DOI 10.15276/imms.v15.no3.439
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 3, pp. 439-453

ІМІТАЦІЙНА МОДЕЛЬ КІБЕРІМУННОЇ СИСТЕМИ: ПЕРЕНЕСЕННЯ МЕДИЧНИХ ПРИНЦИПІВ У СУЧАСНИЙ КІБЕРЗАХИСТ

О.А. Сиропятов, Л.М. Тимошенко

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

Представлено міждисциплінарний підхід до підвищення стійкості інформаційних систем шляхом перенесення принципів біологічної імунної системи та медичних протоколів у галузь кібербезпеки. Проведено порівняльний аналіз фаз розвитку біологічних інфекцій (COVID-19, гепатит А) та сучасних кібератак (PlugX Worm, ILOVEYOU), що дозволило виявити структурні паралелі й визначити універсальні стратегії реагування. Особливу увагу приділено можливості інтеграції медичних принципів у архітектуру сучасних IDS/IPS на прикладі системи SURICATA. Описано ключові обмеження аналогій, пов'язані з відмінностями у механізмах передачі, архітектурі середовища та поведінці загроз. Запропоновано концептуальну імітаційну модель кіберімунної системи, яка базується на багаторівневій структурі, самонавчанні, автоматичній корекції політик і формуванні кіберпам'яті. Модель охоплює компоненти, що відповідають за моніторинг, швидке реагування, аналітику, накопичення знань та еволюцію захисних механізмів. Проведено порівняння з класичними SIEM-системами та показано, що імунна модель забезпечує вищу швидкість реагування, кращу адаптивність і можливість накопичення колективного знання про загрози. Практична значимість дослідження полягає у можливості використання імітаційного моделювання для валідації нових підходів до кіберзахисту, оптимізації процедур реагування та профілактики. Стаття закладає підґрунтя для подальших досліджень у сфері інтеграції медичних принципів у кібербезпеку, пропонуючи концепцію децентралізованих, самонавчальних і стійких систем захисту нового покоління.

Ключові слова: кіберімунна система, медичні протоколи, багаторівнева діагностика, SURICATA, імітаційна модель кіберімунної відповіді, кіберпам'ять, адаптивний захист.

Вступ. Сучасні інформаційні системи стикаються зі зростаючою складністю та динамічністю кіберзагроз, що вимагає пошуку нових, міждисциплінарних стратегій захисту [1]. Останні роки характеризуються не лише із зростанням кількості атак, а й появою складних цільових загроз, що використовують штучний інтелект, соціальну інженерію та автоматизовані інструменти для обходу класичних систем захисту. У такій ситуації актуальним стає пошук нових архітектур кіберзахисту, здатних до самонавчання, адаптації та формування «кіберпам'яті».

Кіберімунна система — це міждисциплінарна концепція, яка імітує принципи біологічної імунної системи та медичної діагностики для побудови стійких і адаптивних систем захисту даних. [2] Основними характеристиками такої системи є багаторівнева відповідь, механізми саморозпізнавання, формування кіберпам'яті, раннє виявлення загроз і можливість самонавчання на основі попереднього досвіду. Подібний підхід активно досліджується у світовій практиці, зокрема в контексті використання AI/ML для підвищення ефективності IDS/IPS-систем[3].

У статті [3] обґрунтовано концептуальну архітектуру кіберімунної системи та визначено основні принципи її функціонування. Однак для переходу від теорії до практики необхідна верифікація запропонованих аналогій на основі реальних сценаріїв атак і медичних протоколів. Зокрема, актуальним є питання: наскільки принципи медичних стратегій реагування на інфекційні захворювання можуть бути адаптовані для

побудови алгоритмів кіберзахисту. Відповідь дозволяє не лише теоретично обґрунтувати міждисциплінарну модель, а й розробити практичний інструментарій для вдосконалення сучасних систем безпеки.

Мета роботи: провести верифікацію концепції кіберімунної системи шляхом порівняльного аналізу протоколів лікування біологічних інфекцій та сценаріїв кібератак; дослідити можливість перенесення медичних принципів у архітектуру сучасних IDS/IPS на прикладі SURICATA; запропонувати прототип імітаційної моделі кіберімунної відповіді, яка окреслює потенційні напрямки R&D для практичного впровадження.

Завдання: здійснити порівняльний аналіз етапів розвитку та протоколів реагування на прикладі пар аналогій (COVID-19 ↔ PlugX Worm, гепатит А ↔ ILOVEYOU); дослідити можливість інтеграції медичних принципів у сучасні системи кіберзахисту; запропонувати концепцію імітаційної моделі кіберімунної системи та визначити її обмеження.

Порівняльний аналіз етапів розвитку та протоколів реагування на прикладі пар аналогій (COVID-19 ↔ PlugX Worm, гепатит А ↔ ILOVEYOU). Для аналізу аналогій між біологічними інфекціями та сучасними кібератаками доцільно брати приклади, які чітко ілюструють ключові етапи розвитку загрози та реакції на неї.

COVID-19 – масштабна інфекція з вираженою фазовістю, а PlugX Worm – сучасний цифровий черв'як, що активно використовується для атак на різні системи.

Збудник COVID-19 - коронавірус SARS-CoV-2. Передача: повітряно-крапельний, контактний шляхи. Фази: експозиція, інкубація (2–14 днів), початкові симптоми, загострення, ускладнення, відновлення. Особливості: тривалий безсимптомний період, складність раннього виявлення, потреба в масовому тестуванні й ізоляції.

PlugX Worm - комп'ютерний черв'як із функціями бекдору. Шляхи проникнення: використання вразливостей ОС, фішингові листи, заражені USB-носії, RDP. Фази: початкове проникнення, прихована присутність, активація, масове поширення, завантаження додаткових модулів, пошкодження інфраструктури. Особливості: маскування, автоматичне поширення, крадіжка даних, запуск додаткових атак

Обидва приклади мають чітко визначені етапи розвитку, що дозволяє провести структурний аналіз аналогій [3]. І COVID-19, і PlugX Worm вимагають системного підходу до виявлення, ізоляції, реагування та відновлення. На рис 1. показано етапи розвитку COVID-19 та PlugX Worm. Зліва наведені основні фази розвитку COVID-19, справа – відповідні етапи атаки PlugX Worm. Така паралельна візуалізація демонструє структурну подібність між біологічною інфекцією та сучасною цифровою атакою[4].

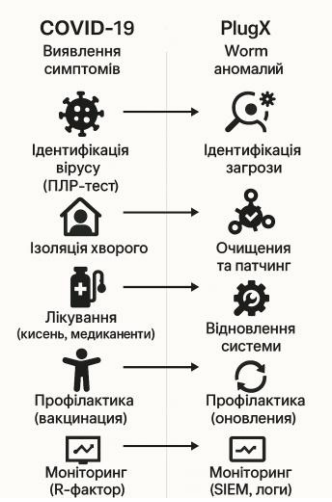

Рис.1. Етапи розвитку COVID-19 та PlugX Worm

Вона дозволяє швидко співставити критичні точки для раннього виявлення, ізоляції, реагування та відновлення в обох сферах. Схема підкреслює, що адаптація медичних

принципів може бути корисною для розробки ефективних стратегій кіберзахисту, але потребує врахування специфіки цифрового середовища[5].

Аналіз цієї пари дає змогу застосувати перевірені медичні підходи для розробки стратегій кіберзахисту, враховуючи сучасні технології та загрози.

Обидва процеси – біологічна інфекція та цифрова атака – мають чітко виражену фазову структуру. Це дозволяє не лише порівнювати окремі етапи розвитку загрози, а й знаходити спільні принципи реагування, які можуть бути корисними для побудови ефективних стратегій захисту в обох сферах. Таблиця 1 ілюструє ці паралелі.

Таблиця 1.

Етапи розвитку: біологічна та цифрова паралель

Фаза COVID-19	Етап атаки PlugX Worm	Опис аналогії
Експозиція	Первинне проникнення	Контакт із вірусом (людина) чи експлуатація вразливості/USB (PlugX)
Інкубаційний період	Прихована присутність	Безсимптомний розвиток інфекції або приховане перебування PlugX у системі до активації
Початкові симптоми	Активація шкідливого коду	Поява перших ознак хвороби чи запуск основних функцій PlugX
Загострення	Масове розповсюдження/завантаження модулів	Прогресування захворювання чи активне поширення PlugX мережею, завантаження додаткового ПЗ
Ускладнення	Пошкодження інфраструктури	Критичний стан організму або руйнування/шифрування цифрової інфраструктури, викрадення даних
Відновлення	Нейтралізація/відновлення	Реабілітація пацієнта або очищення й відновлення системи після атаки

Ця таблиця ілюструє, як структурна подібність фаз розвитку біологічної інфекції та цифрової атаки дозволяє адаптувати перевірені підходи з медицини для розробки ефективних стратегій кіберзахисту.

Ключові обмеження аналогії. Відмінність механізмів передачі: COVID-19 поширюється через фізичний контакт, PlugX – через мережу, USB-носії, фішингові листи [5]. Архітектурна різниця: імунна система діє в межах організму, PlugX часто атакує розподілені IT-інфраструктури. Пам’ять та еволюція: біологічна імунна пам’ять формується природним шляхом або вакцинацією; у PlugX кіберсистеми потребують спеціальних механізмів накопичення знань [6]. Метрики ефективності: медичні показники (летальність, реабілітація) не мають прямих відповідників у кібербезпеці (час виявлення, false positives/negatives) [7].

Визначення цих обме.жень дозволяє уникати некоректних узагальнень і формувати рекомендації, які враховують специфіку цифрового середовища.

Для деталізації особливостей сучасних атак PlugX наведено окрему таблицю 2, що підкреслює ключові характеристики кожного етапу.

Таблиця 2.

Порівняльна таблиця: особливості PlugX (2024)

Фаза біологічної інфекції	Етап PlugX-атаки	Особливості PlugX (2024)
Експозиція	Зараження через USB/мережу	Використання фішингу, USB-носіїв, RDP
Інкубація	Приховане перебування	Складні механізми маскування
Симптоми	Активація, крадіжка даних	Витік даних, запуск бекдорів
Загострення	Масове поширення, завантаження модулів	Завантаження додаткового ПЗ, lateral movement
Відновлення	Очищення системи, оновлення захисту	Відкат систем, оновлення політик

Ця таблиця дозволяє побачити не лише загальні структурні паралелі, а й специфіку сучасних цифрових атак, що важливо для практичного застосування аналогій.

Деталізація допомагає зрозуміти, які підходи з медицини можуть бути корисними для кіберзахисту, а які потребують адаптації чи переосмислення. Водночас очевидно, що не всі принципи можна перенести без змін: відмінності у механізмах передачі, архітектурі середовища та поведінці загроз вимагають обережного й критичного підходу до використання аналогій. Пошук релевантних аналогій і критичний аналіз їхніх обмежень дозволяють не лише підвищити ефективність цифрових систем, а й забезпечити їхню стійкість до нових, раніше невідомих загроз.

Розглянемо аналогію гепатиту А ↔ сучасні атаки соціальної інженерії. Для аналізу аналогій між біологічними інфекціями з тривалим прихованим перебігом і сучасними кібератаками доцільно розглядати приклади, що демонструють залежність від соціальних контактів, пасивну фазу розвитку та відкладений масовий ефект. Гепатит А – класичний приклад інфекції з довгою інкубацією та соціальною передачею. У цифровому середовищі аналогічними є атаки, що поширюються через фішинг, вкладення у листах або соціальні мережі, зокрема історичний випадок ILOVEYOU та сучасні багатоступеневі фішингові кампанії.

Коротко про гепатит А**.** Передача: через інфіковану воду, їжу, побутові контакти. Фази: експозиція, інкубація (15–50 днів), продромальна, іктерична, відновлення. Особливості: тривалий безсимптомний період, приховане поширення, залежність від соціальних контактів.

Коротко про атаки типу ILOVEYOU і сучасний фішинг. Канал: електронна пошта, месенджери, соціальні мережі. Фази: експозиція (отримання листа/вкладення), інкубація (очікування дії користувача), активація, масове поширення, побічні ефекти, відновлення. Особливості: прихована фаза, залежність від людського фактору, лавиноподібне поширення через контакти.

Обидва процеси – біологічна інфекція та цифрова атака – мають фазову структуру з прихованим початком і залежністю від поведінки носіїв/користувачів. Це дозволяє порівнювати ключові етапи розвитку загрози та знаходити спільні принципи реагування. На рис 2. показано етапи розвитку гепатиту А і ILOVEYOU.

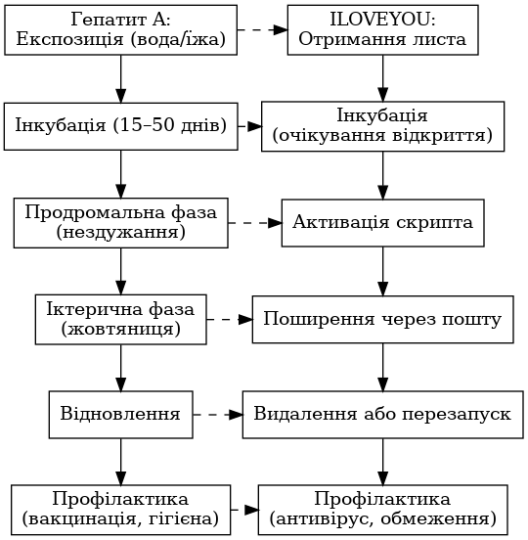

Рис. 2. Зіставлення фаз розвитку гепатиту А та етапів атаки вірусом ILOVEYOU

Далі наведена таблиця 3, яка ілюструє ці паралелі та структурну подібність фаз розвитку біологічної інфекції та цифрової атаки соціальної інженерії. Такий підхід дозволяє адаптувати медичні стратегії для підвищення ефективності кіберзахисту.

Таблиця 3.

Етапи розвитку: біологічна та цифрова паралель між гепатитом А та вірусом ILOVEYOU

Фаза гепатиту А	Етап атаки ILOVEYOU / сучасний фішинг	Опис аналогії
Експозиція	Отримання листа/вкладення	Контакт із джерелом: заражена їжа/вода або фішинговий лист
Інкубаційний період	Прихована присутність	Безсимптомне носійство або очікування дії користувача
Продромальна фаза	Перші ознаки (неспецифічні)	Незначні симптоми або підозріла активність, ще не розпізнана
Іктерична фаза	Активація, масове поширення	Явні симптоми або запуск шкідливого коду, автоматичне розсилання
Відновлення	Очищення системи, профілактика	Реабілітація організму або видалення шкідливого ПЗ, навчання

Ключові обмеження аналогії. Відмінність механізмів передачі: гепатит А – через фізичний контакт, їжу, воду; фішинг – через електронні канали. Інкубаційний період у біології має біохімічну природу, у кіберпросторі – це соціальний фактор (користувач сам запускає шкідливий код). Медична профілактика передбачає вакцинацію, у кіберзахисті – це навчання користувачів та автоматизовані засоби ізоляції. Відновлення після хвороби формує біологічну пам’ять, а у кіберзахисті потрібні спеціальні механізми накопичення знань (playbooks, сигнатури).

Визначення цих обмежень дозволяє уникати некоректних узагальнень і формувати рекомендації, які враховують специфіку цифрового середовища. У таблиці 4 показано особливості сучасних фішингових атак.

Таблиця 4.

Порівняльна таблиця: особливості сучасних фішингових атак

Фаза біологічної інфекції	Етап сучасної фішингової атаки	Особливості (2024–2025)
Експозиція	Отримання email/вкладення/посилання	Використання PDF, ZIP, LNK, SVG, QR-кодів
Інкубація	Приховане перебування	Очікування дії користувача, маскування
Симптоми	Активація, крадіжка даних	Витік даних, запуск бекдорів, credential theft
Загострення	Масове поширення, автоматизація	Автоматичне розсилання, використання AI
Відновлення	Очищення системи, оновлення захисту	Відкат систем, навчання користувачів

Така деталізація допомагає зрозуміти, які саме підходи з медицини можуть бути корисними для кіберзахисту, а які потребують адаптації чи переосмислення. Водночас очевидно, що не всі принципи можна перенести без змін: відмінності у механізмах передачі, архітектурі середовища та поведінці загроз вимагають обережного й критичного підходу до використання аналогій.

Тому наступним кроком є формулювання практичних рекомендацій для кіберзахисту – з урахуванням зазначених обмежень і специфіки сучасних IT-систем.

Рекомендації для кіберзахисту на основі аналізу аналогій COVID/PlugX та Гепатит А/ILOVEYOU. Аналіз аналогій між біологічними вірусними інфекціями (COVID-19, гепатит А) та цифровими атаками (PlugX, ILOVEYOU) дає змогу сформулювати універсальні підходи до підвищення стійкості кіберінфраструктури. Врахування медичних принципів дозволяє пропонувати більш гнучкі, багаторівневі й адаптивні стратегії захисту.

Багаторівнева діагностика та тестування. Доцільно впроваджувати кілька типів детекторів і аналізаторів для різних рівнів інфраструктури (мережа, кінцеві точки, пошта), що сприятиме своєчасному виявленню загроз навіть у розподіленому

середовищі. Варто застосовувати різні методи перевірки вкладень, посилань і файлів для підвищення ймовірності виявлення нових або складних атак.

Контекстна діагностика**.** Рекомендується аналізувати не лише сам факт інциденту, а й джерело, спосіб проникнення, особливості поведінки шкідливого коду чи листа. Використання даних про попередні атаки може підвищити точність реагування та дозволити формувати профілі ризику.

Карантин та ізоляція. Може бути доцільне автоматичне ізолювання підозрілих об'єктів (вкладень, вузлів, листів) до завершення аналізу. Сегментація мережі та ізоляція уражених зон здатна обмежити поширення атаки навіть у разі невідомого джерела загрози.

Формування кіберпам'яті. Рекомендується створювати та оновлювати бази знань про інциденти, сценарії реагування, ознаки компрометації. Використання накопиченого досвіду сприятиме пришвидшенню реагування на повторні чи схожі атаки.

Автоматизація реагування. Варто розглядати впровадження AI/ML для автоматичного виявлення аномалій, фішингових листів і шкідливих вкладень. Політики Zero Trust і концепція Digital Immune System можуть підвищити стійкість інфраструктури навіть у разі проникнення загрози.

Моніторинг ефективності та адаптація. Регулярний аналіз результатів реагування та коригування політик захисту з урахуванням нових типів атак і змін у структурі інфраструктури може підвищити ефективність системи. Автоматичний фідбек-цикл сприятиме постійному вдосконаленню захисних механізмів.

Навчання користувачів. Доцільно проводити регулярні тренінги з розпізнавання фішингу, шкідливих вкладень, соціальної інженерії. Моделювання атак може підвищити обізнаність персоналу й знизити ризики успішних атак соціальної інженерії.

Отже, багаторівневий підхід дозволяє виявляти як типові, так і нові, раніше невідомі загрози, мінімізуючи кількість хибних спрацювань. Контекстна діагностика підвищує точність реагування, дозволяє враховувати індивідуальні особливості інфраструктури та користувачів. Кіберпам'ять і автоматизація забезпечують швидке реагування та адаптацію системи до нових сценаріїв атак. Навчання користувачів підвищує загальний рівень кібергігієни та зменшує ймовірність успішних атак соціальної інженерії. Узагальнення досвіду боротьби з біологічними вірусами (COVID-19, гепатит А) та аналіз сучасних цифрових атак (PlugX, ILOVEYOU) підтверджують ефективність багаторівневого, адаптивного та самонавчального підходу до кіберзахисту. Інтеграція медичних принципів у архітектуру захисних систем може сприяти підвищенню стійкості інфраструктури до складних, цільових і нових загроз.

Дослідження можливості перенесення медичних принципів у архітектуру сучасних IDS/IPS на прикладі SURICATA. Покажемо практичну трансформацію ідей з медичної практики в інструменти кіберзахисту шляхом порівняння функціоналу системи SURICATA (IPS/IDS) із протоколами медичної імунної відповіді [1].

Водночас важливо визнати обмеження такого порівняння. Природа загроз у кіберпросторі та біологічних системах суттєво відрізняється: SURICATA працює з цифровими атаками (шкідливий трафік, експлойти), тоді як імунна система організму протидіє біологічним патогенам [4]. Метрики ефективності також різні: у медицині — це чутливість, специфічність, імунна пам'ять; у кіберзахисті — швидкість виявлення, FP/FN, масштабованість. Крім того, біологічна імунна система функціонує як єдиний цілісний механізм, тоді як IT-інфраструктури часто розподілені та гетерогенні.

Це порівняння не претендує на пряме зіставлення метрик ефективності. Його головна цінність – виявлення архітектурних і концептуальних подібностей та відмінностей і пошук напрямів вдосконалення IPS/IDS через запозичення медичних принципів: контекстуальності, динамічного моніторингу, самонавчання та профілактики [10].

Аналіз призначення SURICATA та її сучасні характеристики. SURICATA– це популярний інструмент з відкритим кодом, який поєднує сигнатурний і поведінковий підходи та інтегрується із SIEM-системами [8]. Проте його архітектура класично реактивна, орієнтована на фіксацію відомих загроз [9]. Це аналіз пакетів (Deep Packet Inspection) та підтримка масштабованих розгортань [12]. SURICATA запобігає атакам - сканування портів і мереж, DDoS-атаки, Brute-force та pass-the-hash атаки, експлуатація вразливостей протоколів, виявлення шкідливого трафіку (malware, botnet C2), аномалії в мережевій поведінці. На рис. 3 схематично зображено алгоритм роботи системи виявлення та запобігання вторгненням SURICATA. Діаграма демонструє основні етапи аналізу мережевого трафіку: від початкового захоплення та парсингу пакетів до прийняття рішень щодо блокування або подальшого моніторингу. Кожна гілка відображає логіку обробки подій – сигнатурний та аномальний аналіз, глибоку перевірку, генерацію алертів і блокування трафіку.

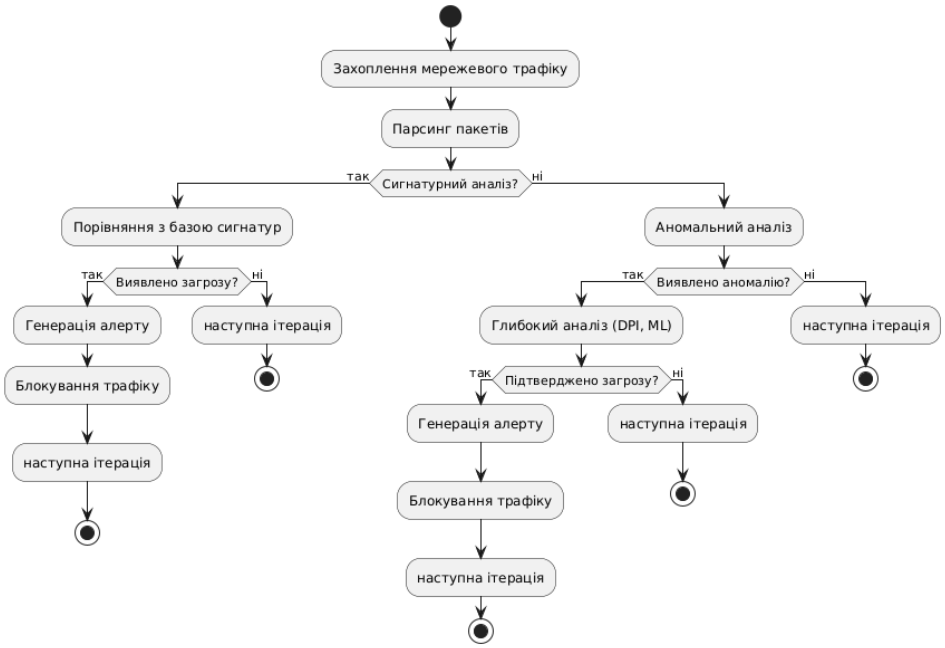

Рис.3. Алгоритм роботи системи SURICATA

Схема ілюструє те, що SURICATA працює у безперервному циклі: після завершення кожної ітерації система повертається до обробки нового трафіку. Відображено два основних підходи до аналізу – сигнатурний (порівняння з базою відомих загроз) та аномальний (виявлення нетипових патернів). Для підозрілих ситуацій передбачено глибокий аналіз із використанням DPI та машинного навчання – це підвищує точність і дозволяє реагувати на нові типи атак. Блок «наступна ітерація» підкреслює циклічність і постійну готовність системи до обробки нових загроз. Ключові алгоритми включають pattern matching, flow analysis, використання flowbits, підтримку динамічних правил та можливість інтеграції з ML-модулями.

Однак, навіть найсучасніші технології кіберзахисту мають обмеження, пов’язані з адаптивністю, контекстною обізнаністю та здатністю до самонавчання. Ці властивості є ключовими для природної імунної системи людини, яка протягом мільйонів років еволюціонувала для ефективного виявлення та нейтралізації вірусних загроз[1,4].

Для подальшого вдосконалення архітектури IDS/IPS доцільно звернутися до досвіду медицини, зокрема, до принципів і алгоритмів роботи імунної системи. Медичні протоколи виявлення вірусних атак побудовані на багаторівневій діагностиці, адаптивності, формуванні пам’яті та динамічній корекції реакцій організму. Їх аналіз дозволяє знайти нові підходи до підвищення ефективності кіберзахисту.

Далі розглянемо, як саме організовані алгоритми та принципи медичних протоколів виявлення вірусних атак, і які з них можуть бути імплементовані в сучасні системи захисту інформації.

Медичні протоколи виявлення вірусних атак: алгоритми та принципи

Медична імунна система людини є унікальним прикладом ефективної багаторівневої системи захисту, яка здатна виявляти, ідентифікувати й нейтралізувати широкий спектр вірусних загроз. Її принципи та алгоритми можуть слугувати джерелом ідей для вдосконалення сучасних систем кіберзахисту.

Основні алгоритми та принципи роботи імунної системи

1. Багаторівнева діагностика: імунна система застосовує поетапний підхід до виявлення патогенів. На першому рівні здійснюється швидкий скринінг (наприклад, неспецифічна імунна відповідь – фагоцитоз, інтерферони), а у разі підозри на інфекцію запускаються глибші лабораторні дослідження (специфічна імунна відповідь - активація Т- і В-лімфоцитів, вироблення антитіл). Такий підхід дозволяє ефективно фільтрувати більшість нешкідливих впливів і зосереджувати ресурси на справжніх загрозах.
2. Імунологічні методи розпізнавання антигенів: ключовим механізмом є розпізнавання чужорідних молекул (антигенів) за допомогою спеціалізованих рецепторів. Це аналог сигнатурного аналізу в IDS/IPS, коли система порівнює зразки з базою відомих загроз1,2,4]. Вироблення антитіл та активація клітинного імунітету забезпечують швидке реагування на знайомі патогени.
3. Адаптивність через формування імунної пам’яті: після контакту з вірусом імунна система формує клітини пам’яті, які дозволяють у майбутньому розпізнавати та нейтралізувати цей патоген значно швидше й ефективніше. Це забезпечує здатність системи навчатися на попередньому досвіді та підвищувати свою ефективність з часом.
4. Алгоритми визначення «своє-чуже»: імунна система використовує складні механізми для розмежування власних і чужорідних клітин та молекул. Алгоритми негативної селекції та клонального відбору дозволяють уникати автоімунних реакцій і зосереджуватися на реальних загрозах. Ці процеси нагадують машинне навчання: система формує набір правил для розпізнавання «чужого» на основі досвіду та селекції.
5. Динамічний моніторинг стану організму: постійний контроль за змінами у внутрішньому середовищі (температура, рівень запальних маркерів, поява нових антигенів) дозволяє імунній системі оперативно реагувати на нові загрози. Це аналог постійного моніторингу мережевого трафіку й поведінки у кіберзахисті.
6. Зворотній зв’язок для корекції імунної відповіді: імунна система здатна коригувати свою активність на основі результатів боротьби з патогеном: посилювати чи послаблювати реакцію, запобігати надмірному ушкодженню власних тканин. Такий механізм зворотного зв’язку є важливим для підтримки балансу між ефективністю захисту та мінімізацією побічних ефектів.

Для кращого розуміння принципів функціонування імунної системи людини схема відображає основні етапи виявлення та нейтралізації вірусних атак організмом. Вона ілюструє, як захист організму організований на різних рівнях – від швидкої неспецифічної відповіді до формування імунної пам’яті для забезпечення стійкості до повторних інфекцій.

Схема (рис.4) демонструє поетапний характер імунної відповіді від моменту проникнення вірусу до активації неспецифічного та специфічного захисту. Важливим етапом є виявлення антигену, після чого запускається адаптивна імунна відповідь із залученням Т- і В-лімфоцитів. Якщо виробляються антитіла, відбувається нейтралізація вірусу та формування імунної пам’яті, що забезпечує швидку реакцію при повторному зараженні. Динамічний моніторинг і зворотний зв’язок дозволяють коригувати інтенсивність імунної відповіді, підтримуючи баланс між ефективністю захисту та мінімізацією шкоди для організму. Такий багаторівневий і адаптивний підхід до захисту є орієнтиром для вдосконалення сучасних систем кібербезпеки.

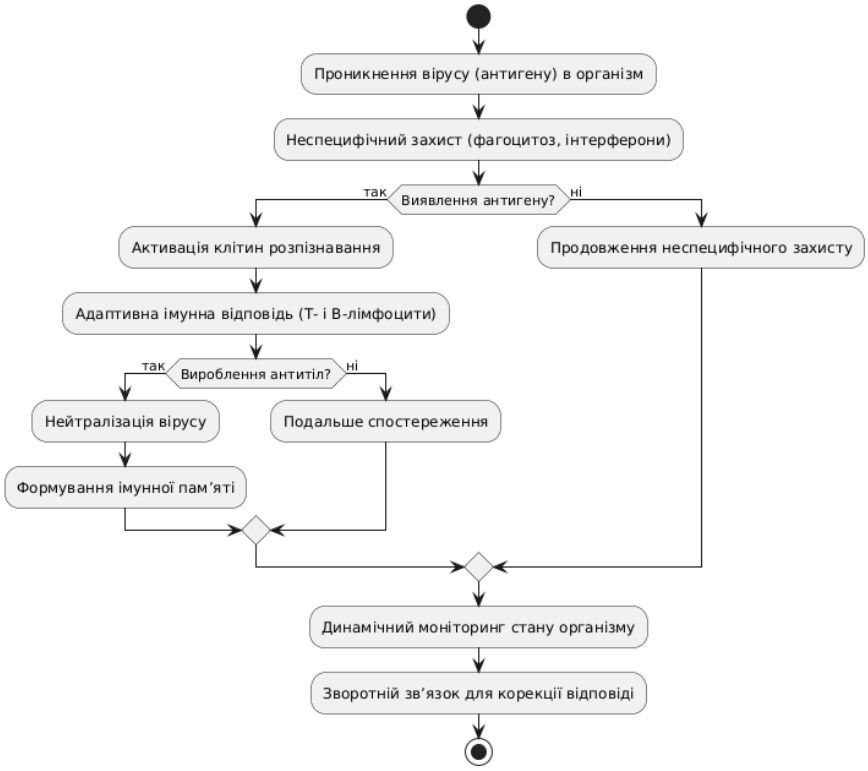

Рис.4. Алгоритм функціонування імунної системи людини

Порівняння алгоритмів SURICATA, медичних протоколів та концепції. Таке порівняння дозволяє не лише виявити спільні риси й ключові відмінності, а й визначити потенційні напрями розвитку сучасних систем кіберзахисту [10]. Концепція - практичний орієнтир для розвитку системи, відображає, як сучасна IDS/IPS може трансформуватися з реактивної у проактивну, самонавчальну й адаптивну платформу, якщо інтегрувати принципи, перевірені мільйонами років еволюції біологічних систем. Порівняння трьох моделей дозволяє чітко побачити, які саме функції вже реалізовані, які відсутні, а які можна впровадити для підвищення ефективності кіберзахисту.

SURICATA (імунна модель) виступає як міст між класичним підходом і майбутніми інтелектуальними системами, придатними до самонавчання, гнучкої адаптації, автоматичного оновлення політик і глибокого контекстного аналізу [13,14].

Отже, медична імунна система забезпечує гнучкий, багаторівневий і контекстно-чутливий захист для ефективного реагування на нові загрози; SURICATA (стандарт) зосереджена на швидкому сигнатурному виявленні, має обмежену адаптивність і контекстну обізнаність; SURICATA (імунна модель), як концепція, об'єднує кращі риси обох систем: багаторівневий аналіз, самонавчання, автоматичну корекцію політик, профілювання та повноцінну роботу з контекстом.

Розширене порівняння демонструє (таблиця 5), що інтеграція імунних принципів у архітектуру SURICATA відкриває шлях до створення дійсно адаптивної, стійкої та самонавчальної системи кіберзахисту нового покоління. Такий підхід дозволяє не лише підвищити точність виявлення складних атак, а й забезпечити гнучкість і швидкість реагування на нові, невідомі загрози.

Як концепція імунної моделі може покращити адаптивність SURICATA. Імунна модель в контексті кіберзахисту – це концепція, що запозичує принципи роботи біологічної імунної системи для побудови гнучких, самонавчальних і адаптивних систем виявлення та реагування на загрози. Її впровадження у SURICATA дає перейти від статичного, реактивного до динамічного, проактивного, контекстно-чутливого кіберзахисту.

Таблиця 5.

Порівняльна таблиця алгоритмів

Критерій	Медична імунна система	SURICATA (стандарт)	SURICATA (імунна модель, концепт)
Природа загроз	Біологічні патогени	Цифрові атаки	Цифрові атаки
Анамнез	Збір анамнезу	Відсутній	Контекстуальний профіль, історія подій
Скринінг	Багаторівневий	Сигнатурний	Сигнатурний + поведінковий аналіз
Підтвердження	Лабораторна діагностика	Частково (правила)	Sandbox, ML-агенти, глибокий аналіз
Імунна оцінка	Оцінка стану організму	Відсутня	Аналіз навантаження, вразливостей
Моніторинг ефективності	Динамічна оцінка лікування	Відсутній	Автоматичний фідбек-цикл
Профілактика	Вакцинація, освіта	Ручне оновлення правил	Автоматичне самооновлення, навчання
Самонавчання	Формування імунної пам’яті	Обмежено (ML-модулі)	Постійне оновлення на основі досвіду
Адаптивність	Висока	Обмежена	Гнучка зміна політик, самонавчання
Динамічна корекція	Автоматична	Переважно ручна	Автоматичне коригування політик
Контекстна обізнаність	Врахування анамнезу, стану	Частково (інтеграція з SIEM)	Повний контекст, профілювання, історія

Ключові механізми покращення адаптивності SURICATA [1,4,10].

1.Контекстна обізнаність та “анамнез”: збір та аналіз історичних даних про мережеву активність, профілювання користувачів і пристроїв. Врахування попередніх інцидентів для формування “імунологічної пам’яті” системи.

2. Багаторівнева діагностика: поєднання швидкого сигнатурного скринінгу з глибинним поведінковим та ML-аналізом підозрілих подій. Автоматичне визначення ступеня загрози та вибір оптимальної стратегії реагування.

3. Адаптивне оновлення правил: використання механізмів зворотного зв’язку: автоматичне коригування політик та правил на основі аналізу результатів реагування. Самостійне формування нових “антитіл” (правил) для невідомих атак за аналогією з клональним відбором у біології.

4. Динамічний моніторинг та оцінка стану: постійний контроль за змінами у мережевому середовищі, виявлення аномалій у реальному часі. Оцінка “здоров’я” інфраструктури та автоматичне пристосування до нових умов.

5. Формування імунної пам’яті: збереження інформації про попередні атаки та ефективні способи реагування. Використання цього досвіду для швидшого й точнішого виявлення повторних або схожих загроз.

Переваги для SURICATA – зменшення кількості хибних спрацювань завдяки врахуванню контексту та історії подій; підвищення стійкості до нових типів атак через самонавчання та автоматичне оновлення правил; гнучкість реагування: зміна стратегії захисту залежно від типу, сили та контексту загрози; підвищення ефективності профілактики – автоматичне впровадження нових політик і навчання користувачів після інцидентів.

Інтеграція імунної моделі в архітектуру SURICATA дозволяє створити дійсно адаптивну систему кіберзахисту, що не лише ефективно реагує на відомі загрози, а й здатна навчатися на нових інцидентах, автоматично вдосконалювати свої механізми захисту та забезпечувати стійкість до складних і цільових атак.

Імітаційна модель кіберімунної відповіді. Попередній аналіз аналогій та порівняння принципів медичної імунної системи з архітектурою SURICATA дозволили окреслити ключові напрями вдосконалення сучасних засобів кіберзахисту. Наступним логічним

кроком є спроба об'єднати ці принципи у єдину концептуальну модель, яка імітує поведінку біологічної імунної системи. Такий підхід не лише демонструє потенціал міждисциплінарного перенесення знань, але й пропонує дорожню карту для подальших досліджень та розробки практичних рішень.

Обґрунтуємо доцільність залучення моделі як дослідницького інструменту [15]. Така модель виконує одразу кілька важливих завдань у контексті розвитку систем кіберзахисту.

По-перше, вона дозволяє синтезувати результати порівняльного аналізу між медичними протоколами та сучасними IPS/IDS (як-от SURICATA), переносячи виявлені принципи (багаторівнева діагностика, формування пам’яті, профілактика) у єдину цілісну архітектуру. Це створює підґрунтя для системного переосмислення підходів до побудови систем захисту. По-друге, імітаційна модель слугує мисленнєвим експериментом – способом формалізувати ідеї ще до етапу інженерного прототипування. Вона дозволяє визначити ключові компоненти, їхню взаємодію та потенційні «точки росту» для подальших R&D-досліджень. По-третє, запропонована модель виконує освітню функцію. Вона допомагає фахівцям із кібербезпеки уявити, як принципи з іншої дисципліни (медицини) можуть бути інтегровані у їхню практику. Такий міждисциплінарний підхід стимулює пошук нових рішень для підвищення стійкості цифрової інфраструктури.

Обґрунтуємо абстрактну архітектуру та її цінність як практичного інструменту для планування інновацій у сфері кіберзахисту. Запропонована імітаційна модель кіберімунної відповіді будується за аналогією з біологічною імунною системою людини, яка характеризується багаторівневою структурою, взаємодією спеціалізованих клітин і механізмами самонавчання [4]. Кожен компонент цієї моделі виконує специфічну роль, що разом створює цілісний, адаптивний механізм захисту (рис.5).

Рис.5. Візуалізація імітаційної моделі кіберімунної відповіді

Клітини-розвідники (сенсори, IDS-агенти): відповідають за постійний моніторинг мережевого трафіку та активності системи. Вони виконують функцію первинного виявлення аномалій або потенційних «антигенів» — підозрілих патернів чи дій.

Макрофаги (IPS, фільтруючі вузли): здійснюють швидке реагування — ізоляцію або блокування виявлених загроз на ранньому етапі. Їхня роль полягає у запобіганні поширенню атаки в межах інфраструктури.

Т-клітини (аналітичні ML-агенти, SIEM): координують реагування системи, проводять поглиблений аналіз інцидентів, класифікують загрози та ухвалюють рішення про подальші дії. Це рівень стратегічного керування безпекою.

Клітини пам’яті (бази інцидентів, системи Threat Intelligence): зберігають інформацію про попередні атаки, типові сценарії реагування та ознаки компрометації; дозволяє системі швидко впізнавати схожі загрози у майбутньому та підвищувати ефективність захисту.

Кістковий мозок (центри оновлення, R&D): відповідає за створення нових «антитіл» –

оновлених правил, сигнатур, політик безпеки. Це аналог постійної еволюції системи через дослідження нових загроз і генерацію оновлень.

Візуалізація узагальнює ідею побудови адаптивної, самонавчальної архітектури кіберзахисту за медичною аналогією. Багаторівнева архітектура дозволяє моделювати поведінку кіберзахисної системи як єдиного адаптивного організму, здатного не лише відбивати відомі атаки, але й самостійно вчитися та вдосконалювати свої механізми протидії у відповідь на нові загрози [10].

Принципи біологічної імунної відповіді: клітини-розвідники — IDS/сенсори для виявлення аномалій; макрофаги – IPS для ізоляції та блокування; Т-клітини – ML-агенти, SIEM для аналітики й координації; клітини пам'яті – бази інцидентів, Threat Intelligence; кістковий мозок – центри оновлення правил, R&D.

Приклад сценарію роботи системи. Для кращого розуміння пропонованої архітектури варто розглянути спрощений сценарій її функціонування у реальному середовищі. Виявлення аномалії. Сенсори та IDS-модулі постійно моніторять трафік і події на хостах. При виявленні підозрілої активності формується початкове повідомлення про загрозу. Попередня оцінка (швидкий скринінг). IPS-модулі (макрофаги) здійснюють негайну перевірку сигнатур і поведінкових правил. Якщо загроза підтверджується – з'єднання блокується або ізолюється.

Поглиблений аналіз. Підозрілі випадки передаються на розгляд аналітичним модулям (Т-клітинам) – ML-агентам або SIEM-системі, які здійснюють кореляцію подій, класифікацію типу атаки та приймають рішення про подальші дії.

Реакція та ізоляція**.** На основі результатів аналізу формуються правила реагування – карантин хосту, зміна політик брандмауера, блокування певних портів чи процесів.

Запис у пам'ять системи**.** Інформація про інцидент, ознаки компрометації та ефективні дії реагування зберігаються у базі знань (клітини пам'яті), що дозволяє швидше реагувати на подібні загрози у майбутньому.

Оновлення та еволюція. Центри оновлення (кістковий мозок) аналізують накопичені дані про нові типи атак, розробляють нові сигнатури, оновлення правил і політик безпеки для розповсюдження на всі вузли системи.

Такий сценарій демонструє можливість створення самонавчальної системи кіберзахисту, яка поєднує швидке реагування, поглиблений аналіз, накопичення знань і постійне вдосконалення [16].

Порівняння з класичною SIEM-архітектурою. Порівняння має важливе значення для оцінки практичності запропонованої кіберімунної моделі. SIEM є стандартним елементом сучасних систем кіберзахисту, забезпечуючи централізований збір, зберігання, кореляцію та аналіз подій безпеки з різних джерел.

Наведемо переваги SIEM-систем. Централізація даних: консолідація журналів подій і логів з різних систем для єдиного моніторингу. Кореляція інцидентів: можливість виявлення комплексних атак через аналіз патернів і зв'язків між подіями. Аудит і відповідність: підтримка відповідності стандартам (PCI DSS, ISO 27001) через документування і зберігання даних. Підтримка розслідувань: надання даних для форензики і аналізу інцидентів.

Обмеження і виклики традиційних SIEM. Реактивний характер: фокус на виявленні після факту, з потенційною затримкою між компрометацією і сповіщенням. Обмежений контекст: аналіз переважно базується на логах без повноцінної оцінки поточного стану системи чи користувача. Високий рівень FP/FN: значна кількість хибнопозитивних і хибнонегативних спрацювань через жорстко задані правила. Трудомістке обслуговування: потреба ручного оновлення правил, сценаріїв кореляції і постійного налаштування.

Обмежене самонавчання: відсутність або обмежене використання механізмів машинного навчання та автоматичного оновлення знань.

Медична імунна система функціонує як інтегрована багаторівнева структура з можливістю раннього виявлення, локалізації, координації реагування та формування імунної пам’яті. Аналогічно кіберімунна модель прагне подолати обмеження SIEM через:

1) децентралізовану архітектуру агентів, які забезпечують гнучке розгортання моніторингу; 2) механізми швидкого реагування на рівні IPS/IDS (аналог макрофагів); 3) координацію через аналітичні модулі (аналог Т-клітин); 4) збереження знань про атаки (клітини пам’яті); 5) автоматичне оновлення та генерацію нових правил (кістковий мозок) [1].

Результати порівняльного аналізу

За такими параметрами можна умовно оцінити відмінності між традиційною SIEM-архітектурою та запропонованою кіберімунною моделлю.

1.Швидкість виявлення і реагування: SIEM часто має затримки через централізований аналіз журналів після факту. Імунна модель передбачає локальне виявлення агентами в реальному часі.

2.Контекстна обізнаність: SIEM обмежена історичними логами без поточного стану системи. Імунна модель інтегрує динамічну оцінку стану хостів і поведінковий аналіз.

3.Самонавчання і оновлення: класична SIEM потребує ручного оновлення правил, що збільшує ризик FP/FN. Імунна модель передбачає автоматичне збереження досвіду інцидентів і генерацію нових правил.

4.Масштабованість: SIEM-централізація ускладнює горизонтальне масштабування без збільшення витрат. Імунна модель ґрунтується на розподілених агентах, що легше масштабуються.

5.Ефективність профілактики: SIEM майже не має профілактичного рівня. Імунна модель включає автоматичне оновлення політик і навчання користувачів.

Умовна інтегральна оцінка: імунна модель пропонує підвищення ефективності захисту за рахунок скорочення часу реагування, зменшення FP/FN, кращої адаптивності до нових типів атак і можливості накопичення колективного знання про загрози. У таблиці 6 показано порівняння класичної SIEM та кіберімунної моделі.

Таблиця 6.

Порівняння класичної SIEM та кіберімунної моделі

Параметр	Класична SIEM	Кіберімунна модель
Швидкість виявлення і реагування	Централізований аналіз логів → затримка між атакою і сповіщенням	Локальне виявлення агентами → реагування в реальному часі
Контекстна обізнаність	Історичні логи без оцінки стану системи	Динамічний моніторинг стану, поведінковий аналіз
Самонавчання і оновлення	Ручне налаштування правил	Автоматичне збереження досвіду і генерація нових правил
Масштабованість	Централізована архітектура обмежує горизонтальне масштабування	Розподілена система агентів → легка масштабованість
Ефективність профілактики	Відсутня або мінімальна	Автоматичне оновлення політик, навчання користувачів

Ця таблиця підкреслює системні відмінності між класичними SIEM-рішеннями та запропонованою кіберімунною моделлю. Хоч SIEM є критично важливою для централізованого аудиту, форензики і відповідності стандартам, вона є переважно реактивним інструментом з обмеженою контекстною обізнаністю та автоматизацією.

Кіберімунна модель пропонує інший підхід: децентралізоване, багаторівневе і самонавчальне середовище захисту, що поєднує швидке локальне реагування з накопиченням колективного знання про атаки. Це дозволяє знизити час реагування, підвищити точність виявлення та адаптуватися до нових типів загроз [17].

Висновки. У статті виконано комплексний міждисциплінарний аналіз можливостей перенесення принципів біологічної імунної системи та медичних протоколів у сферу кіберзахисту. Проведено порівняння етапів розвитку біологічних інфекцій і сучасних кібератак, що дало змогу виявити структурні паралелі та визначити універсальні стратегії реагування. Підтверджено доцільність використання медичних аналогій для побудови багаторівневих, адаптивних і самонавчальних систем кіберзахисту.

Проведено аналіз архітектури SURICATA та визначено обмеження класичних IDS/IPS у контексті адаптивності, формування пам'яті та профілактики. Запропоновано концепцію імітаційної моделі кіберімунної системи, яка об'єднує переваги біологічної імунної відповіді та сучасних технологій машинного навчання для побудови стійких і гнучких захисних архітектур. Розроблено сценарії застосування імітаційного моделювання як інструменту валідації та розвитку нових підходів до кіберзахисту, що дозволяє не лише перевірити життєздатність концепцій, а й виявити їхні переваги й обмеження до етапу практичного впровадження. Проведено порівняння з класичними SIEM-системами та показано, що імунна модель забезпечує вищу швидкість реагування, кращу адаптивність і можливість накопичення колективного знання про загрози.

Результати дослідження можуть бути використані для удосконалення сучасних IDS/IPS-систем шляхом впровадження багаторівневої діагностики, механізмів самонавчання та формування кіберпам'яті; розробки нових прототипів захисних систем, що поєднують переваги біологічних і цифрових підходів; підвищення стійкості IT-інфраструктур до складних, цільових і нових типів атак; оптимізації процедур реагування, профілактики завдяки використанню імітаційного моделювання як інструменту валідації.

Стаття закладає підґрунтя для подальших досліджень у сфері інтеграції медичних принципів у кібербезпеку, пропонуючи нову концептуальну модель, що поєднує міждисциплінарний підхід, імітаційне моделювання та сучасні інструменти кіберзахисту. Отже, проведене дослідження підтверджує ефективність і перспективність використання імунних принципів і імітаційного моделювання для розвитку адаптивних, самонавчальних і стійких систем кіберзахисту нового покоління.

Список літератури

1. Tallam K. The Cyber Immune System: Harnessing Adversarial Forces for Security Resilience. arXiv preprint arXiv:2502.17698. 2024. 15 p. URL: https://arxiv.org/abs/2502.17698.
2. Widuliński P. Artificial Immune Systems in Local and Network Cybersecurity. *ACIG Journal.* 2023. Vol. 12. No. 3. C. 34–45. URL: https://www.acigjournal.com /pdf-184306-105064.
3. Marshall J.S. The cyber-physical immune system: work-in-progress. 2022. No. 4. P. 56–67. URL: https://journals.indexcopernicus.com /publication/4485947.
4. Forrest S., Hofmeyr S. Immunology as inspiration for computer security. *Nature*. 1999. Vol. 397. P. 34–36.
5. World Economic Forum. What the human body teaches us about cyber security. 2015. URL: https://www.weforum.org/stories/2015/08/good-immune-system-wards-off-cyber-threats/
6. Nasreen F. Digital immune system. LinkedIn, 2024. URL: https://www.linkedin.com/pulse/digital-immune-system-fathima-nasreen-awevc
7. Yang H. A Survey of Artificial Immune System Based Intrusion Detection. *Journal of Biomedical Science and Engineering.* 2014. Vol. 7. No. 3. P. 147–156. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC3981469/
8. Rotimi E. Cyber Immune: A New Paradigm in Cybersecurity. LinkedIn, 2024. URL: https://www.linkedin.com/posts/enitan-rotimi-a763baa-cyber-immune-a-new-paradigm-in-cybersecurity-activity-7245067066808963073-loNu
9. Suricata Project. Suricata IDS/IPS Documentation. 2025. URL: https://suricata.io/docs/

10. Stamus Networks. Suricata Architecture Overview. 2024. URL: https://www.stamus-networks.com/suricata-architecture
11. Yu Q. An Immunology-Inspired Network Security Architecture . *Computers & Security*. 2022. Vol. 115. P. 102–115.
12. Hackzone.in. Suricata IDS: Protocol Analysis and Anomaly Detection. 2024. URL: https://hackzone.in/suricata-ids-protocol-analysis
13. Tecracer. SIEM Integration with Suricata. 2024. URL: https://www.tecracer.com/blog/siem-integration-suricata
14. Kantharaju V. Artificial Immune System Inspired Intrusion Detection in IDS/IPS. *IEEE Access*. 2023. Vol. 11. P. 1234–1246.
15. Беляєва О.В., Грицик В.А. Імітаційне моделювання систем захисту інформації: методи та засоби . *Інформаційна безпека*. 2023. Т. 29, № 1. С. 55–68.
16. Сиропятов О.А., Тимошенко Л.М. Кіберімунна модель захисту даних: міждисциплінарний аналіз, діагностика та архітектура. *Informatics and Mathematical Methods in Simulation*. 2025. Vol.15. No. 2. P. 260-275.
17. Gartner Precedence Research. Digital Immune System Market Trends and Forecast. 2024. URL: https://www.gartner.com/en/ insights/digital-immune-system

SIMULATION MODEL OF A CYBER-IMMUNE SYSTEM: TRANSFERRING MEDICAL PRINCIPLES TO MODERN CYBER DEFENCE

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 proposes an interdisciplinary approach to enhancing the resilience of information systems by transferring the principles of the biological immune system and medical protocols to the field of cybersecurity. A comparative analysis was conducted of the phases of development of biological infections (e.g. those of the virus causing the disease known as "coronavirus", or "covid-19", and the liver fluke Hepatitis A) and modern cyberattacks (e.g. the "PlugX" and "Worm" viruses and the "ILOVEYOU" worm). This analysis enabled the identification of structural parallels and the definition of universal response strategies. This study focuses on the potential integration of medical principles into the architecture of contemporary IDS/IPS, using the SURICATA system as a case study. The fundamental limitations of analogies related to differences in transmission mechanisms, environment architecture, and threat behaviour are described. The author proposes a conceptual simulation model of a cyber defence system based on a multi-level structure, self-learning, automatic policy correction and cyber memory. The model incorporates components that are responsible for monitoring, rapid response, analytics, knowledge accumulation and the evolution of defence mechanisms. A comparison with classical SIEM systems is carried out and it is demonstrated that the immune model provides a higher response speed, better adaptability and the ability to accumulate collective knowledge about threats. The practical significance of the study lies in the possibility of using simulation modelling to validate new approaches to cyber defence, optimise response and prevention procedures.The article establishes the foundation for subsequent research endeavours concerning the integration of medical principles into the domain of cybersecurity. It proposes the concept of decentralised, self-learning, and resilient new generation defence systems.

Keywords: cyberimmune system, medical protocols, multilevel diagnostics, SURICATA, simulation model of cyberimmune response, cybermemory, adaptive protection.