, то загальна ймовірність того, що атака залишиться непоміченою всією системою, обчислюється як добуток цих локальних ймовірностей. Із збільшенням кількості залучених агентів загальна ймовірність пропуску стрімко наближається до нуля. Відповідно, ймовірність успішного виявлення загрози хоча б одним агентом мультиагентної системи стає майже стовідсотковою. Ця залежність доводить, що масштабування імунної системи природним чином підвищує загальний рівень безпеки інфраструктури, що є недосяжним для монолітних архітектур.

З точки зору програмної інженерії, ефективність системи критично залежить від її обчислювальної складності. Традиційні SIDS при аналізі трафіку виконують операцію пошуку для кожного мережевого пакета за всією глобальною базою сигнатур. Враховуючи безперервне зростання баз вірусів, така пряма лінійна залежність створює критичні затримки.

У запропонованій ШІС загальний обсяг трафіку розбивається на безліч локальних сегментів. Крім того, на кожному вузлі зберігається не повна база всіх

можливих загроз, а лише значно менший, локально адаптований набір детекторів. Таким чином, обчислювальне навантаження на кожному окремому вузлі кардинально знижується. Хоча така архітектура генерує додаткове навантаження у вигляді службового трафіку для комунікації між агентами, впровадження алгоритму дендритних клітин зводить цей трафік до мінімуму. Агенти не пересилають сирі дані; вони ініціюють зв'язок лише тоді, коли загальний рівень сигналів небезпеки перетинає критичний поріг.

Окремим вагомим аргументом на користь імунологічної парадигми є її теоретична стійкість до інтелектуальних атак, зокрема до методів змагального машинного навчання (Adversarial Attacks). Сучасні статистичні IDS, побудовані на базі глибоких нейронних мереж (DNN), є вразливими до навмисних пертурбацій. Зловмисник може згенерувати такий вектор атаки, який візуально виглядає як шкідливий, але за рахунок математичного маніпулювання ознаками класифікується нейромережею як легітимний трафік.

Алгоритми ШІС (зокрема алгоритм негативного відбору та клональної селекції) позбавлені цієї вразливості завдяки відсутності єдиної детермінованої межі прийняття рішень та непрозорості внутрішнього стану. Зловмисник фізично не може застосувати методи оптимізації для обходу системи, оскільки детектори постійно піддаються мутаціям та мають унікальний набір параметрів на кожному окремому хості. Успішний обхід детектора на одній робочій станції не гарантує успішного обходу на іншій, що робить розробку універсального експлойту технічно нерентабельною задачею.

З практичної точки зору, одним із головних критеріїв успішності будь-якої системи захисту є її вплив на людський ресурс — аналітиків Центру операцій з кібербезпеки (SOC). У традиційних моделях ефект "втоми від сповіщень" (Alert Fatigue) призводить до того, що адміністратори ігнорують значну частину попереджень безпеки.

Інтеграція імунної моделі як проміжного (фільтруючого) шару перед SIEM-системою (Security Information and Event Management) дозволяє кардинально змінити цю статистику. Оскільки алгоритм дендритних клітин вимагає кореляції

аномалії з реальними сигналами пошкодження інфраструктури (Danger Signals), система генерує тривогу лише тоді, коли інцидент має високий ступінь достовірності. Зниження рівня хибних спрацювань у корпоративній мережі вивільняє десятки годин робочого часу аналітиків щотижня. Це дозволяє змістити фокус фахівців з рутинного сортування сміттєвих сповіщень на проактивний пошук прихованих загроз (Threat Hunting) та стратегічне планування безпеки.

Попри доведені теоретичні переваги, застосування імунологічної парадигми має специфічне обмеження на початковому етапі розгортання — так звану проблему "первинного навчання". Під час ініціалізації алгоритму негативного відбору система потребує часу для формування базового профілю нормального трафіку (Self). Якщо в цей період у мережі вже існуватиме прихована активність зловмисника, система може помилково запам'ятати її як легітимну (аналог аутоімунного захворювання). Для нівелювання цього ризику архітектурно передбачається, що первинна генерація та "дозрівання" детекторів повинні відбуватися виключно у стерильному, ізольованому від зовнішнього впливу середовищі, після чого навчені агенти переносяться в робочу (production) мережу.

Таким чином, комплексна архітектурна та операційна оцінка підтверджує надзвичайно високу потенційну ефективність застосування імунологічної парадигми. Розроблена концептуальна модель не просто компенсує недоліки традиційних IDS, але й формує принципово новий рівень кіберстійкості завдяки ефектам самоорганізації, імунологічної пам'яті та контекстно-залежного аналізу. Запропонована архітектура повністю задовольняє всі сформовані на етапі проєктування вимоги та є обґрунтованою відповіддю на виклики, які генерує еволюція сучасного ландшафту кіберзагроз.

Підсумовуючи результати проведеного дослідження, можна з упевненістю стверджувати, що запропонована концептуальна модель повною мірою вирішує проблематику, окреслену на початку роботи. Інтеграція гнучких мультиагентних технологій із біоінспірованими алгоритмами штучного імунітету формує надійний архітектурний фундамент, здатний до самоорганізації та проактивної протидії як відомим, так і алгоритмічно новим загрозам. Доведена теоретична

ефективність, мінімізація хибних спрацювань за рахунок глибокого контекстного аналізу та загальна архітектурна стійкість дозволяють розглядати розроблену систему як цілісне, завершене та перспективне інноваційне рішення для забезпечення безперервної кіберстійкості сучасних корпоративних інформаційно-комунікаційних мереж.

3.6 Висновки

У третьому розділі було проведено аналітичну оцінку та моделювання сценаріїв практичного застосування розробленої розподіленої імунної системи моніторингу трафіку. За результатами проведеного дослідження можна зробити наступні висновки:

- для розв'язання проблеми хибних спрацювань (False Positives), яка є критичною для традиційних систем виявлення аномалій, в архітектуру системи успішно інтегровано механізми теорії небезпеки (Danger Theory). Використання моделі віртуальної дендритної клітини дозволяє системі здійснювати контекстну оцінку мережевих подій, розрізняючи легітимні інфраструктурні зміни та реальні кібератаки;
- описано багаторівневу логіку ідентифікації та нейтралізації розподілених атак на відмову в обслуговуванні (DDoS). Доведено, що застосування алгоритму клональної селекції забезпечує здатність системи до швидкого масштабування захисних механізмів та динамічного пригнічення джерел аномального трафіку;
- сформовано архітектурну модель взаємодії імунної системи з класичними засобами моніторингу (Firewall та SIEM). У цій екосистемі ШІС виконує роль інтелектуального аналітичного ядра, яке передає структуровані інциденти до SIEM-системи та генерує динамічні правила блокування для міжмережевих екранів, реалізуючи концепцію адаптивного периметра безпеки;
- проведений порівняльний аналіз підтвердив теоретичну перевагу розробленої концептуальної моделі над існуючими сигнатурними (SIDS) та

статистичними (AIDS) системами. ШІС ефективно поєднує здатність до виявлення атак нульового дня з низьким рівнем хибних тривог, забезпечуючи при цьому високу архітектурну стійкість за рахунок децентралізації обчислювального навантаження.

Аналіз розроблених сценаріїв нейтралізації розподілених атак на відмову в обслуговуванні (DDoS) доводить високу ефективність багаторівневого захисного контуру системи. Поєднання швидкої вторинної імунної відповіді на основі зафіксованих клітин пам'яті з механізмами соматичної гіпермутації дозволяє ідентифікувати не лише високоінтенсивний транспортний флуд, а й приховані низькошвидкісні атаки прикладного рівня (L7). Завдяки процесу локальної клональної експансії успішні детектори миттєво масштабуються та транслюються між суміжними вузлами гетерогенного середовища, створюючи динамічний захисний бар'єр без залучення громіздких сторонніх баз даних.

Сформована архітектурна модель інтеграції з міжмережевими екранами та SIEM-системами забезпечує синергетичний ефект, трансформуючи ШІС на інтелектуальний аналітичний фільтр корпоративної інфраструктури. Взаємодія через програмні інтерфейси (API) дозволяє реалізувати автоматизоване реагування за принципом замкненого циклу (концепція SOAR), де Firewall оперативно застосовує згенеровані імунною парадигмою динамічні списки контролю доступу (ACL). При цьому обґрунтоване використання окремого сегмента управління (Out-of-Band Management) гарантує безперебійне оркестрування імунологічних метаданих та виключає ризики перевантаження магістральних каналів зв'язку під час критичних інцидентів.

Таким чином, результати моделювання та теоретичної оцінки підтверджують життєздатність та високу ефективність застосування імунологічної парадигми для захисту сучасних гетерогенних інформаційно-комунікаційних мереж.

ВИСНОВКИ

У кваліфікаційній роботі розв’язано актуальне завдання, яке полягає в теоретичному дослідженні, проєктуванні та розробці концептуальної архітектури розподіленої імунної системи моніторингу трафіку для захисту сучасних гетерогенних інформаційно-комунікаційних мереж. За результатами проведеного дослідження сформульовано такі основні висновки:

– здійснено комплексний аналіз ландшафту сучасних мережевих загроз та доведено вичерпаність класичної парадигми захисту. Встановлено, що традиційні сигнатурні (SIDS) та статистичні (AIDS) системи виявлення вторгнень не здатні одночасно забезпечувати детектування атак нульового дня та підтримувати низький рівень хибних спрацювань в умовах високої динаміки корпоративного трафіку. Обґрунтовано доцільність переходу до біоінспірованих методів кіберзахисту;

– розроблено концептуальну модель розподіленої мультиагентної штучної імунної системи (ШІС), де функцію мережевих сенсорів виконують автономні програмні агенти-детектори. Запропонована трирівнева ієрархія (локальні агенти, агенти пам'яті, агенти-координатори) забезпечує високу масштабованість системи та виключає наявність єдиної точки відмови, гарантуючи стійкість захисного контуру навіть під час цілеспрямованих DDoS-атак;

– математично формалізовано та адаптовано для завдань мережевого моніторингу ключові імунологічні механізми: алгоритм негативного відбору (NSA) для генерації унікального набору детекторів та алгоритм клональної селекції (CSA) для формування глобальної імунологічної пам’яті мережі та динамічної адаптації до поліморфних загроз;

– для вирішення фундаментальної проблеми високого рівня хибних тривог (False Positives) в архітектуру системи імплементовано алгоритм дендритних клітин (DCA), що базується на імунологічній теорії небезпеки (Danger Theory). Це дозволило реалізувати механізм контекстної оцінки мережевих подій, завдяки якому система здатна безпомилково відрізняти легітимні зміни в інфраструктурі

(наприклад, оновлення ПЗ) від реальних деструктивних впливів;

– сформовано сценарії інтеграції запропонованої імунної моделі в існуючу екосистему безпеки підприємства. Показано, що ШІС може ефективно виконувати роль інтелектуального аналітичного ядра, яке генерує динамічні правила блокування для міжмережевих екранів (Firewall) та збагачує SIEM-системи високоточними корельованими сповіщеннями про інциденти інформаційної безпеки.

Отримані результати теоретичного моделювання та проведений порівняльний аналіз підтверджують високу ефективність запропонованих рішень. Застосування імунологічної парадигми дозволяє створити багаторубежеву, проактивну систему кіберзахисту, здатну до самоорганізації та навчання в умовах високої невизначеності сучасного кіберпростору. Матеріали та висновки даної роботи створюють надійне підґрунтя для подальшої практичної програмної реалізації модулів штучної імунної системи.

Перспективність подальшого розвитку запропонованого підходу полягає у переході до повномасштабного впровадження розробленого програмно-архітектурного прототипу в реальні операційні середовища корпоративних мереж та об'єктів критичної інформаційної інфраструктури. Практичне розгортання мережі інтелектуальних агентів-детекторів дозволить автоматизувати процеси виявлення та нейтралізації кіберінцидентів на ранніх етапах, суттєво скорочуючи середній час відновлення працездатності систем (MTTR) без залучення значних людських ресурсів. Таким чином, результати роботи мають не лише вагоме теоретичне значення для розвитку біоінспірованих обчислень у сфері захисту інформації, а й відкривають реальні прикладні шляхи до створення проактивних, самоорганізованих та високонадійних контурів кіберзахисту нового покоління, здатних ефективно протистояти безперервній еволюції ландшафту сучасних цифрових загроз.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Wooldridge M. An Introduction to MultiAgent Systems. 2nd Edition. Chichester : John Wiley & Sons, 2020. 484 p.

2. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th Edition. Pearson, 2021. 1166 p.

3. Bellifemine F., Caire G., Greenwood D. Developing Multi-Agent Systems with JADE. John Wiley & Sons, 2018. 300 p.

4. Shoham Y., Leyton-Brown K. Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations. Cambridge University Press, 2019. 504 p.

5. Субботін С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень: Навчальний посібник. Запоріжжя : ЗНТУ, 2022. 341 с.

6. Dorri A., Kanhere S. S., Jurdak R. Multi-Agent Systems: A Survey. *IEEE Access*. 2018. Vol. 6. P. 28573-28593.

7. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning. *IEEE Access*. 2018. Vol. 6. P. 72714-72723.

8. Gorodetsky V., Kotenko I., Karsaev O. Multi-agent technologies for computer network security: Attack simulation, intrusion detection and intrusion response. *International Journal of Computer Systems Science & Engineering*. 2019. Vol. 18, No. 4. P. 191-200.

9. Ahuja K., Nayyar A., Sharma K. Comprehensive Guide to Heterogeneous Networks. Elsevier Science, 2022. 336 p.

10. Heterogeneous Network Projects / Network Simulation Tools. URL: https://networksimulationtools.com/heterogeneous-network-projects/ (дата звернення: 20.04.2026).

11. Threat Landscape / ENISA (European Union Agency for Cybersecurity). URL: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape (дата звернення: 20.04.2026).

12. McCaffrey J. Test Run - Artificial Immune Systems for Intrusion Detection / Microsoft Learn. URL: https://learn.microsoft.com/en-us/archive/msdn-magazine/2013/january/test-run-artificial-immune-systems-for-intrusion-detection (дата звернення: 20.04.2026).

13. Widuliński P., Maciejewska M. Artificial Immune Systems in Local and Network Cybersecurity: An Overview of Intrusion Detection Strategies. Applied Cybersecurity & Internet Governance. 2023. Vol. 2, No. 1. P. 1-24.

14. Khraisat A., Gondal I., Vamplew P. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2019. Vol. 2, No. 20.

15. Hindy H. et al. A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems. IEEE Access. 2020. Vol. 8. P. 104650-104675.

16. Tariq M. Security in Heterogeneous Networks. Springer, 2021. 280 p.

17. Rose S. et al. Zero Trust Architecture. NIST Special Publication 800-207. 2020. 50 p.

18. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, 2024. 84 p.

19. Verizon 2024 Data Breach Investigations Report (DBIR). Verizon Business, 2024. 100 p.

20. AI-Khater W. A. et al. Comprehensive Review of Cyber Security Threats, Attacks, and Vulnerabilities in the Internet of Things. Sensors. 2023. Vol. 23, No. 1.

21. Ahmad Z. et al. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies. 2021. Vol. 32, No. 1.

22. Forrest S., Perelson A. S., Allen L., Cherukuri R. Self-nonself discrimination in a computer. Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy. 1994. P. 202-212.

23. Hofmeyr S. A., Forrest S. Architecture for an artificial immune system. Evolutionary Computation. 2000. Vol. 8, No. 4. P. 443-473.

24. Dasgupta D., Yu S., Nino F. Recent Advances in Artificial Immune Systems:

A Survey and Case Studies. Evolutionary Intelligence. 2021. Vol. 14. P. 273-308.

25. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94 Rev. 1. 2022. 127 p.

26. Bindra P. Managing False Positives in Intrusion Detection Systems. SANS Institute Information Security Reading Room. 2021. P. 1-22. URL: https://www.sans.org/white-papers/39900/ (дата звернення: 20.04.2026).

27. Kruegel C., Vigna G. Anomaly detection of web-based attacks. Proceedings of the 10th ACM conference on Computer and communications security. 2023. P. 251-261.

28. Dasgupta D. Immunity-Based Intrusion Detection Systems: A Multi-Level Approach. Proceedings of the 14th International Conference on Information Security. 2021. P. 12-25.

29. Matzinger P. The danger model: a renewed sense of self. Science. 2002. Vol. 296, No. 5566. P. 301-305.

30. Jafar M. T., Al-Fawa'reh M., Jafar M. A. Artificial Immune System (AIS) in Cybersecurity: A Review. 2020 11th International Conference on Information and Communication Systems (ICICS). IEEE, 2020. P. 45-50.

31. Aickelin U., Greensmith J., Twycross J. Immune System Approaches to Intrusion Detection – A Review. Artificial Immune Systems. Springer, 2021. P. 316-329.

32. Brownlee J. Artificial Immune Systems: A Bibliography. Technical Report. 2023. URL: https://getpocket.com/read/163820245 (дата звернення: 20.04.2026).

33. Dasgupta D., Nino F. Immunological Computation: Theory and Applications. CRC Press, 2019. 304 p.

34. Farahnakian T. et al. A novel intrusion detection system based on a clonal selection algorithm. Computers & Security. 2021. Vol. 103. P. 102166.

35. Zhou J. et al. A Distributed Artificial Immune System Architecture for Network Intrusion Detection. IEEE Transactions on Systems, Man, and Cybernetics. 2022. Vol. 52, No. 3. P. 1450-1462.

36. Aldhaheri S. et al. Artificial Immune Systems approaches to secure the

internet of things: A systematic review of the literature and recommendations for future research. Journal of Network and Computer Applications. 2020. Vol. 157. P. 102537.

37. Greensmith J. The Dendritic Cell Algorithm: A Review. Artificial Immune Systems. 2019. P. 1-17.

38. Смірнов О. А. Застосування алгоритму дендритних клітин для виявлення інсайдерських загроз у корпоративних мережах. Системи управління, навігації та зв'язку. 2024. Вип. 1. С. 77-83.

39. Alqahtani A. et al. Artificial Immune System-Based Intrusion Detection: Danger Theory and Dendritic Cell Algorithm. IEEE Access. 2020. Vol. 8. P. 120532-120554.

40. Tan Z. et al. A survey of AI-based DDoS detection and mitigation strategies in SDN. IEEE Access. 2021. Vol. 9. P. 158219-158238.

41. Axelsson S. Intrusion Detection Systems: A Survey and Taxonomy. Department of Computer Engineering, Chalmers University of Technology. 2020. 142 p.

42. Wang B. et al. Artificial Immune System for Network Intrusion Detection: A Case Study on DDoS Attacks. International Journal of Information Security. 2022. Vol. 21. P. 455-470.

43. Abdulqader A. M. et al. Artificial immune system based intrusion detection: a comprehensive review. Journal of Network and Computer Applications. 2022. Vol. 199.

44. Chuvakin A., Schmidt K., Phillips C. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Syngress, 2021. 412 p.

45. Gartner Glossary: Security Orchestration, Automation and Response (SOAR). URL: https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-and-response-soar (дата звернення: 27.04.2026).

46. Bhatt S., Manadhata P. K., Zomaya A. The State of the Art in Intrusion Prevention and Detection. CRC Press, 2023. 320 p.

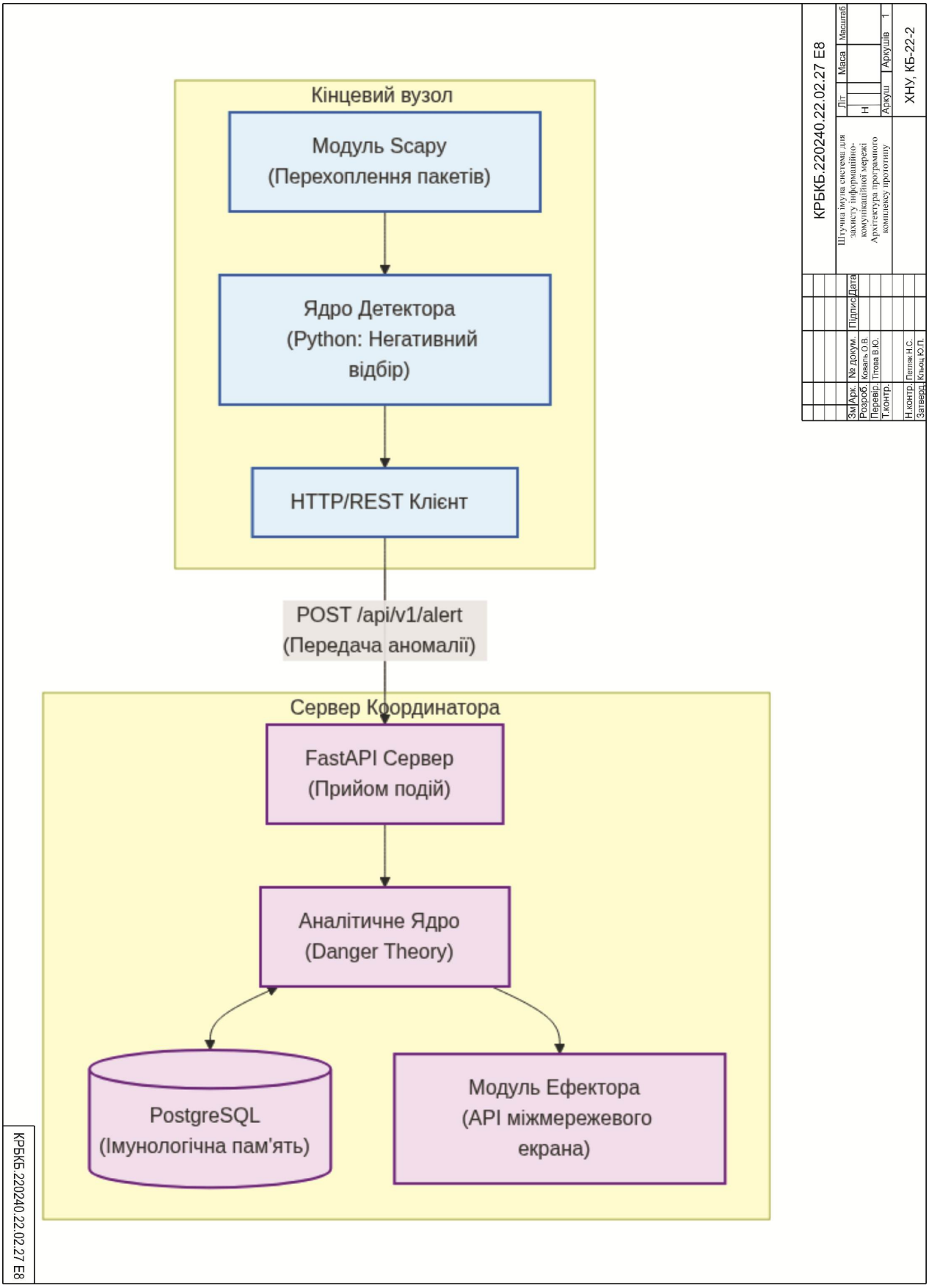
47. Elhag S. et al. Evaluating the performance of artificial immune system algorithms for network anomaly detection. IEEE Access. 2023. Vol. 11. P. 45678-

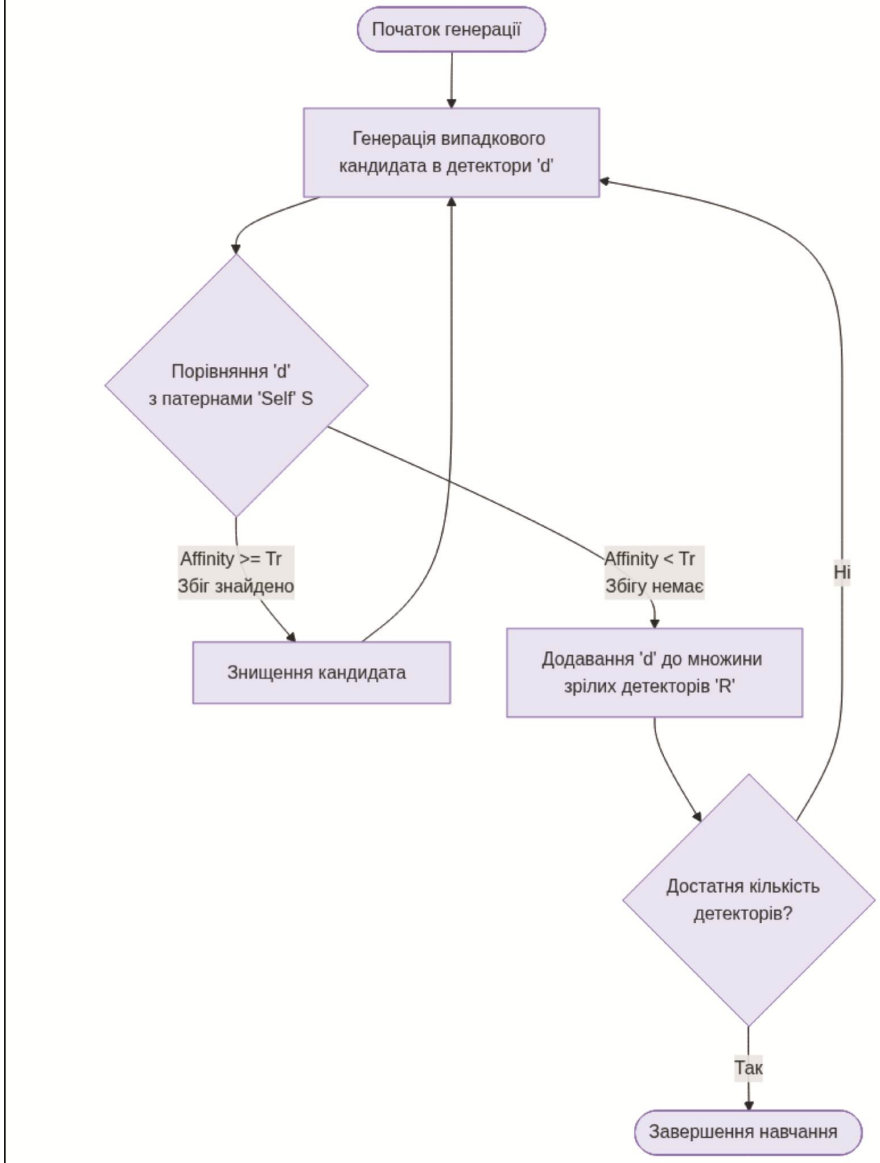
45690.

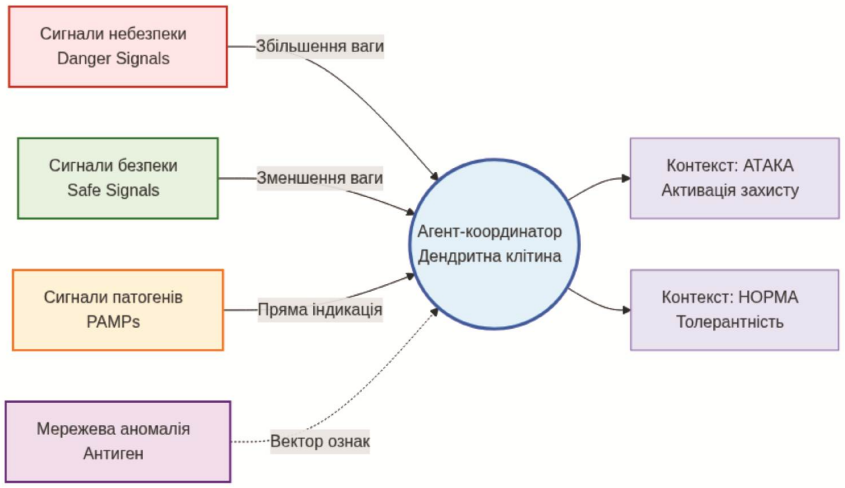
48. Zekri M. et al. DDoS attack detection using machine learning and artificial immune system techniques. Future Generation Computer Systems. 2021. Vol. 114. P. 138-151.

ДОДАТОК А

Копія графічної частини







					КРБКБ.220240.22.02.27 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Штучна імунна система для захисту інформаційно-комунікаційної мережі Алгоритмічна та логічна база	Літ	Маса / Масштаб
Розроб.		Коваль О.В.				Н	
Перевір.		Тітова В.Ю.				Аркуш	Аркушів 1
Т.контр.							
Н.контр.		Петляк Н.С.			ХНУ, КБ-22-2		
Затверд.		Кльоц Ю.П.					

КРБКБ.220240.22.02.27 Е8

Штучна імунна система для захисту інформаційно-комунікаційної мережі
Схема архітектури розподіленої мультиагентної імунної системи

Літ | Маса | Масштаб
Н | | |
Аркуш | Аркушів 1

ХНУ, КБ-22-2

Зм.	Арк.	№ докум.	Підпис	Дата
Розроб.		Ковель О.В.		
Перевір.		Тітова В.Ю.		
Т.контр.				
Н.контр.		Пятяк Н.С.		
Затверд.		Кльоц Ю.П.		

КРБКБ.220240.22.02.27 Е8