DOI 10.15276/imms.v15.no2.260
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 2, pp. 260-275

КІБЕРІМУННА МОДЕЛЬ ЗАХИСТУ ДАНИХ: МІЖДИСЦИПЛІНАРНИЙ АНАЛІЗ, ДІАГНОСТИКА ТА АРХІТЕКТУРА

О.А. Сиропятов, Л.М. Тимошенко

Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044,Україна
Emails: o.a.syropiatov@op.edu.ua, l.m.timoshenko@op.edu.ua

У статті проведено міждисциплінарний аналіз можливостей застосування принципів біологічної імунної системи та методів медичної діагностики для розробки ефективної архітектури кіберімунного захисту даних у телекомунікаційних системах. Здійснено огляд сучасних методологій, заснованих на принципах біологічного імунітету (Somayaji, Kim & Bentley, Dasgupta & Niño), які, попри здатність до виявлення аномалій, обмежені через відсутність повноцінних протоколів комплексного реагування на загрози. Запропоновано інноваційну адаптацію принципів первинної медичної діагностики — анамнезу, скринінгу, експрес-тестів і клінічних протоколів — для створення багаторівневої системи виявлення, класифікації та локалізації кіберзагроз із подальшою адаптивною відповіддю. Окреслено концептуальну архітектуру кіберімунної моделі, що включає механізми саморозпізнавання, раннього виявлення аномалій, формування кіберпам'яті, багаторівневу адаптивну відповідь та інформаційну зв'язність компонентів системи. Такий підхід дозволяє закласти фундамент для розвитку самонавчальних систем кіберзахисту з підвищеною стійкістю до складних і цілеспрямованих атак. У статті також детально розглянуто обмеження запропонованої моделі та визначено перспективні напрямки подальших досліджень, що включають моделювання, практичну верифікацію та інтеграцію з міжнародними стандартами кібербезпеки.

Ключові слова: кіберімунна система, імунна відповідь, діагностика, кібербезпека, адаптивний захист, архітектура системи, телекомунікаційні мережі, міждисциплінарний підхід.

Вступ. Історія людства демонструє, що прогрес часто є завдяки міждисциплінарному перенесенню знань та досвіду з однієї галузі в іншу. Приклади – від винайдення друкарського верстата, що трансформував освіту, до адаптації біологічних і нейрофізіологічних ідей в обчислювальні технології для розвитку штучного інтелекту [1]. У XXI столітті такі міждисциплінарні підходи, зокрема, застосування еволюційних алгоритмів чи моделей поширення інфекцій для аналізу соціальних процесів, стають ключовим фактором наукового прогресу, дозволяючи вирішувати складні завдання, такі як оптимізація логістики чи кібербезпека.

У сучасних умовах кіберзагрози стають дедалі складнішими, що вимагає нових, більш ефективних підходів до захисту інформаційних систем [2]. Використання принципів медичної діагностики та імунітету для побудови архітектур кіберзахисту є перспективним напрямом, що поєднує досягнення медицини, біології та інформаційних технологій. Такий міждисциплінарний підхід дозволяє створити адаптивні, самонавчальні системи, здатні ефективно протидіяти сучасним кіберзагрозам.

Метою роботи є обґрунтування концепції кіберімунної системи захисту даних у телекомунікаційних системах на основі міждисциплінарного підходу, що поєднує принципи біологічної імунної системи, медичної діагностики та сучасних архітектур кібербезпеки. Для досягнення мети необхідно вирішити наступні завдання.

1. Провести аналітичний огляд і порівняльний аналіз основних підходів до застосування принципів імунної системи у кіберзахисті, визначити їх переваги, обмеження та сучасний стан розвитку.

2. Проаналізувати ключові етапи та методи первинної діагностики в медицині, з'ясувати можливість їх адаптації для раннього виявлення та класифікації кіберзагроз.

3. Розробити концептуальну архітектуру кіберімунної моделі захисту даних у телекомунікаційних системах, визначити її рівні, компоненти, механізми взаємодії та відповідність сучасним стандартам.

4. Систематизувати результати дослідження, сформулювати висновки щодо ефективності міждисциплінарного підходу, окреслити обмеження та перспективи подальших досліджень.

Таким чином, міждисциплінарний підхід, що поєднує імунологічні та медичні принципи, створює нову парадигму для архітектури кіберзахисту.

Аналітичний огляд підходів до застосування імунної системи у кіберзахисті

Використання принципів біологічної імунної системи як концептуальної основи для архітектури кіберзахисту має багаторічну історію розвитку. Цей розділ містить критичний аналіз трьох фундаментальних підходів, які сформували теоретичний базис для штучних імунних систем (AIS) та рішень, заснованих на імунній системі (далі immune-inspired підходи), у сфері безпеки.

Підхід, запропонований Somayaji, Hofmeyr та Forrest, став одним із перших системних спроб формалізувати імунологічні принципи для кібербезпеки [3]. Автори виділили ключові властивості природної імунної системи, які можуть бути адаптовані для комп'ютерних систем, зокрема:

- децентралізація та автономність – відсутність єдиного центру управління, що забезпечує стійкість до атак на окремі компоненти;
- відсутність довіреного ядра – система функціонує без припущення про наявність абсолютно захищених елементів;
- динамічна адаптація – постійне оновлення та навчання детекторів для розпізнавання нових загроз;
- різноманіття механізмів – використання множини методів виявлення для підвищення загальної ефективності.

Somayaji та інші запропонували концептуальну модель, яка передбачає розподілену мережу детекторів, що функціонують автономно та адаптуються до змін середовища. Однак їх модель залишилася на рівні абстрактної архітектури без чіткої формалізації процесів виявлення та реагування. Вони не розробили конкретних алгоритмів для реалізації запропонованих принципів, що ускладнює практичне впровадження їх ідей. Критичні обмеження моделі:

- відсутність формалізованого протоколу реагування з чіткими етапами;
- не визначено механізми координації між компонентами системи;
- не розглянуто питання ресурсоємності та масштабованості;
- відсутня інтеграція з існуючими стандартами управління інцидентами.

Kim та Bentley зосередилися на прикладному аспекті імунологічних принципів, спеціально досліджуючи їх застосування для мережевих систем виявлення вторгнень (IDS) [4]. Їх ключові інновації:

- негативна селекція – формування детекторів, що не реагують на нормальну поведінку системи;
- клональна селекція – розмноження та мутація успішних детекторів для підвищення ефективності;
- самоорганізація агентів – розподілена система легковісних сенсорів без централізованого контролю;
- імунна пам'ять – збереження інформації про попередні атаки для прискорення майбутнього реагування.

Kim і Bentley розробили більш формалізовані алгоритми для генерації та навчання детекторів, що дозволило наблизити теоретичні концепції до практичної реалізації. Їх експерименти показали потенціал для виявлення нових типів аномалій без

попереднього навчання на відомих атаках. Проте їх підхід зосереджувався переважно на фазі виявлення, залишаючи без уваги комплексний процес реагування. Критичні обмеження підходу:

- спрощені моделі імунної відповіді без врахування багаторівневої взаємодії;
- відсутність механізмів контекстуального аналізу подій;
- недостатня увага до процесів ізоляції та нейтралізації загроз;
- проблеми з масштабуванням при збільшенні кількості детекторів.

Dasgupta і Niño систематизували напрям штучних імунних систем як окрему гілку обчислювального інтелекту, створивши теоретичний фундамент для формалізації імунологічних механізмів[5]. Їх ключові досягнення:

- математична формалізація – строгий опис імунних механізмів у вигляді алгоритмів;
- форма-простір – концепція для представлення антигенів і антитіл у багатовимірному просторі;
- еволюційні підходи – використання генетичних алгоритмів для оптимізації детекторів;
- універсальність застосування – розширення сфери використання від безпеки до оптимізації та класифікації.

Dasgupta і Niño створили найбільш формалізований і математично обґрунтований підхід до штучних імунних систем. Їхня робота дозволила перейти від концептуальних аналогій до конкретних обчислювальних моделей з чітко визначеними алгоритмами. Однак, зосереджуючись на алгоритмічній стороні, вони приділили менше уваги архітектурним аспектам та інтеграції з існуючими системами безпеки. Критичні обмеження підходу:

- фокус на окремих алгоритмічних задачах без цілісної архітектури;
- відсутність інтегрованого протоколу реагування з чіткими фазами;
- недостатня увага до практичних аспектів впровадження в реальні системи;
- обмежена підтримка контекстної інформації в системах управління інцидентами.

Між біологічною та кіберімунною системами існують фундаментальні відмінності, які ускладнюють пряму інтеграцію [6]. Структурні відмінності:

- контекст середовища: біологічна система функціонує в межах цілісного організму з чіткими межами, тоді як кіберпростір характеризується розмитими кордонами та динамічною структурою;
- еволюційна історія: природна імунна система розвивалася мільйони років, забезпечуючи оптимальний баланс між ефективністю та ресурсоємністю, тоді як кіберімунні системи проєктуються штучно.
- механізми адаптації: біологічна система має вбудовані механізми самонавчання та адаптації, які складно відтворити в цифровому середовищі.

Функціональні відмінності:

- багаторівневість захисту: природний імунітет включає вроджений та адаптивний компоненти з чітким розподілом функцій, тоді як кіберзахист часто реалізується як набір окремих інструментів;
- формування пам'яті: біологічна система ефективно формує довготривалу імунологічну пам'ять, що складно реалізувати в кіберсистемах без надмірного споживання ресурсів;
- протоколи реагування: медицина має формалізовані протоколи діагностики та лікування, тоді як кіберзахист часто залежить від ad-hoc рішень.

Сучасні виклики та нові парадигми

Впровадження immune-inspired підходів у реальні середовища має сучасні виклики. Технологічні виклики:

- постійно зростаюча швидкість і складність атак;
- необхідність контекстуального аналізу подій у реальному часі;

- інтеграція різнорідних джерел даних (SIEM, IDS/IPS, Threat Intelligence);
- балансування між глибиною аналізу та швидкістю реагування.

Нові парадигми безпеки:

- Zero Trust – модель, що базується на принципі "нікому не довіряй, завжди перевіряй" [7];
- XDR (Extended Detection and Response) – інтегровані платформи для наскрізного виявлення та реагування [8];
- SOAR (Security Orchestration, Automation and Response) – автоматизовані платформи з формалізованими сценаріями реагування[9];
- MITRE ATT&CK – для класифікації та аналізу тактик і технік атак[10].

Ці сучасні рішення, хоча й не використовують біологічні метафори напряму, реалізують принципи адаптивності, автоматизації та координації, необхідні для ефективного кіберзахисту. У таблиці 1 показано переваги та обмеження цих підходів.

Таблиця 1.

Ключові переваги та обмеження підходів

Підхід	Основні ідеї та переваги	Ключові обмеження
Somayaji et al.	Децентралізація, автономність, різноманіття; відсутність єдиної точки відмови; адаптивність до нових загроз	Абстрактність, відсутність формалізованого протоколу реагування; немає інтеграції зі стандартами
Kim & Bentley	Негативна селекція, клонування, самоорганізація; генерація детекторів для IDS; виявлення нових аномалій; простота імплементації	Спрощені моделі, відсутність багатошарової взаємодії; немає комплексного протоколу реагування
Dasgupta & Niño	Формалізація імунних механізмів у вигляді алгоритмів; еволюційні підходи; автоматизація виявлення загроз; адаптивність через навчання	Фокус на окремих задачах; відсутність інтегрованого протоколу реагування; обмежена робота з контекстом
Запропонована кіберімунна модель	Адаптація принципів імунної відповіді та медичної діагностики; багаторівнева архітектура; саморозпізнавання; раннє виявлення аномалій; адаптивна відповідь; формування кіберпам’яті; інформаційна зв’язність компонентів; основа для самонавчальних систем	Потребує подальшого моделювання, практичної верифікації та інтеграції з міжнародними стандартами

Стан застосування та перспективи

Аналіз сучасного стану застосування immune-inspired підходів виявляє суттєві прогалини. Поточні обмеження:

- більшість досліджень зосереджені на алгоритмах аномального виявлення (негативна селекція, клональна селекція, моделі небезпеки);
- AIS використовуються для оптимізації та класифікації, але не забезпечують комплексної взаємодії між компонентами захисту;
- галузеві стандарти (NIST SP 800-61, MITRE ATT&CK, SIEM, SOAR) не інтегрують імунологічні метафори як основу архітектури.

Перспективні напрями розвитку:

− розробка багаторівневих архітектур з чітким розподілом функцій між компонентами;

− формалізація протоколів реагування за аналогією з медичними протоколами лікування;

− інтеграція контекстуального аналізу для підвищення точності виявлення загроз;

− створення механізмів формування "кіберпам'яті" для ефективного навчання на інцидентах.

Проведений аналіз існуючих immune-inspired підходів показує, що, незважаючи на значний теоретичний фундамент, вони є фрагментарними і не забезпечують комплексного вирішення проблем кіберзахисту. Для подальшого розвитку необхідно перейти від окремих алгоритмів до інтегрованих систем управління інцидентами, які поєднують принципи імунної системи на всіх етапах – від виявлення до формування кіберпам'яті. Це вимагає розробки формалізованої архітектури, що адаптує біологічні механізми до специфіки кіберсередовища з урахуванням сучасних викликів і технологічних можливостей.

Аналогії у діях біологічної імунної системи та кіберзахистом

Методи первинної діагностики в медицині

Первинна діагностика є фундаментом сучасної медицини, оскільки дозволяє виявляти захворювання на ранніх стадіях, коли лікування найбільш ефективне, а ризики ускладнень – мінімальні [11]. Вона поєднує в собі як наукові методи, так і мистецтво інтерпретації симптомів у контексті індивідуальних особливостей пацієнта. Сучасна медицина постійно вдосконалює підходи до первинної діагностики, впроваджуючи нові технології та стандарти.

Основні етапи первинної діагностики.

1. Анамнез (збір інформації): передбачає детальний збір відомостей про самопочуття, скарги, історію хвороб, спадковість, спосіб життя пацієнта, формує основу для подальшого аналізу, допомагає окреслити зону пошуку проблеми та визначити пріоритети обстеження.

2. Фізикальне обстеження: безпосереднє вивчення стану організму за допомогою огляду, пальпації, аускультації, перкусії, вимірювання життєвих показників (температура, тиск, пульс). Мета – виявити об'єктивні ознаки порушень та уточнити локалізацію проблеми.

3. Скринінгові дослідження: масові скринінгові тести (наприклад, мамографія, тести на глюкозу, онкомаркери) для виявлення прихованих, безсимптомних або латентних захворювань, дозволяють своєчасно виявити ризики та розробити превентивні заходи.

4. Експрес-тести: у разі необхідності швидкої оцінки стану пацієнта використовуються експрес-методи (швидкі тести на інфекції, біохімічні аналізи). Вони забезпечують оперативне прийняття рішень у невідкладних ситуаціях.

5. Клінічні протоколи: діагностичний процес завершується застосуванням стандартизованих клінічних протоколів – алгоритмів, що регламентують дії лікаря у типових і складних випадках, що забезпечують єдність підходів та підвищують якість медичної допомоги[12].

Важливо, що ефективність первинної діагностики визначається не окремим методом, а їх поєднанням. Синергетичне використання анамнезу, фізикального обстеження, лабораторних тестів і протоколів дозволяє підвищити точність діагнозу та мінімізувати ризик помилок.

Сьогодні до традиційних методів активно додаються цифрові технології – електронні медичні картки, телемедицина, автоматизовані системи підтримки прийняття рішень. Це підвищує швидкість і якість діагностики, а також відкриває нові можливості для інтеграції медичних підходів у суміжні галузі [13].

Системний аналіз методів первинної діагностики в медицині дає змогу визначити

ключові механізми раннього виявлення загроз, що можуть бути адаптовані для підвищення ефективності кібербезпеки.

Імунна відповідь - біологічна основа для кіберімунної моделі.

Побудова кіберімунної моделі неможлива без глибокого розуміння ключових механізмів біологічної імунної системи, які демонструють структурну та функціональну схожість із процесами кіберзахисту [14]. Одним із універсальних та вивчених процесів в імунології є виявлення, обробка та нейтралізація антигену. Саме цей сценарій, що охоплює як вроджений, так і адаптивний імунітет, дозволяє простежити повний цикл захисту – від першого контакту з потенційною загрозою до формування довготривалої пам'яті. У біології антигеном вважають будь-яку молекулу, яка розпізнається імунною системою як "чужа" і здатна викликати імунну відповідь.

Антигени поділяють на екзогенні антигени: віруси, бактерії, токсини, пилок, чужорідні агенти, що потрапляють у організм із зовнішнього середовища; ендогенні антигени: білки змінених клітин, вірусні білки всередині заражених клітин, пухлинні маркери – власні компоненти організму, які зазнали змін або виявляються у незвичних контекстах. Ключовими властивостями антигену є імуногенність – здатність викликати імунну відповідь, та специфічність – забезпечує точність розпізнавання.

На рис.1 показано, як працює імунна система при зустрічі з антигеном.

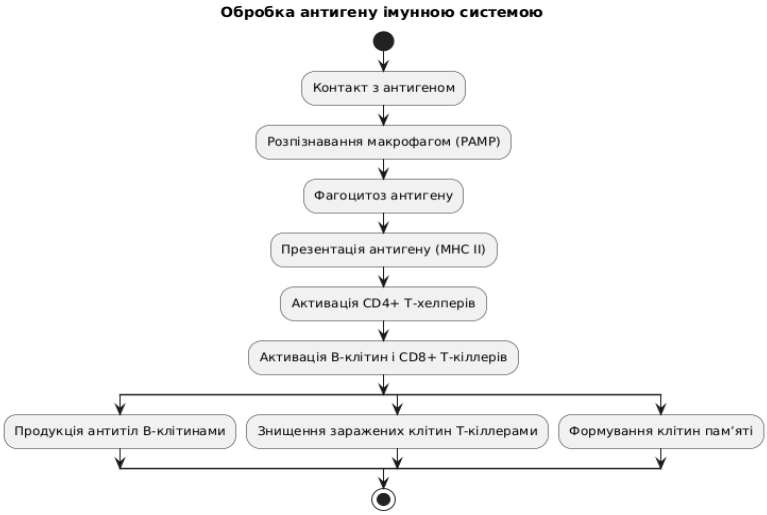

Рис.1. Обробка антигену імунною системою

Етапи імунної відповіді.

1. Розпізнавання антигену (вроджена система): клітини вродженого імунітету (макрофаги, дендритні клітини, нейтрофіли) виявляють характерні патерни (PAMPs), захоплюють антиген (фагоцитоз), переносять його до лімфатичних вузлів і запускають сигнальний каскад.

2. Презентація антигену: оброблений антиген презентується через молекули MHC. MHC класу II – CD4+ Т-хелперам; MHC класу I – CD8+ Т-кілерам.

3. Активація Т-клітин: CD4+ Т-хелпери активують В-клітини (продукують антитіла), макрофаги та інші Т-клітини.

CD8+ Т-кілери знищують клітини-мішені, ініціюючи апоптоз.

4. Вироблення антитіл і клітинна відповідь: антитіла нейтралізують антигени, блокують віруси, позначають їх для фагоцитозу, Т-клітини атакують заражені або атипові клітини.

5. Формування імунної пам'яті: створюються живучі клітини пам'яті (Т- і В-), які забезпечують швидку і потужну вторинну відповідь у разі повторного контакту з тією ж загрозою.

Ключові властивості імунної системи – адаптивность (здатність підлаштовуватися під нові загрози), скоординованость (узгоджена робота різних клітин і механізмів), еволюційноя ефективность (відбір найкращих механізмів захисту).

Здатність імунної системи до точного розпізнавання загроз, запуску цільової реакції та формування стійкої пам'яті є ключовою передумовою для побудови аналогічних захисних механізмів у цифровому середовищі.

Перенесення цих можливостей у цифрову сферу створює передумови для розробки кіберзахисних систем, які не лише реагують на відомі атаки, а й здатні ефективно протистояти новим загрозам завдяки механізмам адаптації та накопичення досвіду[15].

Методи первинного виявлення атак у кібербезпеці.

У сфері кібербезпеки, як і в медицині, ключовим завданням є своєчасне виявлення порушень цілісності складних систем. Хоча об'єкт захисту тут – не фізичне тіло, а інформаційне середовище, принципи виявлення загроз демонструють дивовижну подібність із медичними підходами до діагностики. Інформаційні системи так само піддаються зовнішньому впливу, «інфікуванню», зловживанню та зносу, що вимагає розробки ефективних методів раннього виявлення атак.

Нижче показано основні рівні первинного виявлення атак.

Перший рівень – системне логування («анамнез» інформаційної системи). Системне логування є базовим джерелом інформації про стан цифрового середовища. Воно включає хронологічний запис усіх подій: входів, виходів, помилок, змін конфігурацій. Цей «анамнез» дозволяє аналітикам відстежувати розвиток подій, виявляти аномалії та встановлювати причини інцидентів.

Другий рівень – моніторинг системних показників («життєві параметри»). На цьому рівні здійснюється безперервний моніторинг ключових метрик: навантаження процесора, обсяг переданих даних, кількість підключень, звернень до файлової системи тощо. Подібно до вимірювання температури чи тиску в медицині, ці показники допомагають оцінити, чи перебуває система в стані «інформаційного гомеостазу» або ж виникають відхилення, що сигналізують про потенційну загрозу.

Третій рівень – системи виявлення та запобігання атак (IDS/IPS) («експрес-тести»). Цей рівень передбачає використання IDS/IPS, які швидко реагують на відомі шаблони атак і сигнатури шкідливої поведінки. Хоча їхній діапазон обмежений, ці інструменти дозволяють оперативно виявляти та блокувати найпоширеніші загрози.

Четвертий рівень – сканування вразливостей («скринінгові дослідження»). Подібно до медичних скринінгів, у кібербезпеці застосовуються регулярні сканування вразливостей - спеціальні програми, що перевіряють IT-системи на наявність відомих слабких місць. Це дозволяє виявити потенційні точки входу для зловмисників ще до початку атаки.

П'ятий рівень – автоматизовані сценарії реагування (SIEM/Playbooks) («клінічні протоколи»). Завершальний рівень – автоматизовані сценарії реагування, реалізовані у SIEM-системах. Playbooks визначають послідовність дій у разі певних комбінацій подій: від надсилання сповіщень до автоматичного блокування джерел загроз. Це цифровий аналог клінічних протоколів, що забезпечує стандартизовану та швидку реакцію на інциденти.

Жоден із перерахованих рівнів не є самодостатнім. Ефективність забезпечує лише їх комплексне застосування, коли автоматизовані засоби, логічний аналіз, сканування та поведінковий моніторинг працюють у взаємозв'язку. Такий синергетичний підхід формує надійний фундамент для розвитку адаптивної системи кіберзахисту, здатної до самонавчання й превентивного реагування.

Комплексне застосування різних методів виявлення атак у кібербезпеці забезпечує своєчасне реагування та підвищує стійкість інформаційних систем до сучасних загроз. Взаємодія логування, моніторингу, сканування вразливостей та автоматизованих сценаріїв реагування створює основу для формування адаптивної системи кіберзахисту,

здатної до безперервного удосконалення [16]

Кіберобробка аномалій: структурна аналогія з імунітетом

Аномалія як "антиген" цифрового середовища

У цифровому середовищі аналогом біологічного антигену виступає аномалія – подія або поведінка, що не відповідає стандартному (еталонному) профілю функціонування системи. Виявлення таких аномалій є першим кроком до захисту інформаційної інфраструктури від потенційних загроз.

Типові приклади аномалій – логін у нетиповий час або з незвичної IP-адреси; раптове зростання трафіку без пояснення; запуск невідомого процесу; несанкціонована зміна конфігурації.

На рис.2 показано, як працює кіберзахист при виявленні та реагуванні на атаку.

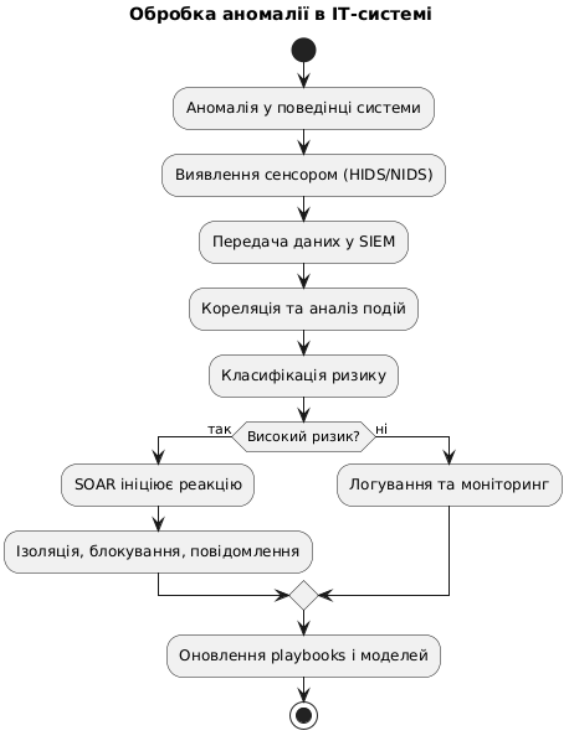

Рис.2. Виявлення та реагування кіберзахисту на зовнішню атаку

Етапи виявлення та реагування, кібернетична імунна відповідь:

- спостереження і моніторинг: агенти моніторингу (HIDS/NIDS, логери, сенсори) безперервно сканують середовище в реальному часі, збираючи дані з мережі (пакети, порти), хостів (процеси, логи), а також із зовнішніх джерел (SOC feed);
- виявлення і кореляція: аналітичні платформи (SIEM, XDR) корелюють події, зіставляють їх із шаблонами та використовують машинне навчання для виявлення нетипових дій, що можуть свідчити про атаку;
- оцінка та класифікація: визначається характер події (шкідлива/нешкідлива), рівень ризику та відповідність сценаріям реагування; у складних випадках подія передається на ручну оцінку SOC-аналітику.
- реакція: активується SOAR або вручну ініціюються дії: блокування IP-адреси, ізоляція пристрою, оновлення фаєрволу, запуск скриптів реагування;
- формування кіберімунної пам’яті: оновлюються правила, сигнатури, ML-моделі, сценарії playbooks, система накопичує досвід для швидшого і точнішого реагування на аналогічні загрози в майбутньому.

Нижче у таблиці 2 наведено порівняння ключових компонентів біологічної імунної системи та відповідних механізмів кібербезпеки, що ілюструє аналогії в процесах виявлення та реагування на загрози.

Таблиця 2.

Аналогія між біологічною імунною системою та кіберзахистом

Імунологія	Кібербезпека	Функція
Антиген	Аномалія	Запуск реакції
Макрофаг	Сенсор/агент моніторингу	Первинне виявлення
Презентація (MHC)	Кореляція в SIEM	Передача у систему аналізу
Т-клітини	SOAR/аналітик	Класифікація та відповідь
Пам’ять	Playbooks, сигнатури	Повторне реагування

Аналіз механізмів виявлення та нейтралізації загроз у біологічних і цифрових системах підтвердив глибоку структурну і функціональну схожість між імунною відповіддю організму та алгоритмами кіберзахисту. Як у медицині, так і в кібербезпеці, ефективний захист базується на поетапному виявленні порушень, їх точному розпізнаванні, адекватній реакції та збереженні досвіду для подальшого самонавчання.

Ці паралелі створюють концептуальне підґрунтя для розробки кіберімунної архітектури, яка здатна самостійно виявляти аномалії; класифікувати джерела загроз; обирати рівень і форму реагування; накопичувати та використовувати кіберпам’ять.

Таким чином, узагальнення виявлених відповідностей дозволяє перейти від описових аналогій до побудови цілісної ідеології кіберімунної системи, що є основою для подальшої практичної реалізації цієї моделі у цифровому середовищі [17].

Архітектура кіберімунної моделі захисту.

Попередній аналіз виявив суттєві концептуальні паралелі між імунною відповіддю біологічних систем та методами кіберзахисту. Ці паралелі слугують підґрунтям для формалізації цілісної кіберімунної моделі – інноваційної архітектури, що інтегрує біологічні принципи в інформаційну безпеку [18].

Перейдемо до розробки концептуальної архітектури кіберімунної моделі, здатної інтегруватися в існуючі системи кіберзахисту з метою підвищення їх ефективності, адаптивності та стійкості до нових типів загроз.

Архітектура кіберімунної моделі базується на основних принципах, адаптованих із біологічної імунної системи, що забезпечують її ефективність, гнучкість і стійкість.

1. Саморозпізнавання і самовизначення (Self-awareness): система повинна чітко визначати власний «нормальний стан» для своєчасного виявлення відхилень і потенційних загроз.
2. Раннє виявлення аномалій (Early Detection): постійний моніторинг, евристичний аналіз та використання методів машинного навчання і штучного інтелекту для швидкого виявлення нетипових подій.
3. Адаптивність (Adaptability): самонавчання та динамічне оновлення алгоритмів реагування відповідно до появи нових загроз і змін у середовищі.
4. Мінімізація хибнопозитивних результатів: валідація дій на основі контекстного аналізу та крос-даних для зниження кількості помилкових спрацювань і підвищення точності.
5. Багаторівнева відповідь (Layered Response): диференційовані реакції залежно від рівня ризику, типу загрози та контексту подій.
6. Формування кіберпам’яті (Cyber Memory): накопичення досвіду, збереження ефективних шаблонів реагування та їх використання для підвищення ефективності майбутніх дій.
7. Інформаційна зв’язність (Information Integration): забезпечення обміну та узгодженого аналізу даних між усіма компонентами системи для цілісного розуміння ситуації.
8. Стійкість до внутрішніх збоїв (Fault Tolerance): здатність системи зберігати функціональність навіть при частковій відмові окремих компонентів.

Ці принципи забезпечать надійність, гнучкісь та масштабованість системи кіберзахисту та відповідають сучасним підходам до побудови адаптивних систем виявлення та реагування.

Для практичної реалізації кіберімунної моделі важливо чітко продемонструвати, як саме принципи втілюються у цифровому середовищі. Таблиця 3 систематизує відповідність між біологічними принципами імунітету та їх реалізацією в архітектурі кіберзахисту, ілюструючи алгоритм роботи моделі на кожному етапі. Тут кожен принцип імунітету має свою функціональну реалізацію в архітектурі кіберімунної моделі. Запропонований алгоритм передбачає послідовне проходження етапів – від самовизначення до формування пам'яті та адаптації, що дозволяє системі не лише реагувати на відомі загрози, а й навчатися на нових інцидентах [19].

Таблиця 3.

Алгоритм імунної відповіді в кіберпросторі: реалізація принципів

Принцип біологічного імунітету	**Реалізація в кіберпросторі**	**Опис/Функція**
Саморозпізнавання і самовизначення	Визначення еталонного стану системи	Формування профілю «нормальної» поведінки, базових політик безпеки, білих списків тощо
Раннє виявлення аномалій	Постійний моніторинг, евристика, ML/AI	Виявлення відхилень у реальному часі, запуск аналізу при появі підозрілих подій
Адаптивність	Динамічне оновлення правил, самонавчання	Впровадження алгоритмів, що змінюють поведінку системи відповідно до нових загроз
Мінімізація хибнопозитивних результатів	Контекстний аналіз, крос-верифікація	Перевірка підозрілих подій за декількома джерелами, зниження кількості помилкових спрацювань
Багаторівнева відповідь	Диференційовані сценарії реагування	Реакція залежно від рівня ризику: від сповіщення до ізоляції чи блокування
Формування кіберпам'яті	Оновлення бази сигнатур, шаблонів, playbooks	Збереження даних про атаки, автоматичне оновлення механізмів реагування
Інформаційна зв'язність	Інтеграція даних між компонентами	Обмін інформацією між сенсорами, аналітичними модулями, системами реагування
Стійкість до внутрішніх збоїв	Резервування, децентралізація	Забезпечення роботи системи навіть за відмови окремих вузлів або каналів

Такий підхід базується на багаторівневій організації, адаптивності та здатності до накопичення кіберпам'яті. Комплексна реалізація підходу забезпечує гнучкість, стійкість і самонавчання системи у динамічному кіберсередовищі .

Завдяки структурі кіберімунна система здатна не лише імітувати біологічні механізми захисту, а й підвищувати ефективність реагування на нові, ще невідомі типи атак, що створює потужне підґрунтя для подальшої деталізації структурних компонентів моделі, які розглядаються далі.

Структура кіберімунної моделі базується на принципах багаторівневої організації та розподілу функцій, що детально описані у фундаментальних роботах з штучних імунних систем (AIS) [5]. Для реалізації цих принципів кіберімунна система має містити такі основні компоненти з відповідними біологічними аналогіями:

− сенсори моніторингу (аналог макрофагів) які постійно сканують цифрове середовище, виявляють аномалії та передають інформацію для подальшого аналізу;

− аналітичний центр (аналог лімфатичних вузлів) здійснює кореляцію подій, класифікацію загроз і приймає рішення щодо необхідних заходів реагування;

− виконавчі модулі реагування (аналог Т-клітин та антитіл) виконують блокування, ізоляцію, відновлення або інші дії залежно від типу та рівня загрози;

− блок кіберпам'яті (аналог клітин пам'яті) зберігає шаблони атак, сценарії реагування та моделі машинного навчання для швидкого і ефективного повторного реагування;

− інтеграційний модуль забезпечує обмін даними між компонентами системи, а також інтеграцію з іншими системами кіберзахисту (SIEM, SOAR, XDR тощо).

Ця багаторівнева модульна архітектура дозволяє забезпечити цілісність, гнучкість та стійкість системи кіберзахисту, а також адаптивність до нових типів загроз у динамічному інформаційному середовищі [20].

Архітектура кіберімунної моделі розробляється з урахуванням вимог міжнародних стандартів інформаційної безпеки: ISO/IEC 27001, NIST SP 800-61 та ISO 15189. Це забезпечує відповідність системи найкращим практикам управління безпекою, моніторингу, виявлення інцидентів та реагування на них, сприяє уніфікації процедур кіберзахисту, полегшує сертифікацію системи та підвищує довіру користувачів і партнерів.

Для коректної адаптації біологічних механізмів у цифровому середовищі сформовано глосарій відповідностей між ключовими елементами імунної системи та їх кібернетичними аналогами. Таблиця 4 демонструє відповідність між біологічними механізмами та кіберімунними компонентами, що дозволяє будувати ефективні системи виявлення та реагування на аномалії.

Таблиця 4.

Відповідність між біологічними механізмами та кіберімунними компонентами

Біологічний аналог	**Кіберімунний компонент**	**Функціональна роль**	**Приклад систем**	**Коротке пояснення**
Макрофаги	Агенти моніторингу	Первинне виявлення загроз	HIDS, SNMP-агенти	Виявляють аномалії на рівні вузлів і мережі
Дендритні клітини	Комутатори, логери	Збір та передача подій	NetFlow-колектори, лог-сервери	Агрегують і пересилають дані для подальшого аналізу
Т-хелпери (CD4+)	AI/SOC класифікатор	Вибір типу реагування	SIEM з ML, SOC-аналітик	Класифікують загрози, визначають сценарії реагування
Т-кілери (CD8+)	Реактивні механізми	Ізоляція, блокування, знищення	SOAR, автоматичне блокування	Здійснюють активну відповідь: блокують

Біологічний аналог	Кіберімунний компонент	Функціональна роль	Приклад систем	Коротке пояснення
				трафік, ізолюють вузли
В-клітини	Генератор сигнатур/правил	Створення шаблонів для виявлення	IDS/IPS, генерація YARA-правил	Формують нові правила для розпізнавання атак
Клітини пам'яті	Playbooks, архів інцидентів	Повторне реагування	Бази інцидентів SOC, бібліотеки playbooks	Зберігають досвід для швидкої реакції на повторні загрози
Кістковий мозок	База знань, система оновлень	Підживлення моделі новими даними	Централізовані репозиторії IOC	Постачають нові знання про загрози та способи реагування
Кровоносна система	Канали телеметрії	Обмін інформацією між модулями	Syslog, MQTT, REST API	Забезпечують циркуляцію даних у системі
Нейронна система	Центр управління	Координація, прийняття рішень	NOC/SOC, оркестратори мережі	Координують процеси та приймають стратегічні рішення

Таблиця ілюструє структурну та функціональну відповідність між ключовими елементами біологічної імунної системи та сучасними компонентами кіберзахисту у телекомунікаційних мережах. Використання реальних прикладів (HIDS, SOAR, SIEM, playbooks, репозиторії IOC, NOC/SOC) демонструє, як міждисциплінарна аналогія переходить у практичну площину. Ця відповідність є основою для побудови ефективної, самонавчальної та адаптивної кіберімунної системи, яка не лише імітує біологічні механізми, а й підсилює можливості сучасних телекомунікаційних платформ у протидії складним загрозам.

Візуалізація архітектури кіберімунної моделі.

Для кращого розуміння логіки взаємодії структурних компонентів кіберімунної моделі доцільно представити її архітектуру у вигляді структурної схеми (рис. 3). На схемі відображено основні функціональні блоки системи, їхні біологічні аналоги та інформаційні зв'язки, що забезпечують цілісність і адаптивність моделі. Схема ілюструє взаємодію основних компонентів: сенсорів моніторингу, аналітичного центру, виконавчих модулів реагування, системи кіберпам'яті, бази знань, каналів телеметрії та центру управління. Кожен елемент виконує функцію, аналогічну до відповідної структури імунної системи організму, а їхня взаємодія забезпечує самонавчання, адаптацію та стійкість до динамічних кіберзагроз.

Представлена архітектура кіберімунної моделі захисту даних загалом відповідає ключовим біологічним принципам імунної системи, адаптованим для цифрового середовища.

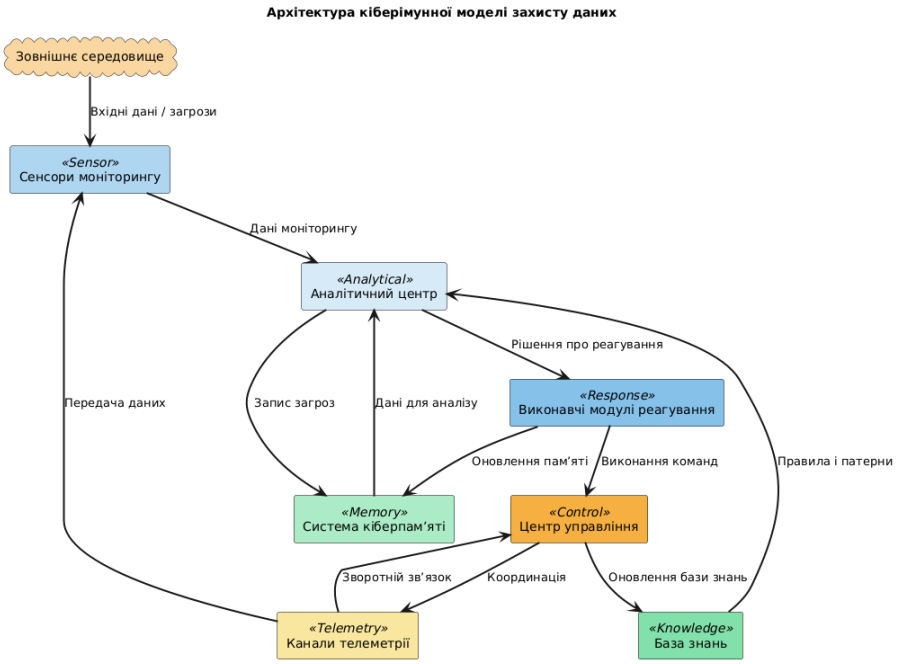

Рис. 3. Архітектура кіберімунної моделі захисту даних у комунікаційних системах

Розглянемо відповідність по кожному з основних принципів.

1. Саморозпізнавання і самовизначення (Self-awareness): архітектура включає сенсори моніторингу, які збирають дані про «нормальний стан» системи, а аналітичний центр формує профіль нормальної поведінки. База знань і кіберпам'ять підтримують збереження еталонних станів і політик.
2. Раннє виявлення аномалій (Early Detection) : постійний моніторинг сенсорами та аналітичний центр із застосуванням евристик, машинного навчання та штучного інтелекту забезпечують швидке виявлення відхилень і підозрілих подій.
3. Адаптивність (Adaptability): кіберпам'ять і база знань оновлюються на основі нових інцидентів і шаблонів реагування, а динамічне оновлення правил у аналітичному центрі й центрі управління забезпечує самонавчання і адаптацію системи.
4. Мінімізація хибнопозитивних результатів: архітектура передбачає контекстний аналіз і крос-верифікацію даних між компонентами (аналітичний центр, база знань, кіберпам'ять), що дозволяє знижувати кількість помилкових спрацювань.
5. Багаторівнева відповідь (Layered Response): диференційні реакції реалізуються через послідовність компонентів: аналітика формує рішення, центр управління координує дії, виконавчі модулі реагування реалізують різні сценарії залежно від рівня загрози.
6. Формування кіберпам'яті (Cyber Memory): система кіберпам'яті зберігає інформацію про атаки та ефективні шаблони реагування, що використовується для покращення майбутніх реакцій.
7. Інформаційна зв'язність (Information Integration): архітектура забезпечує обмін даними між усіма компонентами через канали телеметрії та внутрішні зв'язки, що гарантує цілісний аналіз і координацію дій.
8. Стійкість до внутрішніх збоїв (Fault Tolerance): для реалізації цього принципу доцільно впровадити такі технічні механізми:

- кластеризація ключових компонентів (аналітичний центр, система кіберпам'яті, база знань) із розподіленим навантаженням, що запобігає втраті працездатності при виході з ладу окремих вузлів.
- реплікація даних у реальному часі з георепліkацією або через системи високої доступності (HA), що забезпечує збереження критичних даних навіть при втраті

доступу до окремих дата-центрів.

− Failover-сценарії та автоматичне перемикання на резервні ресурси з мінімальним часом відновлення (RTO) і допустимим вікном втрати даних (RPO).

− самодіагностика та автоматичне відновлення: регулярна перевірка стану компонентів, виявлення деградації продуктивності, ініціювання перезапуску або перенесення процесів на резервні вузли.

− логічна децентралізація функцій для уникнення єдиної точки відмови (SPOF), з дублюванням логіки прийняття рішень у кількох сегментах системи (наприклад часткове дублювання аналітичного центру в регіональних вузлах).

Архітектура відповідає основним принципам кіберімунної моделі, демонструючи послідовний алгоритм імунної відповіді: від самовизначення нормального стану, раннього виявлення аномалій, через адаптивний аналіз і багаторівневу реакцію, до формування кіберпам'яті та забезпечення інформаційної зв'язності. Вона відображає цифрову реалізацію біологічних механізмів імунітету, що забезпечує гнучкість, самонавчання і ефективний захист у динамічному кіберсередовищі.

Висновки. У роботі проведено комплексний міждисциплінарний аналіз теоретичних, методологічних та архітектурних основ побудови кіберімунної моделі захисту даних.

1. Теоретико-методологічний внесок: проведено системний огляд ключових immune-inspired підходів до кіберзахисту. Виявлено, що більшість існуючих рішень фрагментарно застосовують біологічні метафори, зосереджуючись переважно на виявленні аномалій, не охоплюючи повний цикл реагування та навчання.

2. Міждисциплінарний підхід: продемонстровано ефективність адаптації принципів первинної медичної діагностики для виявлення та класифікації кіберзагроз, що підвищує точність і швидкість реагування.

3. Архітектурні рішення: запропоновано модульну архітектуру кіберімунної моделі, що базується на ключових біологічних принципах імунної системи, адаптованих для цифрового середовища. Архітектура забезпечує децентралізацію, автономність, адаптивність, а також високу стійкість завдяки механізмам кластеризації, реплікації даних і автоматичного відновлення. Це сприяє масштабованості системи та підвищує її ефективність у протидії складним багатовекторним атакам.

4. Відповідність міжнародним стандартам: розробка архітектури здійснюється з урахуванням вимог міжнародних стандартів інформаційної безпеки, зокрема NIST SP 800-61 та ISO/IEC 27001, які визначають найкращі практики управління інцидентами, моніторингу, реагування та підтримки безперервності бізнес-процесів. Це забезпечує уніфікацію процедур кіберзахисту, полегшує сертифікацію та впровадження системи.

5. Практичне значення: обґрунтовано доцільність впровадження кіберімунних підходів до підвищення стійкості інформаційних систем до багатовекторних загроз.

6. Обмеження та перспективи: визначено виклики, пов'язані зі складністю формалізації біологічних процесів, необхідністю адаптації до динамічних умов і ризиками хибних спрацювань. Подальші дослідження планується зосередити на моделюванні, симуляціях і практичній верифікації [21].

7. Наукова та практична новизна: результати створюють основу для розвитку нового класу адаптивних, самонавчальних систем кіберзахисту, здатних автономно виявляти, ідентифікувати та нейтралізувати загрози у реальному часі.

8. Перспективи подальших досліджень: це перша частина комплексного дослідження, присвяченого розробці кіберімунної моделі захисту даних. У ній зосереджено увагу на теоретичних і методологічних засадах, а також на архітектурних рішеннях. Далі планується представити результати валідації сформульованих теоретичних положень, а також запропонувати практичні напрямки вдосконалення методів виявлення загроз із застосуванням розробленої кіберімунної моделі. Це дозволить оцінити ефективність підходу в реальних умовах та сприятиме подальшому розвитку адаптивних і самонавчальних систем захисту.

Список літератури

1. Smith J. *History of Interdisciplinary Science*. Берлін: Springer, 2018. 320 с.
2. European Union Agency for Cybersecurity (ENISA). *Threat Landscape 2024*. Athens: ENISA, 2024. 150 с.
3. Somayaji A., Hofmeyr S.A., Forrest S. *Principles of a Computer Immune System*. Proceedings of the National Information Systems Security Conference (NISSC). Baltimore, USA, 1997. С. 335–345.
4. Kim J., Bentley P.J. *Towards an Artificial Immune System for Network Intrusion Detection: Anomaly Detection Using Dendritic Cells*. Proceedings of the Genetic and Evolutionary Computation Conference (GECCO). San Francisco, USA, 2001. С. 12–19.
5. Dasgupta D., Niño L.F. *Artificial Immune Systems and Their Applications*. New York: Springer, 2009. 264 с.
6. Stepney S., et al. *Concepts of Biological Immunity and Computer Security*. Theoretical Computer Science. Amsterdam: Elsevier, 2005.– Т. 337, № 1–3. С. 131–156.
7. National Institute of Standards and Technology (NIST). *Special Publication 800-207. Zero Trust Architecture*. Gaithersburg, USA: NIST, 2020. 59 с.
8. Gartner. *Innovation Insight for Extended Detection and Response (XDR)*. Stamford: Gartner Research, 2022. 35 с.
9. IBM Security. *SOAR: Security Orchestration, Automation and Response*. Armonk, USA: IBM White Paper, 2023. 28 с.
10. MITRE. *ATT&CK Framework*. Режим доступу: https://attack.mitre.org/ (дата звернення: 03.06.2025).
11. World Health Organization (WHO). *Guidelines on Diagnostic Procedures*. Geneva: WHO Press, 2023. 88 с.
12. Centers for Disease Control and Prevention (CDC). *Guidelines for Diagnostic Tests*. Atlanta, USA: CDC, 2022. 76 с.
13. ISO 15189:2022. *Medical laboratories – Requirements for quality and competence*. Geneva: ISO, 2022. 46 с.
14. Timmis J., Neal M., Hunt J. *An Artificial Immune System for Data Analysis*. Biosystems. – Amsterdam: Elsevier, 2000. Т. 55, № 1–3. С. 143–150.
15. Johnson M. *Interdisciplinary Approaches in IT*. IT Review. London: IT Press, 2022. Т. 12, № 4. С. 45–58.
16. ISO/IEC 27001:2022. *Information Security Management Systems – Requirements*. Geneva: ISO, 2022. 35 с.
17. Hart E., Timmis J., Hone A. *Artificial Immune Systems*. In: Gendreau M., Potvin J.-Y. (eds.) *Handbook of Metaheuristics*. – 3rd ed. New York: Springer, 2019. С. 421–448.
18. Hofmeyr S.A., Forrest S. *Architecture for an Artificial Immune System*. Evolutionary Computation. Cambridge, USA: MIT Press, 2000. – Т. 8, № 4. С. 443–473.
19. ISO/IEC 27035-1:2016. *Information Security Incident Management Part 1: Principles of Incident Management*. Geneva: ISO/IEC, 2016. 28 с.
20. ETSI GS NFV 002 V1.2.1. *Network Functions Virtualisation (NFV); Architectural Framework*. Sophia Antipolis: ETSI, 2014. 72 с.
21. Berner E.S., La Lande T.J. *Clinical Decision Support Systems: Successes and Failures*. Yearbook of Medical Informatics. Schattauer, 2016. Т. 25, № 1. С. 103–110.

A CYBER IMMUNE MODEL OF DATA PROTECTION: INTERDISCIPLINARY ANALYSIS, DIAGNOSTICS, AND ARCHITECTURE

O.A. Syropiatov, L.M. Tymoshenko

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: o.a.syropiatov@op.edu.ua, l.m.timoshenko@op.edu.ua

The article presents an interdisciplinary analysis of the possibilities of applying the principles of the biological immune system and medical diagnostic methods to develop an effective architecture for cyberimmune data protection in telecommunications systems. A review of modern methodologies based on the principles of biological immunity (Somayaji, Kim & Bentley, Dasgupta & Niño) is carried out, which, despite the ability to detect anomalies, are limited due to the lack of full-fledged protocols for a comprehensive response to threats. The article proposes an innovative adaptation of the principles of primary medical diagnosis - history, screening, rapid tests and clinical protocols - to create a multi-level system for detecting, classifying and localizing cyber threats with a subsequent adaptive response. The author outlines the conceptual architecture of the cyber immune model, which includes mechanisms for self-recognition, early detection of anomalies, formation of cyber memory, multi-level adaptive response, and information connectivity of the system components. This approach allows laying the foundation for the development of self-learning cyber defense systems with increased resistance to complex and targeted attacks. The article also discusses in detail the limitations of the proposed model and identifies promising areas for further research, including modeling, practical verification, and integration with international cybersecurity standards.

Keywords: cyber-immune system, immune response, diagnostics, cybersecurity, adaptive defense, system architecture, telecommunication networks, interdisciplinary approach.