Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Застосування штучних імунних систем у забезпеченні інформаційної безпеки

Виконав: студент VI курсу, групи СБм-61
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Гангала О.М. (прізвище та ініціали)

Керівник (підпис) Александер М. Б. (прізвище та ініціали)

Нормоконтроль (підпис) Лечаченко Т.А. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль - 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

		ЗАТВЕРДЖУЮ		
		Завідувач кафедри		
				Загородна Н.В.
		(підпис)		(прізвище та ініціали)
		«__» _____ 2021 р.		

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Гангалі Олександру Михайловичу
(прізвище, ім'я, по батькові)

1. Тема роботи Застосування штучних імунних систем у забезпеченні інформаційної безпеки

Керівник роботи Александер Марек Богуслав, д.т.н., проф., кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора «16» 11 2023 року № 4/7-1061

2. Термін подання студентом завершеної роботи 25.12.2023р.

3. Вихідні дані до роботи наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
1. Аналіз предметної області.
2. Теоретична частина.
3. Побудова моделей імунологічних систем.
4. Охорона праці та безпека в надзвичайних ситуаціях

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

1. Тема роботи. 2. Актуальність. 3. Мета, задачі дослідження, об'єкт, предмет дослідження. 4. Наукова новизна, практичне значення роботи. 5. Поняття штучної імунної системи. 6. Схема функціонування системи виявлення аномалій. 7. Напрямки досліджень ШІС. 8. Структурна схема імунокомп'ютингу. 9. Основні сфери застосування імунологічного підходу в ІБ. 10. Структура системи виявлення вторгнень. 11. Порівняльний аналіз імунної системи людини та антивірусної програми. 12. Структура антивірусного захисту з урахуванням імунологічних принципів. 13. Структура двопотокової моделі аутентифікації. 14. Структура системи активного аудиту. 15. Функціональна модель імунологічної системи захисту інформації. 16. Модель принципу дії. . 17. Структурна модель 18. Основні результати дослідження

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., зав. каф. КС		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з АГРБ		

7. Дата видачі завдання 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.11 – 17.11	*Виконано*
2.	Підбір джерел про дослідження імунологічних систем у		
	забезпеченні інформаційної безпеки	18.11 – 26.11	*Виконано*
3.	Опрацювання джерел про дослідження імунологічних		
	систем у забезпеченні інформаційної безпеки	27.11 – 30.11	*Виконано*
4.	Виконання дослідження щодо розробки моделей		
	імунологічних систем	01.12 – 06.12	*Виконано*
5	Розробка алгоритмів функціонування моделей	07.12 – 10.12	
6.	Оформлення розділу «Аналіз предметної області»	11.12 – 13.12	*Виконано*
7.	Оформлення розділу «Теоретична частина»	14.12 – 15.12	*Виконано*
8.	Оформлення розділу «Побудова моделей імунологічних		
	систем»	16.12 – 18.12	*Виконано*
9.	Виконання завдання до підрозділу «Охорона праці та		
	безпека в надзвичайних ситуаціях»	06.12 – 16.12	*Виконано*
10.	Оформлення кваліфікаційної роботи	14.12 – 19.12	*Виконано*
11.	Нормоконтроль	18.12 – 20.12	*Виконано*
12.	Перевірка на плагіат	16.12 – 19.12	*Виконано*
13.	Попередній захист кваліфікаційної роботи	17.12 – 20.12	*Виконано*
14.	Захист кваліфікаційної роботи	26.12	

Студент _____ Гангала О.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Александер Марек Богуслав
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Застосування штучних імунних систем у забезпеченні інформаційної безпеки // Гангала Олександр Михайлович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2023 // С. – 70, рис. – 19, табл. – 2 , слайдів – 18, бібліогр. – 33.

Ключові слова: ІМУНОЛОГІЧНА СИСТЕМА, СИСТЕМА ВИЯВЛЕННЯ ПОРУШЕНЬ, ІНФОРМАЦІЙНА БЕЗПЕКА, АЛГОРИТМ НЕГАТИВНОГО ВІДБОРУ, ПОДВІЙНА ПЛАСТИЧНІСТЬ, ІМУННА ВІДПОВІДЬ

В першому розділі наведено основні компоненти штучної імунної системи, проведено аналіз теоретичних аспектів дослідження штучних імунних систем у забезпеченні інформаційної безпеки. Здійснено критичний огляд передумов та перспектив побудови моделей штучних імунних систем у інформаційній безпеці, контроль взаємовідносин захищеної системи із навколишнім середовищем.

У другому розділі наведені особливості детектування порушень інформаційної безпеки та призначення способів відповіді на них, описаний сучасний стан та напрямки розвитку імунологічного підходу в інформаційній безпеці, найважливіші області його використання.

У третьому розділі було створено набір моделей імунологічних систем, котрий включає функціональну; принципу дії; структурну. Побудовано алгоритми функціонування моделей. Розроблено алгоритм придушення порушень на основі алгоритму негативного відбору.

У четвертому розділі розглянуто важливі питання охорони праці та безпеки життєдіяльності.

ANNOTATION

Application of artificial immune systems in ensuring information security // Hanhala Oleksandr // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security // Ternopil, 2023 // P. - 70, Fig. - 19, Table - 2, Slides - 18, References - 33.

Keywords: IMMUNOLOGICAL SYSTEM, INTRUSION DETECTION SYSTEM, INFORMATION SECURITY, NEGATIVE SELECTION ALGORITHM, DOUBLE PLASTICITY, IMMUNE RESPONSE

In the first chapter, the main components of the artificial immune system are given, an analysis of the theoretical aspects of the study of artificial immune systems in ensuring information security is carried out. A critical review of the prerequisites and prospects for building models of artificial immune systems in information security, regulation of the relationship between the protected system and the environment was carried out.

In the second section, the peculiarities of the definition of information security violations and the appointment of methods of response to them are given, the current state and directions of development of the immunological approach in information security, the main areas of its use are described.

In the third section, a set of models of immunological systems was created, which includes functional; principle of action; structural Algorithms for functioning of models have been built. A violation suppression algorithm based on the negative selection algorithm is proposed.

The fourth chapter deals with important issues of labor protection and life safety.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

АА – активний аудит.

АНВ - алгоритм негативного відбору.

БД – база даних.

ЗЗІ – засіб захисту інформації.

ІБ – інформаційна безпека.

ІП – імунологічний підхід.

ІС – інформаційна система.

ІТ – інформаційні технології.

КМ – клавіатурний моніторинг.

НСД – несанкціонований доступ.

ОС – операційна система.

ПЗ – програмне забезпечення.

СВВ – система виявлення вторгнень.

СЗІ – система захисту інформації.

ШІС (штучна імунна система) – адаптивна обчислювальна система, що використовує моделі, принципи, механізми та функції, описані в теоретичній імунології, які застосовуються для вирішення прикладних завдань.

ШНМ – штучна нейронна мережа.

ЗМІСТ

ВСТУП

Актуальність теми. У світі інформація стоїть першому місці, будучи найбільш затребуваним ресурсом. Втрата або небажана модифікація інформації в більшості випадків може призвести до значної шкоди. Основне завдання у забезпеченні ІБ – це побудова СЗІ. Найголовнішою проблемою при створенні СЗІ є проблема постійного виникнення нових, раніше не виявлених загроз. Для ефективної роботи система ІБ повинна мати властивість самонавчання, мати механізми генерації нових правил ІБ. Також однією з найважливіших характеристик СЗІ є така властивість як адаптивність, оскільки адаптивна система зберігає працездатність при будь-яких змінах властивостей об'єкта або навколишнього середовища шляхом зміни алгоритму свого функціонування [1].

Принципи роботи та механізми ШІС використовуються для побудови алгоритмів аналізу даних, оптимізації та розпізнавання систем ІБ [2].

Актуальність даної теми обумовлена необхідністю автоматизації процесу реагування СЗІ на порушення, атаки під час функціонування, а також зростанням атак на ІС, що тягне за собою низку різноманітних збитків.

Мета дослідження: дослідити можливості створення ШІС в ІБ та способи детектування порушень.

В роботі поставлено та розв’язано наступні задачі:

– проаналізувати стан та тренди розвитку даного напряму в ІБ;

– виконати огляд можливостей створення моделей ШІС ІБ;

– провести огляд регулювання спорідненості захищеної системи із навколишнім середовищем;

– дослідити способи детектування порушень ІБ та визначення заходів впливу на них;

– з’ясувати основні сфери використання ІП;

– створити моделі ШІС (функціональну, принципу дії, структурну).

Об’єкт дослідження: ШІС.

Предмет дослідження: проектування та використання ШІС у забезпеченні ІБ.

Методи дослідження: наукові роботи українських та зарубіжних вчених за темою дослідження, фундаментальні положення ІБ; методи - аналітичний, порівняльний, системного аналізу, індукції та проектування.

Наукова новизна отриманих результатів:

- досліджено основні способи виявлення порушень у ІБ і призначено заходів впливу на них;
- запропоновано алгоритм придушення порушень на основі АНВ;
- побудовано комплекс моделей ШІС.

Практичне значення одержаних результатів. Результати проведеного дослідження можуть бути використані в реальних установах, підприємствах для автоматичного реагування СЗІ на вторгнення, порушення, атаки під час роботи для мінімізації чи уникнення збитків різного роду.

Апробація. Результати дослідження апробовано на XI науково-технічній конференції «Інформаційні моделі, системи та технології» у вигляді опублікованих тез [4].

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається з вступу, 4 розділів, висновків, списку використаної літератури та додатків. Обсяг роботи: пояснювальна записка – 70 арк. формату А4, графічна частина – 18 слайдів.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Поняття штучної імунної системи

Під ШІС маються на увазі адаптивні обчислювальні системи, котрі застосовують моделі, норми, правила, алгоритми і функції, що описані в теоретичній імунології, та котрі використовуються для розв’язання практичних задач [1-3].

Процес розробки ШІС потребує наявності таких основних складових частин (рис. 1.1) [3]:

– представлення для елементів системи;

– множину певних механізмів, котрі дають змогу оцінити взаємозв’язок індивідуумів із навколишнім середовищем (із однією чи більше цільових функцій) і між собою;

– процедури адаптації, котрі управляють зміною поведінки із плином часу (динамікою).

Рисунок 1.1 – Основні елементи ШІС

Таким чином, формальне зображення й конструювання імунних і гібридних імунних систем припускає наявність трьох компонентів (рис. 2.2):

– схеми зображення компонентів ШІС;

– однієї або більше мір для кількісної оцінки стану системи (афінність і міри оцінки придатності);

Рисунок 1.2 – Структурні елементи ШІС

1.2 Вимоги та наявність умов для побудови моделей імунних систем для їх використання в інформаційній безпеці

Сучасні СЗІ не повністю справляються із завданнями, які до них ставляться: виявлення порушень, підтримка прийнятного рівня захисту. Захист від шкідливого ПЗ, в більшості випадків, реалізується за рахунок використання спеціального антивірусного ПЗ, що здійснює перевірку компонентів комп'ютерної системи на наявність вивчених раніше сигнатур шкідливого ПЗ. Бази сигнатур оновлюються виробником антивірусного ПЗ та постачаються користувачам, які здійснили підписку. У більшості випадків підписка на отримання оновлень антивірусного ПЗ є платною, оскільки вимагає від виробників такого ПЗ витрат на пошук та вилучення сигнатур нових і нових шкідливих програм, що з'являються щодня. Але навіть часті оновлення таких БД не можуть повністю убезпечити систему при зустрічі з новим шкідливим ПЗ, невідомим раніше виробникам антивірусного ПЗ.

Більшість технологій та методів захисту інформації спочатку запозичені із механізмів, підглянутих людиною у живій природі. Багато цих механізмів також є прямим відображенням механізмів організації людського суспільства Шкідливі програми є аналогами вірусів, від яких і отримали свою загальноприйняту назву, їх аналогами у суспільстві є злочинці. Природні механізми дуже складні за рахунок неоднорідності живої природи та не всі вони до кінця вивчені, їх аналоги в ІТ набагато примітивніші. При розгляді та використанні суті природних механізмів не потрібне їх абсолютне усвідомлення, досить близької моделі. Важливим є розгляд захисних механізмів, які живі організми застосовують для підтримки життя у небезпечних умовах довкілля. У таких умовах живі організми були змушені знайти найкращі із можливих способів захисту на всіх рівнях життєдіяльності. Наприклад, механізми імунітету, створені у процесі еволюції, дозволяють знищувати шкідливі клітини всередині організму, і, навіть, частини самого організму, котрі втратили можливість правильно функціонувати. При цьому практично всі живі організми мають можливості виявлення шкідливих впливів та регенерації при незворотних ушкодженнях частини організму, дозволяючи частково або повністю відновити його функціональність, відновивши або замінивши зруйновані тканини.

Розглядаючи механізми імунітету, можна помітити, що існує чітка спеціалізація імунних клітин - деякі з них дозволяють виявити місце прояву проблеми, інші блокують пошкоджені ділянки, дозволяючи локалізувати наслідки, окремі клітини спеціалізуються на виявленні та маркування чужих об'єктів, які нестандартно функціонують власних клітин, існують маркованих об'єктів, а також клітини, що очищають, які видаляють наслідки знищення сторонніх об'єктів і т.д.

Основне питання у забезпеченні ІБ – це створення СЗІ, при якій головною проблемою є безперервна поява нових, раніше незвіданих загроз. Тому для ефективної роботи СЗІ повинна вміти навчатися і сама здійснювати заходи боротьби та захисту. Така СЗІ повинна саморозвиватися, вона могла б самостійно реагувати на загрози ІБ. Також СЗІ повинна бути адаптивною системою, що зберігає працездатність за будь-яких змін внутрішнього чи зовнішнього

середовища. Принцип роботи таких систем полягає в застосування імунної системи людини, котра забезпечує захист організму від різноманітних загроз і є складною адаптивною системою. Головним завданням імунної системи є принцип поділу на «своїх» та «чужих».

При виявленні чужорідних клітин активуються захисні механізми людини. Надалі відбувається розпізнавання цієї загрози, після чого формується пам'ять до неї, щоб надалі при зустрічі такої ж загрози негайно протидіяти їй. Принципи ШІС активно використовуються при вирішенні завдань, пов'язаних з ІБ, наприклад:

– виявлення комп'ютерних вірусів;
– організація парольного захисту;
– моніторинг процесів у системі UNIX та ін.

ШІС необхідна для автоматизації процесу реагування системи на зовнішні та внутрішні порушення функціонування.

У сфері ІБ ШІС можуть вирішувати такі завдання:

– протидія розповсюдженню шкідливої активності;
– виявлення неавторизованого використання інформаційних ресурсів;
– виявлення порушень у ІС;
– виявлення аномалій в інформаційних процесах;
– збереження цілісності інформації;
– управління інцидентами ІБ та ін.

Більшість із перелічених вище завдань зводиться до проблеми знаходження відмінностей «свого» від потенційно небезпечного «чужого».

ІП дозволяє системам навчатися під час функціонування, самостійно виявляти порушення та самостійно продукувати способи боротьби з ними. Внаслідок здатності до навчання під час функціонування, ШІС відносяться до систем штучного інтелекту, які знаходять все більше застосування в СЗІ.

Розпізнавання образів здійснюється централізовано, на системному рівні із застосуванням різних методів зіставлення невідомих зразків із еталонними зразками, використовуючи при цьому такі методи:

– геометричні;
– параметричні;

– статистичні;

– апарат ШНМ та ін.

Ухвалення рішення про те, до якого класу слід віднести невідомий зразок здійснюється після закінчення всього циклу зіставлення зразків, що у багатьох випадках може бути вже запізнілою реакцією.

До найбільш розвинених ІТ, придатних для вирішення завдань ІБ, можна віднести ШНМ та генетичні алгоритми, а до найбільш перспективних - ШІС та імунокомп'ютинг.

Імунна система живого організму здійснює регулювання його взаємовідносин із зовнішнім середовищем у сфері мікробіологічної безпеки, з її допомогою організм людини протидіє чужорідним клітинам. Основна властивість імунної системи людини – виявлення антигенів та активація імунної відповіді. Ключовим механізмом появи такої здатності є негативний відбір – складний фізико-хімічний процес розпізнавання антигенів. При виявленні «чужих» включаються механізми нейтралізації та руйнування антигенів [6-8].

Імунна система здатна ефективно обробляти значні обсяги даних. Дослідження імунних систем у сфері інформатизації, зокрема у сфері ІБ, призвело до появи ШІС. На відміну від ІС ШІС виконують повністю децентралізовану обробку, у тому числі і при вирішенні задач розпізнавання [8, 9].

Можна помітити схожість функцій природної імунної системи з базовими функціями, які має здійснювати система керування інцидентами ІБ:

– детектування, реєстрування, оцінювання подій, які, ймовірно, є інцидентами, збір доказів для здійснення наступного розслідування;

– ідентифікація непередбачуваної події, прийняття рішення в умовах повної невизначеності наявної інформації та за необхідності сповіщення про інцидент;

– ліквідація наслідків непередбачуваної події за допомогою безпекових ресурсів.

Аналогію імунної системи з ІС наведено на рис. 1.3.

Рисунок 1.3 – Аналогія імунної системи людини з ІС

Найпоширенішою моделлю ШІС, що застосовується в області ІБ, є АНВ.

Однією з необхідних складових адаптивних систем захисту є підсистеми моніторингу та АА, за допомогою яких здійснюється збір статистичних даних про події в системі, ключових параметрів функціонування системи та робиться висновок щодо порушень у роботі, можливих аномалій, що відбуваються у системі та відмінності поточного рівня безпеки з допустимим.

Виявлення атак та аномалій у стані системи є процесом виявлення відхилень від еталона стану системи.

ШІС активно застосовуються у таких областях:

– прийняття рішень;
– управління ІБ;
– діагностика атак;
– діагностика аномальних станів;
– розпізнавання образів та ін.

Формування ШІС ґрунтується на імунній системі людини, перевагою якої є можливість отримання протидії до невідомих загроз, що дозволить суттєво підвищити адаптивність механізмів та функцій підсистем захисту інформації та впоратися із проблемами засобів забезпечення ІБ.

Спочатку ШІС необхідний тимчасовий період, під час якого система проходить навчання, формування БД. До кожного стану роботи системи

формується діапазон допустимих значень, в межах якого допустиме певне відхилення. Потім під час функціонування ШІС здійснює оцінку відхилення поточних значень від тих, котрі одержані у період навчання, прийнятих за зразок. Якщо відхилення виходять за межі допустимого інтервалу, то фіксується наявність аномалії або атаки. Наявність високого рівня помилкових спрацьовувань під час використання у локальних мережах характерно для статистичного аналізу.

Імунна відповідь є першим етапом боротьби зі шкідливою активністю, котра запускається відразу ж після реалізації і полягає у локалізації місця впливу шкідливого фактору на елементи СЗІ з метою запобігання подальшого порушення процесу функціонування підсистем захисту інформації та системи в цілому.

Захисний механізм СЗІ включає наступні етапи:

– визначення місця відмови ресурсу, тобто слабкого місця, в якому було реалізовано атаку;

– зняття з цього ресурсу системних процесів;

– перенаправлення системних завдань на інший ресурс;

– виключення ресурсу, що відмовив, з конфігурації СЗІ;

– припинення взаємозв'язку з ресурсом, що відмовив, і заборона доступу до нього;

– спроба відновлення ресурсу, що відмовив.

Якщо порівнювати ШІС з імунною системою людини, необхідно враховувати, що застосування ШІС в ІБ повинно мати різноманітний характер.

Існуючі системи виявлення аномалій мають ряд недоліків, які не дозволяють їх широко використовувати в корпоративних мережах, це пояснюється складністю їх реалізації, що включає:

– вибір методики збирання даних про ІС;

– вибір способу протидії атаці;

– обробку вхідних даних;

– вибір методу визначення атак;

– розподіл навантаження на компоненти ІС.

Вже досліджені методи визначення атак, такі як метод виявлення аномалій

і сигнатурний метод, не дозволяють досягти потрібного ефекту виявлення атак. Нейромережні методи виявлення дозволяють досягти прийнятних характеристик, але мають такі недоліки:

– складність вибору параметрів;
– складність вибору структури ШНМ;
– ресурсомісткий характер навчання ШНМ;
– складність донавчання та перенавчання ШНМ.

Виникає необхідність у виборі та застосуванні такого методу, з допомогою якого стало б можливим уникнути зазначених вище недоліків за необхідного рівня надійності виявлення атак. Перспективним напрямом є побудова систем з урахуванням технологій ШІС. Даний метод має ряд переваг у порівнянні з іншими методами, забезпечуючи:

– високу швидкість роботи;
– порівняно простий алгоритм навчання;
– низьку ресурсомісткість.

Режим функціонування ШІС – безперервний системний процес перевірки ІС на відповідність декларованим цілям політики безпеки, організації обробки даних, норм експлуатації засобів обчислювальної техніки, а також автоматичного реагування на виявлені відхилення.

Виділяючи імунологічні системи, можна сказати, що їхня суттєва перевага перед генетичними алгоритмами та ШНМ - це здатність до навчання та наявність пам'яті.

З наведеного вище можна зробити висновок про те, що дослідження ШІС є дуже перспективним напрямом у забезпеченні ІБ.

1.3 Аналіз налаштовування взаємозв’язків захищеної системи із навколишнім середовищем

Основною задачею системи ІБ є гарантування захисту інформації та постійне функціонування ІС з дотриманням таких властивостей інформації:

– конфіденційність (визначення ймовірних джерел її витоку; запобігання

НСД);

– цілісність (попередження несанкціонованої зміни інформації);

– доступність (попередження несанкціонованого обмеження доступу до інформації).

СІЗ вже свідомо функціонує у небезпечному зовнішньому середовищі. Регулювання взаємовідносин захищеної системи із довкіллям визначається прийнятою політикою безпеки. У разі виявлення порушення ІБСЗІ вживає певних заходів реагування.

Більшість завдань системи ІБ зводиться до проблеми знаходження відмінностей «свого» (користувачів, котрі володіють певними повноваженнями, допустимих процесів, допустимого програмного коду та ін.) від потенційно небезпечного «чужого» (користувачів, які не мають певних повноважень і неприпустимих процесів, зіпсованих даних, шкідливого програмного коду) [7-10].

Регулювання взаємовідносин організму із зовнішнім середовищем у сфері мікробіологічної безпеки називається імунною відповіддю, суть якої полягає в нейтралізації чи знищенні шкідливих клітин. Дане рішення приймається спільними діями клітин імунної системи самостійно, без залучення нервової системи організму (верхніх рівнів ієрархії) [7-10]. Ключовою властивістю ШІС, які не знайшли відображення в АНВ, є їх подвійна внутрішня пластичність. Подвійна пластичність забезпечує функціонування імунологічної системи в умовах безперервних збурень, що викликаються онтогенетичними змінами організму та його взаємодією із зовнішнім середовищем. Подвійна пластичність відображає здатність ШІС до адаптації на основі параметричних та структурних змін. Терміном «параметрична пластичність» позначають механізм адаптації, що дозволяє системі в ході виконання деякої задачі змінювати параметри функціонування підвищення її ефективності [11-13] .

За допомогою подвійної пластичності забезпечується функціонування ШІС в умовах безперервних збурень, що викликаються онтогенезом та зовнішнім середовищем. Структурна пластичність дає системі нові можливості адаптації. У системах взаємодіючих елементів структурна пластичність зводиться до можливості додавання нових елементів та виключення вже існуючих елементів.

Структурні зміни (приплив нових антитіл) відбуваються рідше, ніж параметричні зміни (зміна концентрації антитіл).

Структурні зміни залежить від тимчасової еволюції параметрів системи. Приплив антитіл другого типу відбувається лише після того, як концентрація антитіл першого типу досягає певного рівня. Характер структурних змін визначається системними взаємодіями, а чи не лише зовнішніми чинниками. Нові елементи комплементарні, а не подібні вже наявним.

З розгляду моделі функціонування ШІС можна зробити наступний висновок: досягнення корисного результату отримується за рахунок спільної поведінки системи, а не її взаємодії із зовнішнім середовищем [14-16].

Саме це дає можливість використовувати ІП, важливі властивості ШІС у моделях систем ІБ для застосування властивостей адаптивності в умовах високої динаміки взаємодії з потенційно небезпечним зовнішнім середовищем.

Властивість подвійної пластичності ШІС дозволяє сформулювати основні принципи параметричної та структурної адаптації при їх моделюванні у системах ІБ:

– структурні зміни повинні визначатися динамікою зміни параметрів системи, зумовлених внутрішньо системними процесами, та не залежати від зовнішніх факторів;

– масштаб часу структурної адаптації має бути більшим за масштаб часу параметричної адаптації;

– структурні зміни повинні відбиватися в кількісних характеристиках системи, що відбивають спільні дії елементів.

АНВ, що відображає дві стадії пластичності, властиві ШІС, у спрощеному вигляді виглядає наступним чином:

– початкова конфігурація СЗІ, як моделі ШІС, створюється на основі АНВ, після чого вона включається до режиму функціонування;

– у процесі функціонування СЗІ виникатимуть події, що перебувають у появі рядків вхідного сигналу, зазначених у пам'яті системи як «чужі» (антиген); ці події викличуть активування певних детекторів (антитіла);

– детектори, що активувалися, розмножуються зі збереженням афінності з

рядками вхідного сигналу, що викликали їх спрацювання.

Наведено такий приклад.

На вхід системи надійшов сигнал, що містить поєднання значень

10 30 21,

яке призвело до спрацювання одного з детекторів

8 5 23 10 30 21 14.

Інші позиції рядка заповнюються випадковим чином у заданому діапазоні значень, генеруються нові детектори - вторинні детектори, в яких міститься те саме поєднання, але розміщується на різних позиціях:

- 6 45 10 30 21 86 18
- 98 10 30 21 2 14 61
- 10 30 21 34 67 12 5.

Вторинні детектори перевіряються на відповідність до шаблону «свого». При збігу вторинні детектори видаляються як зайві. З вторинних детекторів, що залишилися, формуються шаблони первинних детекторів. Число згенерованих вторинних детекторів регулюється заданим числом вторинних детекторів, що залишилися після перевірки, відповідно до шаблону «свого». Нові вторинні детектори з позиції моделювання ШІС є антитілами, що належать “чужому” (антигену).

Вторинні детектори необхідні для проведення аналізу вхідного сигналу та сприяють підвищенню ефективності розпізнавання «чужого», що викликав їх появу. При повторному появі «чужого» зі схожими параметрами вторинні детектори будуть функцією пам'яті системи ІБ даний вид її порушення.

Постійний процес створення вторинних детекторів для різних «чужих» призводитиме до необмеженого зростання загальної кількості детекторів.

Передбачувані порушення ІБ та відповідна реакція СЗІ формується як сукупність відгуків усіх детекторів (як первинних, так і вторинних).

Схема формування набору детекторів показано на рис. 1.4.

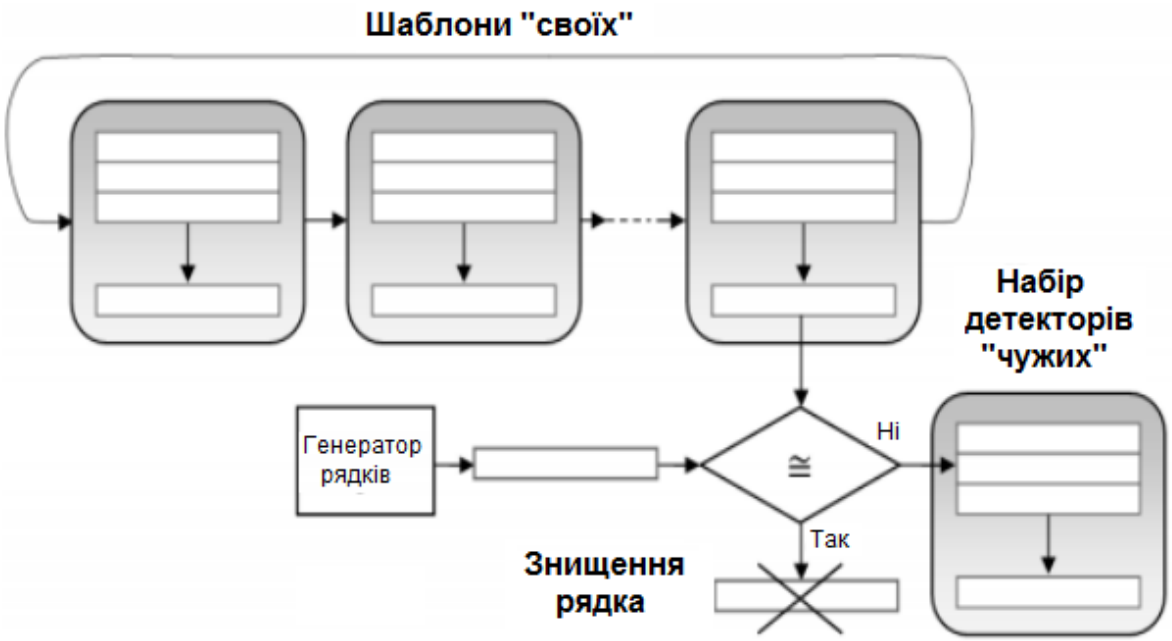

Рисунок. 1.4 – Схема формування набору детекторів

Для постійного контролю детекторів на заданому рівні необхідний механізм їх регулювання. Якщо порівняти ШІС з нервовою системою, то можна вбудувати механізм визначення первинних детекторів, які жодного разу не активувалися в процесі аналізу вхідного сигналу, і знищувати їх у кількості, пропорційній кількості вторинних детекторів, що включаються.

У такому механізмі також має бути функція забування, яка вибиратиме кандидатів на видалення за значенням періоду часу, що минув після їхньої останньої активації [17-19].

Формування детекторів відбувається під час функціонування системи ІБ. Навчання та режим функціонування взаємопов'язані між собою та регулюються внутрішніми взаємодіями елементів, лише опосередковано стимульованими зовнішнім середовищем. Система ІБ, створена за описаною схемою, буде мати адаптивну структуру, котра самоорганізується, орієнтовану на підтримку ефективного рівня виявлення порушень ІБ в умовах довільно змінюються внутрішніх станів ІС і зовнішніх впливів.

Після аналізу було зроблено такі висновки:

– якість моніторингу інформаційними процесами методами ШІС залежить

від кількості детекторів;

– для виявлення «чужих» потрібна достатня кількість рядків.

1.4 Висновки до першого розділу

В цьому розділі приведено поняття ШІС, показано основні її елементи та її структура.

Проаналізовано теоретичні моменти дослідження ШІС у забезпеченні ІБ. Були оглянуті передумови та перспективи побудови моделей ШІС ІБ, можливості управління взаємовідносинами захищеної системи із оточуючим середовищем.

2 ТЕОРЕТИЧНА ЧАСТИНА

2.1 Способи визначення відхилень від правил у інформаційній безпеці і призначення заходів впливу на них

Процес детектування шкідливої активності включають виявлення порушень і аномалій. Порушення - це атаки, які використовують відомі слабкі місця в системах ІТ, а аномалії - це діяльність, що виходить від зовнішніх зловмисників. Процес виявлення аномалій полягає тому, що відбувається порівняння поведінки системи з деяким шаблоном, прийнятим зразок стану системи, при цьому відбувається формування БД. Процес виявлення порушень у тому, що діяльність користувача порівнюється з шаблонами порушників [20] .

Більшість систем виявлення порушень та аномалій ґрунтуються на моделі Деннінга. Суть цієї моделі ґрунтується на: підтримці набору профілів для користувачів, оновленні профілів користувачів, узгодженні записів підсистеми аудиту, оповіщенні про всі виявлені аномалії. Для виявлення аномальної активності застосовуються статистичні методи порівняння, коли порівнюються команди користувача з нормальною поведінкою. Роботу користувача в системі можна представити у вигляді моделі на основі правил [21-23] .

На рис. 2.1 наведено схему функціонування системи виявлення аномалій, що використовує принципи ШІС.

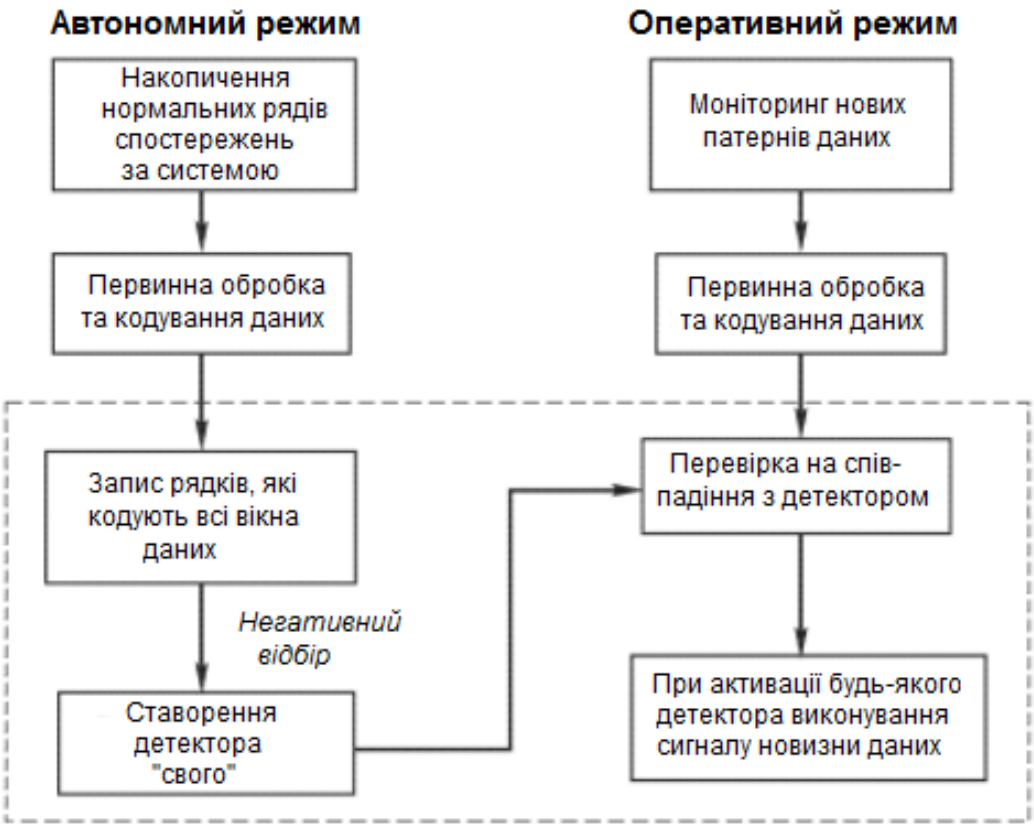

Рисунок 2.1 – Схема функціонування системи виявлення аномалій, що використовує принципи імунітету

Основними алгоритмами, заснованими на методі ІП, є:

– АНВ;

– алгоритм негативної селекції;

– імунна відповідь та ін.

Саме ці алгоритми є основою для моделей СЗІ, проте, необхідне їхнє доповнення та модифікація під конкретний вид функціонування.

У системах виявлення атак використовується наступний варіант застосування ІП: експертні системи доповнюються ШІС для того, щоб знизити частоту помилкових спрацьовувань. Якщо в період навчання ШІС стала виявляти нові невідомі атаки, то необхідно оновити і експертну систему, якщо цього не зробити, то нові атаки, що з'являються, не будуть виявлятися експертною системою.

Якщо ж ШІС представлена самостійно функціонуючою системою виявлення атак, то при обробці трафіку відбувається обробка інформації з метою

виявлення в ньому зловживань. При виявленні активності, прийнятої за атаку, відбувається активація режиму реагування та очікується втручання адміністратора безпеки. Порівняно з попереднім методом, цей підхід швидший.

Властивість адаптивності імунологічних систем дозволяє вирішувати окремі завдання ідентифікації загроз, зіставлення поведінки користувачів з наявними в системі шаблонами, автоматично формувати нові правила при зміні поля загроз, а також реалізувати СЗІ технічної системи в цілому.

Для виявлення порушень у ШІС також використовується АНВ.

У загальному вигляді АНВ формулюється так:

– визначається поняття «свій» як нормальна динаміка поведінки системи, яка описується сукупністю рядків символів фіксованої довжини. При цьому значення даних у рядках квантуються за рівнями;

– створюється набір детекторів «чужих», кожен із яких має збігатися з шаблоном «свого». При цьому використовується правило часткової відповідності, згідно з яким два рядки збігаються тоді і лише тоді, коли вони ідентичні у певному числі суміжних позицій;

– при моніторингу нових надходжень даних спочатку провадиться їх квантування за рівнями у форматі, після здійснюється перевірка змін за допомогою постійного зіставлення з детекторами.

Спрацювання будь-якого детектора означає, що з'явився змінений рядок.

Описаний АНВ спирається на три важливі принципи:

– кожен варіант алгоритму унікальний;

– процес виявлення змін має імовірнісний характер;

– надійна система має виявляти як заздалегідь відомі варіанти змін, а й будь-яку чужорідну активність.

АНВ ґрунтується на перевірці збігів. На рис. 2.2 представлений процес генерації детекторів в АНВ.

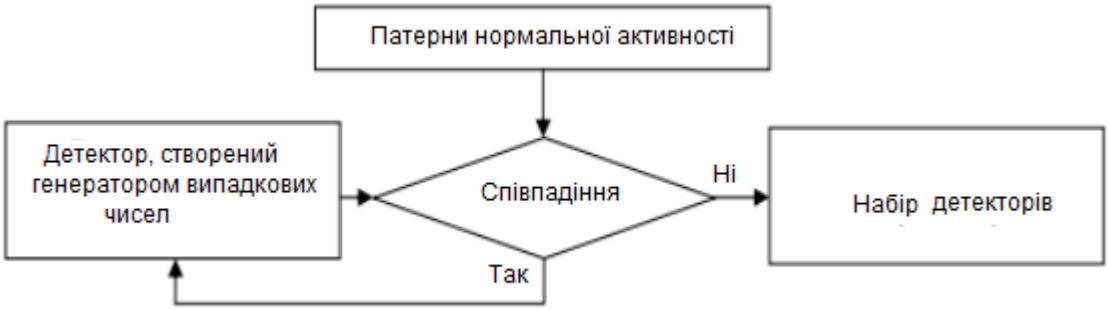

Рисунок 2.2 – Процес генерації детекторів в АНВ

АНВ, що використовується в системах безпеки, у спрощеній формі відображає лише одну початкову стадію формування імунної відповіді.

Перший пункт АНВ моделює принцип мережного уявлення вихідних даних системи ІБ у вигляді сукупності клітин, що підлягають аналізу щодо чужорідності. У другому пункті АНВ показаний принцип формування детекторів, що моделює створення в організмі імунокомпетентних клітин. У третьому пункті АНВ шляхом перевірки вхідного сигналу з детекторами моделюється процес виявлення чужорідних даних (антигенів). У робочому режимі (режимі моніторингу) система функціонує у реальному масштабі часу та реалізує третій пункт АНВ.

Види заходів на порушення ІБ можуть бути істотно різними:

– видалення шкідливого програмного коду,
– закриття портів,
– перевірка прав користувачів для певних дій,
– обмеження дій користувачів та ін.

Прийняття рішення може здійснюватися на різних рівнях ієрархії: на рівні системи безпеки (наприклад, вбудований антивірусний захист); виконання певних дій), а також на вищих рівнях ієрархії управління (наприклад, видача повідомлень адміністратору, який приймає остаточні рішення). Тому при моделюванні системи безпеки на засадах імунологічної системи політику безпеки захищеної системи умовно обмежуються простими реакціями, що зводяться до видачі сигналів про наявність порушень ІБ. Завдання інформаційної цілісності даних вирішується засобами самої системи (дублювання інформації, знищення даних тощо).

2.2 Сучасне становище і аспекти розвитку імунологічного підходу в інформаційній безпеці

В даний час імунна система живого організму відіграє роль джерела нових знань про ефективні алгоритми та структури даних для використання в системах ІБ.

За останнє десятиліття з'явилося значне число моделей, які використовують імунологічні системи як базу або як ключові вузли. ШІС з успіхом використовуються для розв’язання задач оптимізації та класифікації, а для стиснення даних, їх кластеризації, відшукання аномалій, машинного навчання, опрацювання неструктурованих даних та видалення даних, комп'ютерної безпеки та адаптивного контролю.

Про сфери досліджень імунологічних систем в даний час можна стверджувати як про активний етап застосувань та досліджень взаємозв'язку природних систем та ІС через їхню схожість.

Сфера застосування методів, заснованих на принципах імунології, дуже велика, такі методи мають різні назви: ШІС, імунологічні обчислення, системи, засновані на принципах імунітету та ін.

На рис. 2.3 представлені основні напрямки досліджень ШІС

Зараз вивчення імунологічних систем торкаються застосування прогресу у біології в завданнях комп'ютерних наук, удосконалення методів функціонування штучних імунних клітин, дослідження функцій афінності тощо.

Рисунок 2.3 - Напрямки досліджень ШІС

Обчислювальними здібностями імунологічних систем займається напрямок, названий імунокомп'ютингом.

Імунокомп'ютер дозволяє з великою ефективністю вирішувати наступні завдання:

– навчання з експертом,
– самонавчання (навчання без експерта),
– угруповання та класифікації,
– подання результатів обчислень у просторі образів.

Структурна схема імунокомп'ютингу для вирішення перерахованих вище завдань показана на рис. 2.4.

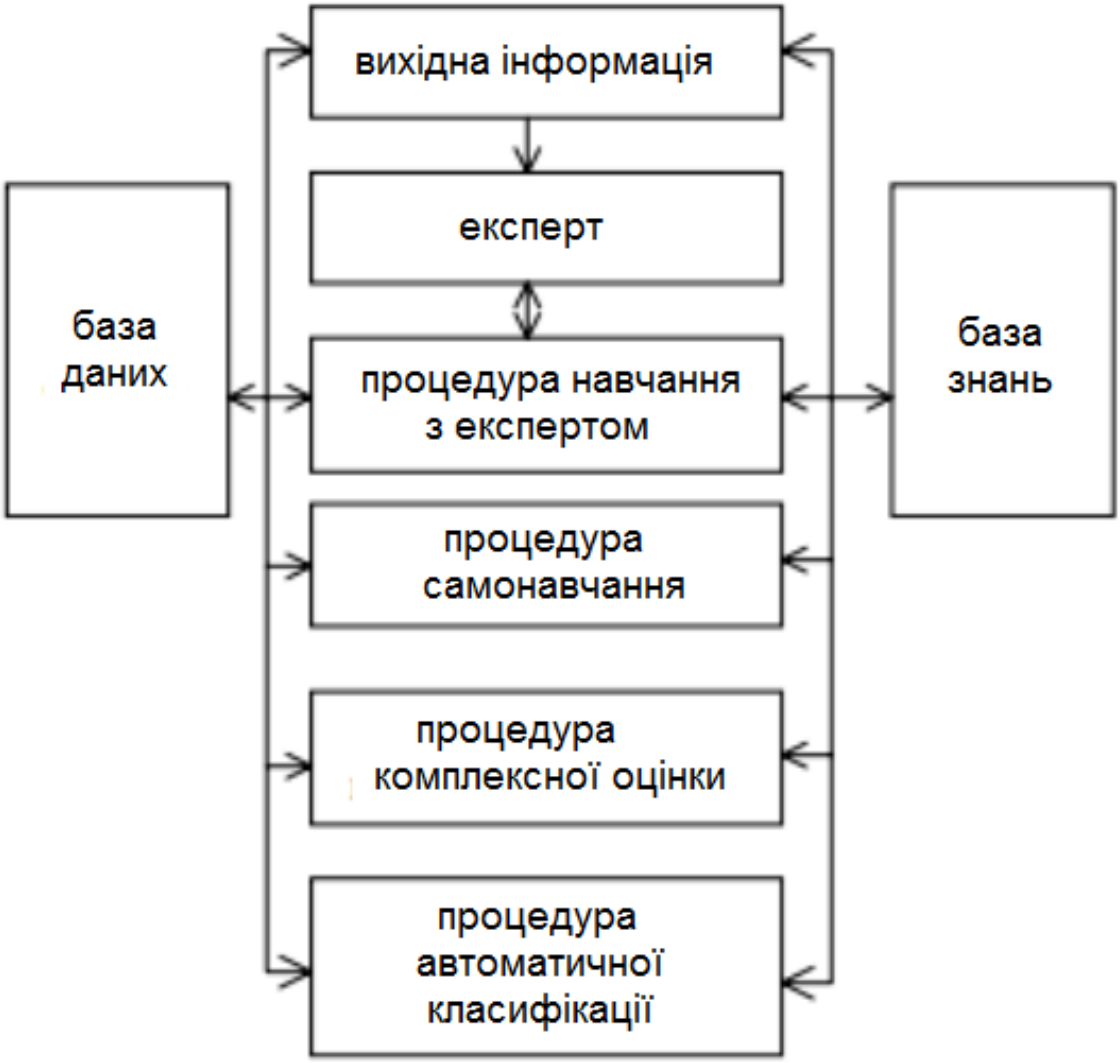

Рисунок 2.4 – Структурна схема імунокомп'ютингу

На основі вихідної інформації формується БД та база знань. У БД містяться дані про систему, у базі знань зберігається інформація, що відображає закономірності та дозволяє отримувати нові знання та прогнозувати у майбутньому можливі стани, відомості про структуру та зміст БД. У основі знань містяться загальнодоступні дані та знання експерта та інших.

Одним із найпоширеніших напрямків ШІС є захист інформації, коли природна імунна система вважається джерелом ідей та методів розв’язання завдань ІБ.

Можна виділити два загальні піднапрямки досліджень ШІС для ІБ:

– виявлення вторгнень на базі АНВ;

– детектування свіжих комп'ютерних вірусів.

Розглядаються питання створення методів визначення аномальної активності в ШІС у порівнянні з її нормальним станом, навчання системи, аналізу ефективності таких систем для захисту від певного типу атак, а також низку інших наукових та практичних узагальнень, що становлять теоретичну та методологічну базу цього дослідження.

До перспективних моделей, що використовують аналогію імунної системи людини та ІТ, належать такі:

– модель оцінки ефективності СЗІ ІТ;
– модель діагностики СЗІ ІТ;
– модель виявлення передумов дії загроз (модель "мертвого коду");
– корпоративна модель СЗІ;
– модель прогнозування дії загроз та ін.

При використанні методу ІП у технологіях та організації СЗІ зменшуються

Досі залишилися не вирішеними питання застосування ІП для автоматизації та інтелектуалізації процесів ІБ, оскільки відкритим залишається питання самостійного ухвалення рішення під час виявлення вторгнення чи аномалії.

У майбутньому, необхідне подальше вивчення та розвиток цього напряму через ускладнення сучасних ІТ, необхідно, щоб ШІС відповідали динаміці змін.

2.3 Основні сфери застосування імунологічного підходу

В даний час принципи роботи та механізми імунологічної системи закладені в основу для побудови алгоритмів аналізу даних, оптимізації та розпізнавання, систем ІБ.

Сфера застосування ШІС дуже велика, тому що ШІС мають різноманітний характер.

ШІС лягли в основу таких засобів (способів) ІБ:

– мережевого самозахисту;
– антивірусного захисту;
– аутентифікації;
– КМ;

– АА та ін.

Ключові сфери використання ІП в ІБ представлені на рис. 2.5.

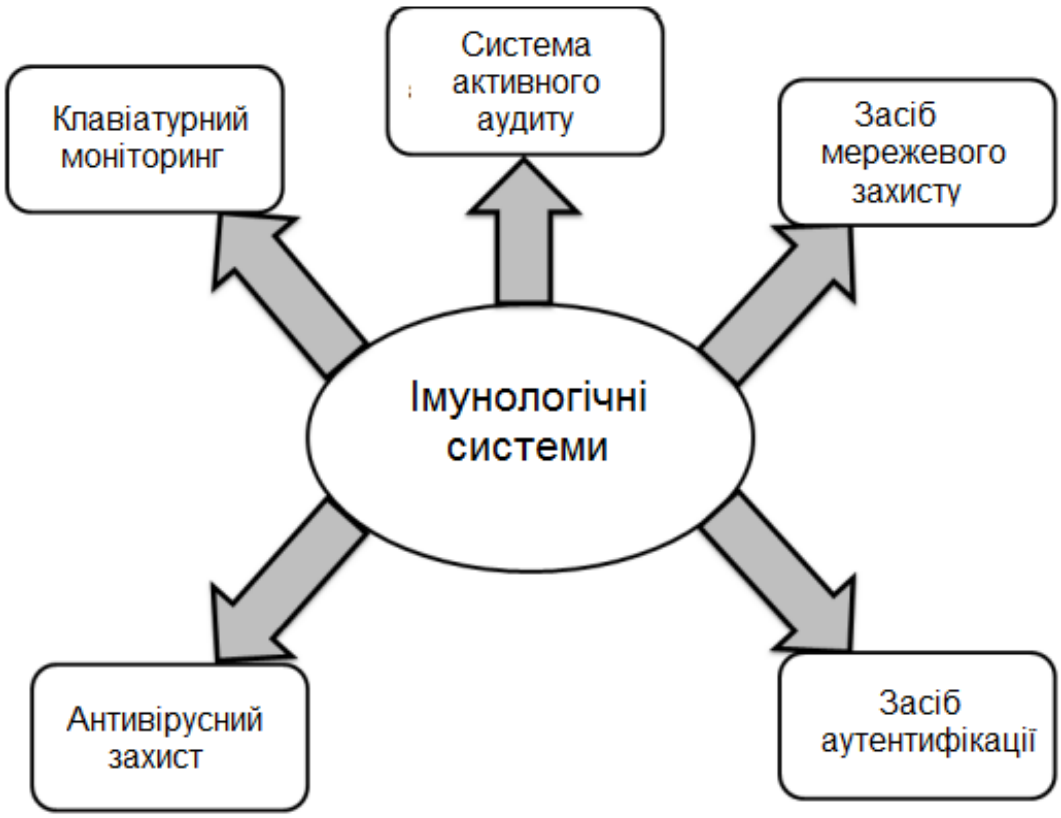

Рисунок 2.5 – Основні сфери застосування ІП

2.3.1 Спосіб самозахисту в мережі

Варто відзначити основні властивості імунної системи людини:

– розподілена;
– така, що самоорганізується;
– легковісна.

Даними властивостями також має володіти СВВ у мережу.

СВВ, побудована на основі ШІС, поділяється на основну та набір вторинних. В основній системі на базі ШІС відбуваються два процеси:

– еволюція генної бібліотеки;
– негативна селекція даних.

На етапі еволюції генної бібліотеки здійснюється збір інформації про аномалії мережного трафіку. У генну бібліотеку ШІС заносяться дані про

кількість пакетів, їх структуру, розмір та ін. Ця інформація є формуючою для наборів детекторів. Враховуючи мережеві протоколи, формуються первинні дані для створення генної бібліотеки. Якщо будь-який детектор виявив шкідливу активність, то вносяться оновлення до генної бібліотеки, заносяться нові гени, що відповідають даній активності. У генній бібліотеці зберігаються тільки гени, що найчастіше зустрічаються, а вже повторювані гени видаляються. Потім генеруються набори предетекторів наступним чином: відбувається комбінування генів, потім за допомогою механізму негативної селекції визначається їхня сумісність і несумісність з нормальним мережевим трафіком. Відбувається аналіз інформації про характер мережного трафіку, потік вхідних даних, котрі поступають від маршрутизатора. Суть полягає у створенні обмеженого набору детекторів, за допомогою якого можна було б найефективніше виявити мережеві аномалії. Такий тестовий набір детекторів розсилається на всі вузли мережі, утворюючи вторинну СВВ.

Відомі сьогодні алгоритми негативної селекції ґрунтуються на імовірнісних характеристиках, тобто використовує неповний збіг. Зміна допустимого відхилення від еталона призводить до зменшення або збільшення помилкових спрацьовувань детекторів, ніж менше допустиме відхилення, тим частіше відбуватиметься виявлення аномалії та навпаки.

При виявленні шкідливої активності відповідний їй детектор розмножується і відправляється розсилкою на інші вузли системи. Власне саме рішення, чи є активність дійсно шкідливою приймається, якщо отримані сигнали від кількох вузлів, а не в оди від одного. У кожному вузлі та в основній СВВ є комунікатор, який здійснює управління рівнем ризику. Якщо якийсь вузол надіслав сигнал про виявлення шкідливої активності, то комунікатор збільшує свій рівень ризику та надсилає повідомлення іншим комунікаторам, які у свою чергу також збільшують свої рівні ризику. Якщо відразу кілька вузлів виявили шкідливу активність за короткий проміжок часу, то рівень ризику різко зростає, і якщо буде перевищено граничне значення ризику, то адміністратору мережі прийде повідомлення про виявлення шкідливої активності [24].

Структура СВВ наведена на рис. 2.6.

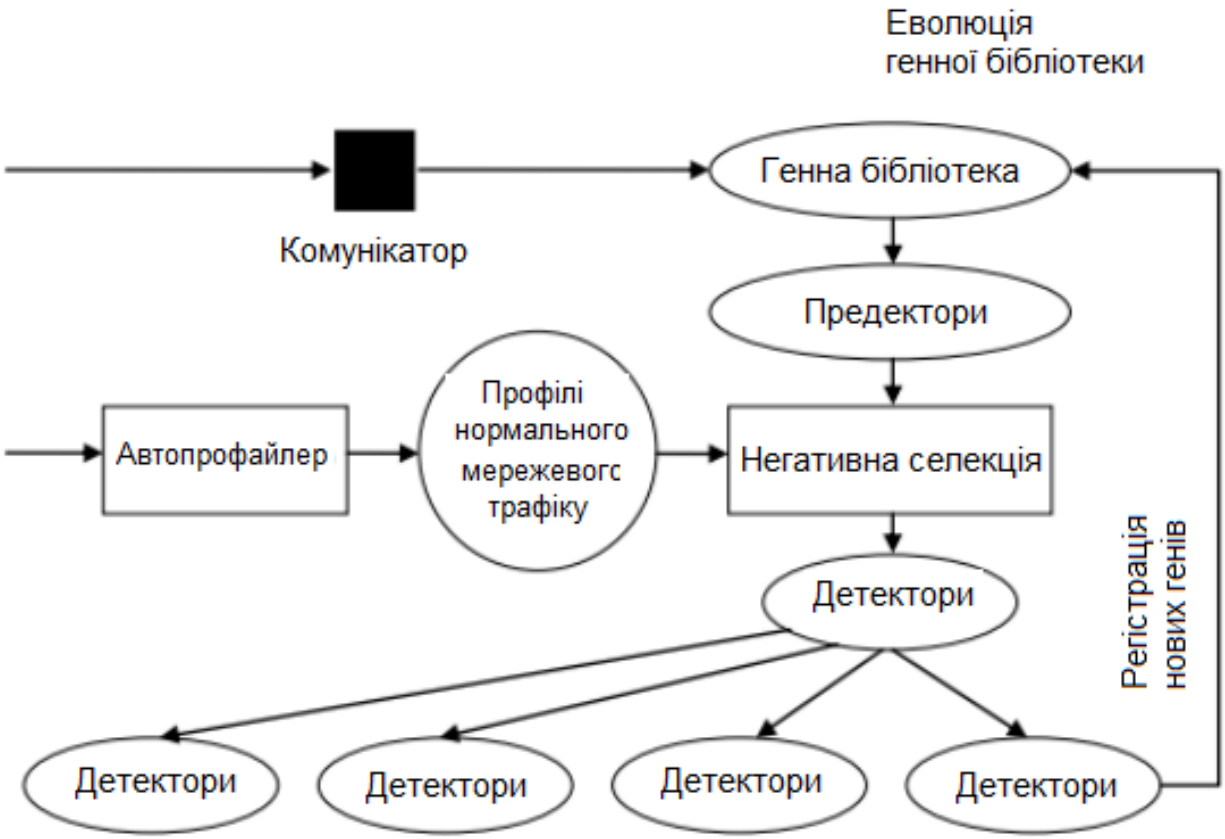

Рисунок 2.6 – Структура СВВ

На рис. 2.7 представлено класифікацію СВВ з погляду ІП.

Архітектура засобу виявлення вторгнень складається з:

– сенсорної підсистеми, що здійснює збір подій;

– сховища, де нагромаджуються первинні події та результати аналізу;

– підсистеми аналізу, яка виявляє атаки та аномальну активність на основі даних, отриманих від сенсорів;

– консолі управління, за допомогою якої можна спостерігати статус системи, котра захищається, переглядати виявлені інциденти, здійснювати управління системою, що захищається.

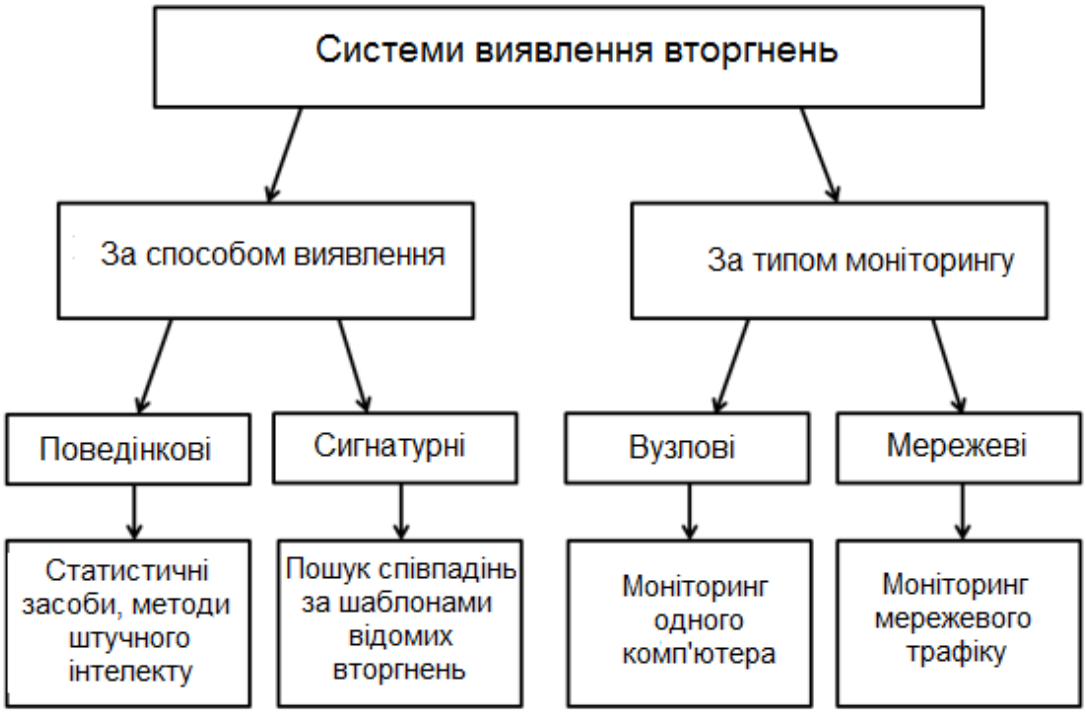

Рисунок 2.7 - Класифікація СВВ

2.3.2 Спосіб антивірусного захисту

Імунна система людини дуже схожа із системою антивірусного захисту, оскільки їх принципи роботи дуже схожі, виконують одні й самі функції. Для виявлення зараження даних і програмних файлів, що захищаються, дуже ефективним є використання такого підходу ШІС, як АНВ.

У таблиці 2.1 наведено порівняльний аналіз імунної системи людини та антивірусної програми.

Таблиця 2.1 - Порівняльний аналіз імунної системи людини та антивірусної програми

Імунна система	Антивірусна комп'ютерна програма
1. Призначення	
Для захисту організму як від внутрішніх порушень, і від зовнішніх вірусів.	Для виявлення та видалення шкідливого коду як від зовнішніх загроз так і від зараження встановленими програмами.

Продовження таблиці 2.1

Імунна система	Антивірусна комп'ютерна програма
2. Функціонування у разі виявлення вже відомих зовнішніх загроз	
У разі потрапляння в організм людини вже відомого вірусу імунна система виявляє його і знищує.	У разі потрапляння до комп'ютера вже відомого вірусу програма виявляє його, ізолює та знищує.
3. Функціонування щодо невідомих зовнішніх загроз	
Невідомий раніше вірус не виявляється і потрапляє в тканини організму, завдаючи шкоди організму.	Невідомий раніше вірус буде пропущений, а він у свою чергу завдасть шкоди комп'ютеру.
4. Функціонування у разі виявлення відомих внутрішніх загроз	
Імунітет повинен їх виявляти та знищувати.	При виявленні небезпечної активності вже встановленого або встановлюваного на комп'ютер ПЗ антивірус має обмежити дію таких програм.
5. Функціонування щодо невідомих внутрішніх загроз	
Збільшується ризик утворення хвороб.	Зростає ризик пошкодження ОС та зниження працездатність комп'ютера.
6. Інформація та навчання	
Отримує базову інформацію та навчання при її народженні: об'ємну БД від попередніх поколінь про всі відомі досі загрози, а також здатність виявляти нові загрози. У процесі життя організм стикається з новими загрозами та система, що отримала базовий імунітет, імунна система повинна їх виявляти та боротися з ними, після чого інформація про загрозу зберігається для подальшого швидкого реагування (вторинний імунітет). Імунна інформація записується на дрібних білкових молекулах - трансфер факторах	Антивірусна комп'ютерна програма має БД про всі вже відомі віруси, а також здатність виявляти нові загрози. Постійно антивірус оновлюється, тобто отримує інформацію про нові віруси та інші загрози і точно знає, як виглядає потенційний шкідник, завдяки чому надійно захищає від них комп'ютер.

Близько 70 % вірусних атак здійснюється із зовнішнього середовища через точку входу в мережу, що захищається, і лише близько 30 % вірусних атак є внутрішніми. Необхідність виявлення зовнішніх загроз вище, ніж необхідність виявлення внутрішніх загроз.

Використання ШІС полягає в тому, що у разі виявлення в мережі ознак зараження відбувається відправлення образу нового вірусу в антивірусний центр, через деякий час створюється оновлення для антивірусної бази, яке розсилається корпоративною мережею з необхідністю випередити поширення вірусу. Даний метод суперечить ІП тим, що антивірусний центр знаходиться поза самою системою, а в ШІС всі процеси відбуваються всередині системи, ця відмінність є дуже вразливим місцем у системі. Коли антивірусний центр знаходиться за межами системи ІТ, що захищається, порушники можуть сформувати канал для завантаження вірусів і шкідливих програм під виглядом оновлення антивірусної бази, отримати доступ до конфіденційної інформації у разі автоматичного відправлення на аналіз підозрюваних на наявність вірусу файлів.

АНВ легко знаходить зміни у заражених файлах, однак, він призначений для захисту постійних файлів даних або програмних файлів, а користувачі регулярно оновлюють ПЗ, редагують файли даних. Це свідчить, що зразок повинен теж постійно змінюватися, відповідати динаміці змін середовищ (внутрішнього та зовнішнього).

Для виявлення комп'ютерних вірусів варто застосовувати метод, котрий базується на принципі імунної відповіді. Суть даного методу полягає в наступному: відомі віруси виявляються за сигнатурами, а невідомі віруси виявляються за аномальною активністю у системі.

Структура технології антивірусного захисту з урахуванням аналогії з імунної системою людини наведена на рис. 2.8.

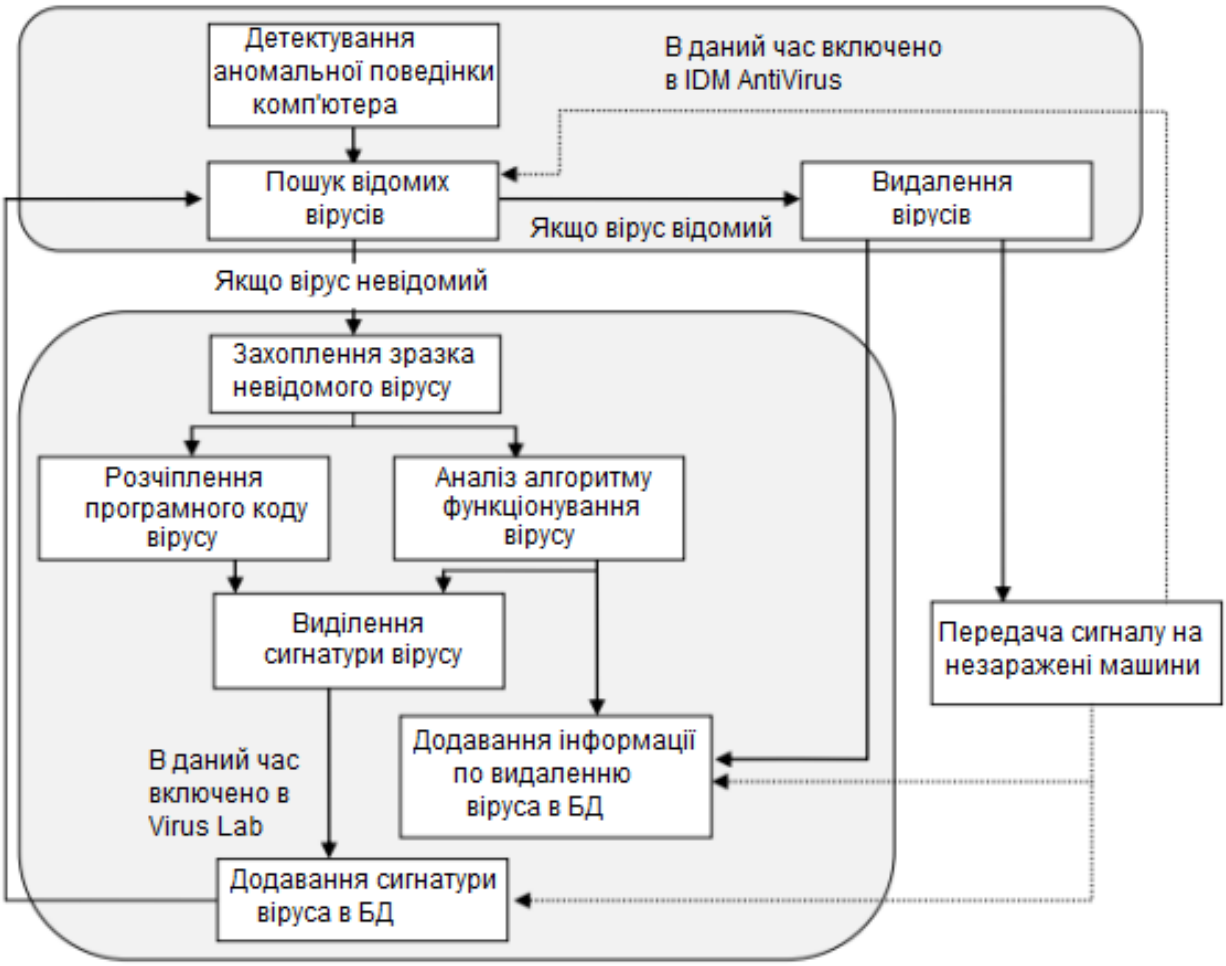

Рисунок 2.8 – Структура антивірусного захисту з урахуванням імунологічних принципів

2.3.3 Спосіб аутентифікації

Найефективнішим ЗЗІ при НСД є система аутентифікації. Найпоширенішою серед систем аутентифікації є двопотокова модель аутентифікації, в якій використовується безліч детектуючих наборів, що оновлюються, на основі ІП. Від імунологічної системи вона успадковує механізми, які дозволяють ефективно розпізнавати дії порушника. Перший потік аутентифікації здійснює в базі пошук загроз, що вже зустрічалися, а другий потік знаходить нові. Також від імунологічної системи успадковується механізм підтвердження результатів, який заснований на отриманні сигналу від сусідніх наборів, що детектують при аналізі масиву даних, що надаються одним і тим же суб'єктом [25].

Структура двопотокової моделі аутентифікації показана на рис. 2.9.

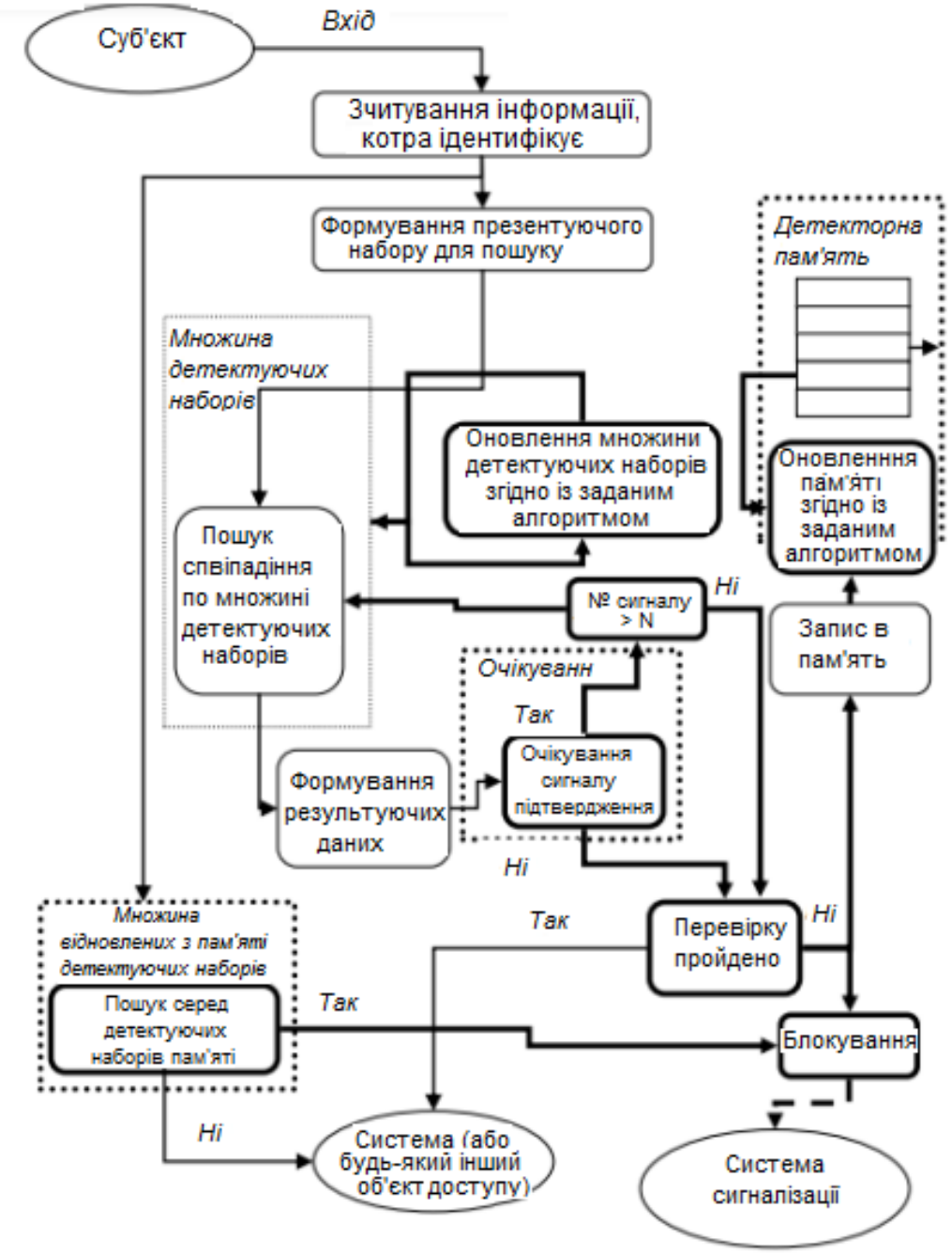

Рисунок 2.9 – Структура аутентифікації із використанням множини наборів, що оновлюються

2.3.4 Спосіб клавіатурного моніторингу

КМ є засобом комп'ютерної безпеки, за допомогою якого здійснюється постійна прихована автентифікація користувачів. Для вдосконалення засобів КМ необхідно аналізувати всі дії користувача повністю, а не окремо. Такий підхід відповідає принципу роботи ШІС. ІП, що використовується в КМ, ґрунтується на АНВ. Засіб КМ працює наступним чином: під час навчання створюється шаблон

кожного користувача, на основі якого формуються детектори для виявлення порушень на множині можливих поєднань клавіатурних параметрів. Засіб КМ виявляє порушення частоти спрацьовування сформованих раніше детекторів [26]
.

З допомогою КМ здійснюється постійний аналіз клавіатурного почерку користувачів комп'ютерних систем. КМ може функціонувати таємно від користувачів, у разі, якщо він є прихованим. На основі прихованого КМ вирішуються такі завдання:

– ведення постійної аутентифікації користувачів;

– проведення оцінки достовірності повідомлень;

– виявлення психофізичних відхилень користувачів від нормального стану;

– виявлення користувачів комп'ютерних систем, які вчинили порушення чи зловживання повноважень.

Перше завдання вирішується для того, щоб створити БД для підрозділу на "своїх" та "чужих". Класифікація користувачів на "своїх" та "чужих" у біометричних системах вирішується двома способами:

– за допомогою верифікації;

– за допомогою ідентифікації.

При верифікації у системі створюється єдиний еталон для кожного користувача, інформація про невідомого користувача порівнюється лише єдиним еталоном. При ідентифікації інформація про невідомого користувача порівнюється з усіма еталонами користувачів. На ефективність роботи систем КМ впливає точність та швидкість здійснення верифікації, які залежать від способів подання та підрозділу клавіатурних параметрів. Клавіатурні параметри зводяться до певного структурованого вигляду, що дозволяє виявити характерні ознаки комп'ютерного почерку користувача, що відрізняється від інших. Під час навчання системи КМ за допомогою характерних ознак і будуються шаблони «своїх», тобто еталон поведінки користувача. Під час роботи здійснюється порівняння характеристик комп'ютерного почерку працюючого користувача з клавіатурним еталоном користувача, що вже склався. Потім, якщо були виявлені

відхилення, робота користувача блокується системою КМ.

Цей метод відповідає імунологічному принципу виявлення аномалій в ІС. В ШІС вхідна інформація аналізується виявлення аномалій шляхом порівняння з детекторами. Порівняння здійснюється не в одиночних, а одночасно у кількох суміжних позиціях. Ширина зони порівняння визначається параметром r, який визначає ступінь зв'язності подій і називається в імунології ступенем афінності.

Як згадувалося вище, робота КМ грунтується на АНВ, важливою відмінністю АНВ від простого розпізнавання, є те що, що зразок формується і використовується лише за навчанні ШІС до створення детекторів. Під час розпізнавання невідомі образи порівнюються не з зразками, і з детекторами.

Застосування ІП в КМ дає можливість отримати системи з наступними властивостями:

– при роботі в системі КМ декількох користувачів, відбувається збільшення числа еталонів, а при використанні АНВ, навпаки, кількість детекторів залишається постійним;

– АНВ виявляє більшу стійкість до шумів через високо розподілену масову обробку даних;

– в АНВ виявлення «чужих» проходить у темпі надходження вхідних даних, і відображається частотою активації детекторів.

Таким чином, застосування ІП до створення засобу КМ є дуже актуальним.

2.3.5 Система активного аудиту

Аудит системи стає дедалі більше застосовуваним у сфері забезпечення ІБ.

Система АА - це процес отримання якісних та кількісних показників про стан системи в порівнянні з еталонними показниками та критеріями безпеки [27].

Суть аудиту полягає у перевірці системи та порівнянні отриманих результатів з еталоном. Виділяються основні складові аудиту, які можуть відрізнятися для різних видів аудиту:

– засоби та способи перевірки системи;

– результат перевірки системи;

– стандарт для порівняння результатів перевірки системи.

Найпоширенішим є АА - дослідження стану захищеності системи з погляду порушника, який є хорошим фахівцем у галузі ІТ та має навички реалізації загроз.

Алгоритм дій АА зводиться до того, що за допомогою спеціального ПЗ та методів здійснюється збирання інформації про стан системи мережевого захисту.

На рис. 2.10 представлено структуру системи АА.

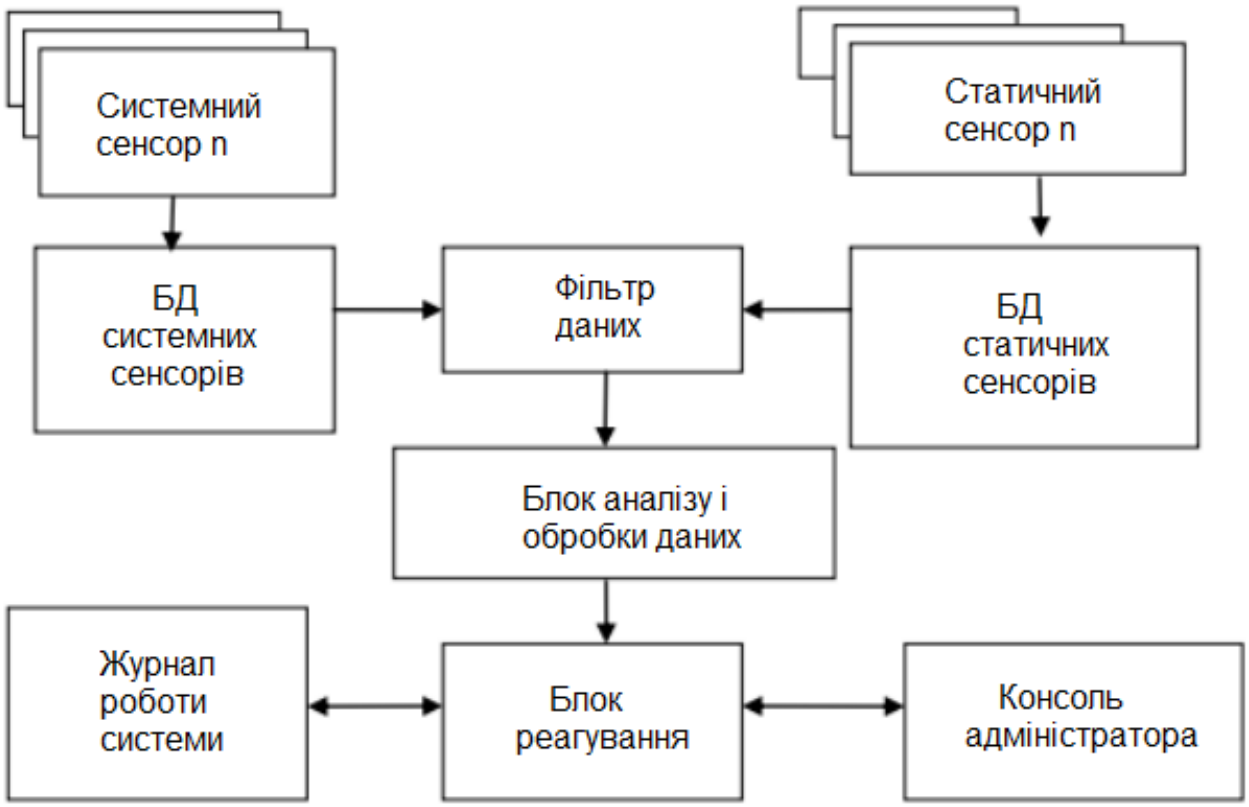

Рисунок 2.10 – Структура системи АА

Система АА складається з:

– набору сенсорів для перевірки інформації про роботу ІС та діях користувачів;

– БД, де зберігаються одержані результати у вигляді звітів;

– блоку аналізу та обробки даних, який проводить обробку вхідних даних та здійснює управління ІС;

– блок реагування, який виконує функцію відповіді;

– сервера адміністратора;

– журналу обліку АА.

Набір сенсорів призначений для порівняння показників системи та дій користувачів, здійснення оповіщень для обробки в блоці аналізу та обробки даних про вже відомі події. Також здійснюється аналіз та прогнозування поведінки всіх користувачів системи. Для користувача створюється окремий профіль, до якого записується вся інформація про його роботу в системі з певною періодичністю, яку задає адміністратор безпеки системи.

Для підвищення ефективності роботи системи в ній є фільтр даних, який видаляє інциденти, що вже зустрічалися. Також фільтр даних необхідний економії пам'яті.

Для підвищення ефективності аналізу вхідної інформації необхідно:

– забезпечити надійне зберігання інформації, що надходить до її обробки системою АА;

– забезпечити швидку обробку сигналів сенсорів з метою виявлення атак системою АА та прийняття рішення щодо запобігання атаці;

– забезпечити безпечне зберігання необхідної інформації з метою збереження історії атак та оновлення профілів користувачів.

При виявленні інциденту система АА приймає рішення про реакцію у відповідь. Система прийняття рішення ґрунтується на нечіткій логіці, за допомогою якої можна прийняти правильне рішення, яке залежить від типу об'єкта, що зазнає загрози та умов виконання порушення.

Реакція у відповідь може бути наступною:

– повідомлення адміністратора системи про інцидент;

– блокування користувача у системі;

– перезавантаження робочої станції;

– вивантаження програм із пам'яті робочої станції та інших.

При проектуванні системи АА слід враховувати, що виклики процесів управління апаратними засобами системи можуть призвести до більш небезпечних ушкоджень, ніж виклики процесів користувача. Також є можливість відслідковувати наслідки двох одночасних атак. Виявляти джерела аномальної активності дозволяють короткі послідовності дзвінків самої системи.

2.4 Висновки до другого розділу

У другому розділі роботи було досліджено шляхи визначення порушень ІБ та виявлення способів реагування на них, стан та аспекти поступу ІП в ІБ, головні сфери використання ІП.

3 ПОБУДОВА МОДЕЛЕЙ ІМУНОЛОГІЧНИХ СИСТЕМ

3.1 Функціональна модель

Функціональна модель необхідна для упорядкування взаємозв'язків підцілей та функціональних операцій.

Було розроблено таку модель імунологічної системи, при цьому були виділені такі рівні функціонування:

– управління;
– рівень мережевих вузлів;
– прикладний;
– компонентів.

На рівні управління здійснюється керування СЗІ. Цей рівень має ієрархічну структуру, що складається з декількох центрів управління, своєю чергою кожен центр управління є самостійним. Центр управління може складатися з кількох серверів адміністрування, а кожен сервер адміністрування керує певною частиною СЗІ. Управління комплексною СЗІ здійснюється на підставі політики безпеки, яка визначає правила функціонування для всіх програмних ЗЗІ.

Рівень мережних вузлів є категорії програмних ЗЗІ, спрямованих на захист різних вузлів мережі (сервера, шлюзи, робочі станції, мобільні пристрої та ін.). На цьому рівні визначаються типи та кількість вузлів мережі, відбувається їх сегментація, а також визначаються відповідні типи програмних засобів захисту, визначається ступінь розподілу проектованої комплексної СЗІ від порушень ІБ.

Прикладний рівень являє собою комплекс ПЗ, спрямованого на захист вузлів мережі залежно від їх призначення та ОС, що використовується. Цей рівень впливає на гетерогенність проектованої комплексної СЗІ від порушень ІБ, визначає типи політик безпеки.

Рівень компонентів складається з модулів, що входять до складу ПЗ та спрямовані на захист від конкретних загроз [28].

Для створення функціональної моделі ШІС необхідно спочатку визначити мінімальний набір вимог до системи, яким вона повинна задовольняти.

Описана схема дозволяє створити шаблон системи захисту від порушень ІБ на підставі сформованого списку функціональних операцій, що виконуються СЗІ.

Шаблон СЗІ на базі ІП складається з наборів функціональних операцій:

– котрі виконуються імунними механізмами захисту;
– які виконує система управління програмними засобами захисту.

Для формування шаблону СЗІ був складений список функціональних операцій, виконуваних імунними механізмами захисту та системою управління цими механізмами. Потім був проведений аналіз списку функціональних операцій для виявлення найбільш значущих і важливих з точки зору їх застосування у ШІС та СЗІ експертами з ІБ.

До списку функціональних операцій були включені наступні:

– захист робочих станцій;
– захист файлових серверів;
– захист інтернет-шлюзів;
– захист серверів БД;
– захист усієї системи;
– попередження потенційних загроз;
– виявлення погроз;
– виявлення погроз;
– ліквідація загроз;
– ліквідація наслідків загроз;
– оповіщення про шкідливу активність;
– блокування частини функцій системи;
– припинення роботи всієї системи;
– формування звітних документів;
– очікування на прийняття рішення;
– ідентифікація осіб, які претендують на доступ;
– реєстрація звернень до ресурсів, що захищаються;
– перевірка повноважень;
– реагування під час спроб несанкціонованих дій користувачів;
– розпізнавання об'єкта чи суб'єкта за пред'явленим ідентифікатором.

Слід зазначити, що у цьому дослідженні слід покладатися на компетентність експертів, оскільки виявлення критеріїв значимості функціональних операцій важко відтворити практично.

В якості експертів мною було обрано 3 спеціалісти, які мають достатній досвід у галузі ІБ, чия професійна діяльність безпосередньо пов'язана із забезпеченням ІБ в різних організаціях:

– студентка кафедри КБ Бучко Анастасія (працівниця ТОВ ХАБЛЕЙЗ)
– студент кафедри КН Тененський Максим (працівник ТОВ Unicorn UA);
– інженер 1-ої категорії ЦІТ університету Лобур Тарас.

Опитування експертів з ІБ здійснювалося методом анкетування. В анкеті необхідно було проранжувати функціональні операції з погляду їхнього досвіду та міркувань, а також значущості. У цьому найзначніша функціональна операція має посісти перше місце, а найменш значима - останнє місце.

Основне призначення системи ІБ - це забезпечення безпеки інформації та функціонування за будь-яких умов.

Основні завдання, що висуваються до ШІС:

– захист об'єктів системи;
– визначення підцілей забезпечення безпеки;
– міра реагування на інцидент;
– керування доступом.

Проаналізувавши заповнені експертами з ІБ анкети, було виявлено такі основні функціональні операції:

– захист усієї системи;
– попередження потенційних загроз;
– оповіщення про шкідливу активність;
– реагування під час спроби несанкціонованих дій.

Анкета, котру повинні заповнити експерти з ІБ, представлена у табл. 3.1.

Таблиця 3.1 – Анкета для заповнення експертами з ІБ

П.І.Б. експерта _____

Посада, науковий ступінь_____

Функціональна операція	Коефіцієнт значущості (від 1 до 5)
Захист об'єктів системи	
захист робочих станцій	
захист файлових серверів	
захист інтернет шлюзів	
захист серверів баз даних	
захист усієї системи	
Підцілі забезпечення безпеки інформації	
попередження потенційних загроз	
виявлення погроз	
виявлення загроз (можливість появи загроз)	
ліквідація погроз	
ліквідація наслідків загроз	
Міра реагування на інцидент	
оповіщення про шкідливу активність	
блокування частини функцій системи	
припинення роботи всієї системи	
формування звітних документів	
очікування на прийняття рішення	
Управління доступом	
ідентифікація осіб, які претендують на доступ	
реєстрація звернень до ресурсів, що захищаються	
перевірка повноважень	
реагування під час спроб несанкціонованих дій	
упізнання об'єкта чи суб'єкта за пред'явленим ідентифікатором	

Дата заповнення , підпис_____

На основі аналізу анкет, заповнених експертами з ІБ, було створено шаблон функціональної моделі ШІС, представлений на рис. 3.1.

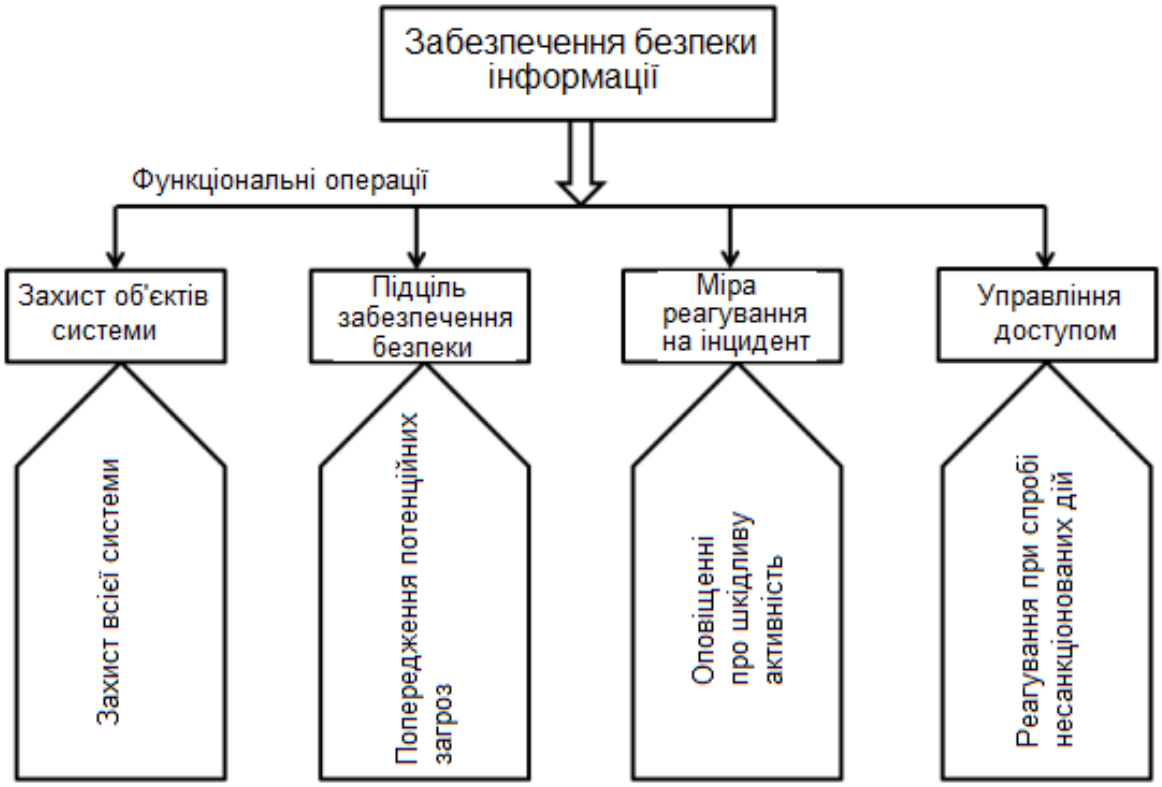

Рисунок 3.1 – Функціональна модель імунологічної СЗІ

Залежно від типу деструктивного впливу, його спрямованості та наслідків для системи підбираються та формуються групи прийняття рішень певного типу, які є найефективнішими саме для цієї конкретної ситуації. Було виділено такі загальні принципи функціонування ШІС:

– здатність реєструвати, виявляти та визначати місце деструктивного впливу на елемент структури системи;

– проводити оцінку серйозності дестабілізуючих впливів на ранніх стадіях реалізації;

– ідентифікувати тип деструктивного впливу на основі оперативного аналізу та приймати рішення в умовах не повної визначеності наявної інформації та за необхідності генерувати сигналу тривоги;

– виробляти захисні механізми, специфічні до відповідного деструктивного впливу;

– запускати процес відновлення (регенерації) ушкоджених елементів.

3.2 Модель принципу дії

За підсумками методу індукції (дослідження, узагальнення результатів) першого розділу цієї роботи було створено модель принципу дії імунологічної системи.

Можна виділити такі етапи функціонування імунологічних систем:

– детектори ідентифікують будь-яку аномальну активність;

– ідентифікатори розпізнають аномальну активність як певний тип порушення, за умови перебування у основі знань відповідної сигнатури або детектування відхилення стосовно стандарту поведінки;

– формуються тестові набори механізмів захисту відповідно до алгоритму, котрий генерує база знань;

– перевірка ефективності тестового набору механізмів захисту;

– ухвалення рішення щодо вибору такого набору;

– подання підсистемою опрацювання сигналу модулю реагування щодо реагування на порушення при допомозі набору механізмів захисту;

– автономія та оцінка підсистемою зворотного зв'язку та детекторами ефективності застосування такого набору поповнення бази знань новою інформацією, розслідування та аналіз порушення, подання сигналу щодо попереджувальних дій.

Адаптивний самонавчальний ЗЗІ, заснований на принципах ШІС, починає свою роботу з генерації детекторів, щоб відповідність детекторів і відомостей про правильну роботу не перевищувала вхідного значення, що задається. Фрагмент алгоритм генерації детекторів показаний на рис. 3.2.

Рисунок 3.2 – Послідовність дій процесу генерації детекторів

У режимі функціонування засіб збирає дані про автоматизовану систему та перевіряє їх на відповідність згенерованим раніше детекторам.

Алгоритм функціонування адаптивного ЗЗІ, що самонавчається, представлений на рис. 3.3.

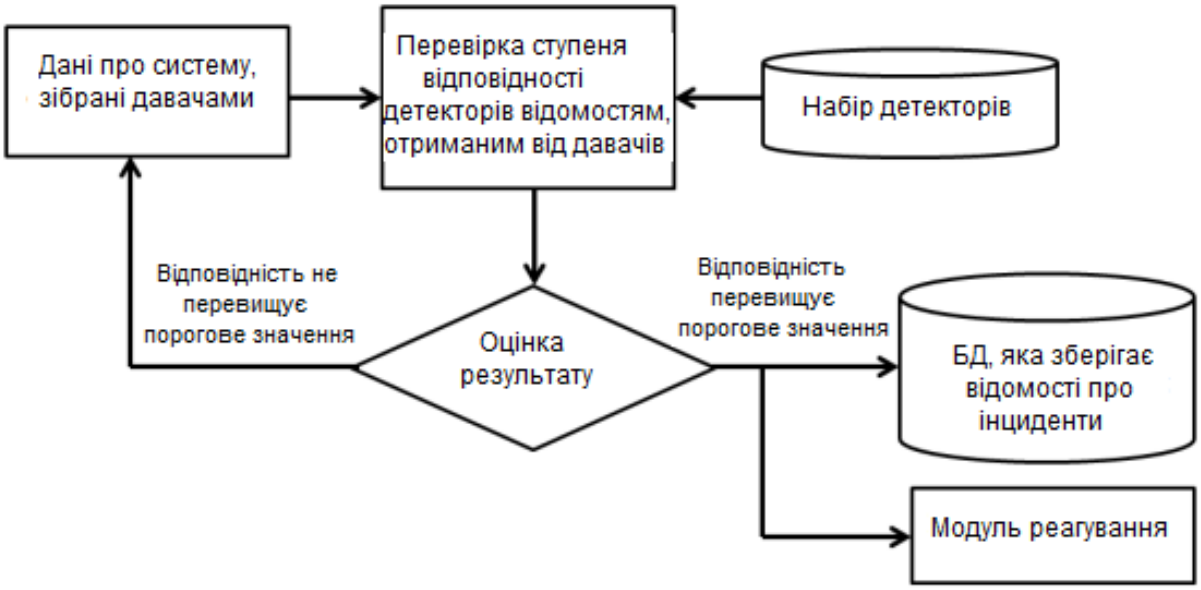

Рисунок 3.3 – Алгоритм функціонування ЗЗІ

Якщо один із детекторів відповідає отриманим даним, ці дані заносяться до журналу обліку інцидентів ІБ та передаються в модуль реагування.

Модуль виявлення загроз ґрунтується на АНВ чи його модифікаціях.

Крок 1. Визначається поняття «своє» як сукупність рядків А довжини Р над кінцевим алфавітом, яку і необхідно захищати. Під сукупністю А розуміється інформація, що є програмою, файлом даних, ПЗ.

Крок 2. Створюється набір детекторів D, кожен з яких не повинен відповідати будь-якому рядку з А, два рядки відповідають один одному, тоді і тільки тоді, коли вони збігаються принаймні в наступних один за одним позиціях, де r - цілочисельний параметр.

Крок 3. Відбувається перевірка на наявність модифікацій шляхом безперервного порівняння детекторів D з елементами сукупності А. Якщо який-небудь детектор збігається, це означатиме, що відбулася модифікація, так як

детектори відібрані таким чином, щоб не відповідати рядкам А.

Описаний вище АНВ спирається такі принципи:

– кожен варіант алгоритму унікальний;

– процес виявлення модифікацій має імовірнісний характер;

– надійна СЗІ має вміти виявляти як відомі варіанти модифікацій, а й будь-яку аномальну активність.

3.3 Структурна модель

Початком будь-якої системи є її структура, яка дає можливість розпізнати взаємозв'язки між елементами системи та підсистемами. Структурна модель будується тільки після створення функціональної моделі та моделі принципу дії, оскільки спочатку необхідно проаналізувати, які саме елементи системи виконуватимуть вибрані функціональні операції.

Структура адаптивного ЗЗІ, що самонавчається, створеного на основі принципів роботи ШІС повинна мати такі елементи:

– давачі, які збирають інформацію про стан системи;

– модуль виявлення загроз, який за допомогою апарату ШІС визначає, чи є події, отримані від давачів, інцидентами ІБ;

– модуль зберігання даних, який містить відомості про інциденти ІБ, журнал обліку інцидентів, інформацію про параметри алгоритму функціонування;

– модуль реагування, який здійснює дію системи у разі виявлення порушення ІБ.

Реагування на порушення визначається політикою безпеки та залежить від ступеня можливої шкоди. Це може бути сповіщення про інцидент, блокування частини функцій системи, припинення роботи системи та інші дії, а також їхня сукупність.

Структура імунологічної системи наведена на рис. 3.4.

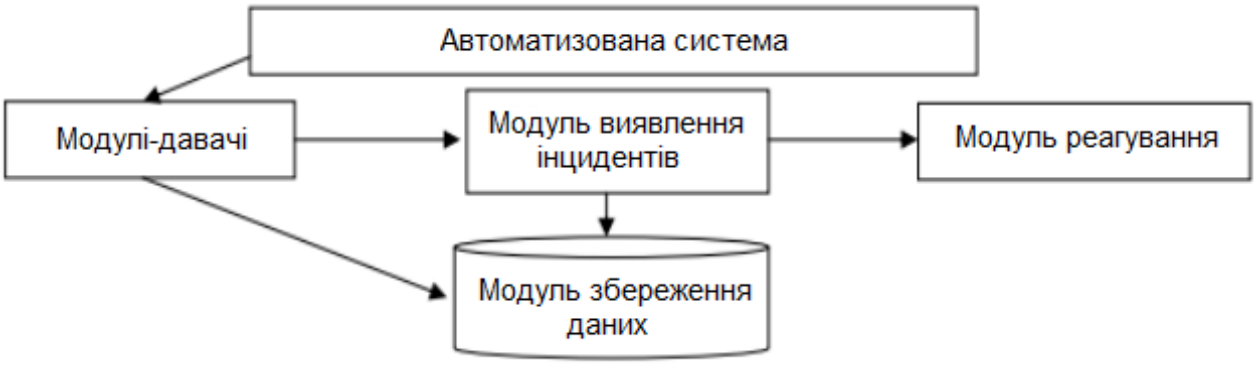

Рисунок 3.4 – Структура модель ШІС

3.4 Висновки до третього розділу

У цьому розділі було побудовано комплекс моделей імунологічних систем, що включає: функціональну, принципу дії та структурну.

Запропоновано провести анкетування експертів з ІБ для визначення основних функціональних операцій за коефіцієнтом їх значимості (від максимального до мінімального). Наведено алгоритми процесу генерації детекторів та роботи ЗЗІ, описано основні компоненти структури ШІС.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою кваліфікаційної роботи магістра є дослідження можливостей створення ШІС в ІБ та способи детектування порушень. Оскільки, проведення робіт з розробки та використання алгоритму передбачає застосування комп'ютерної техніки, зокрема ПК та периферійних пристроїв, то обов'язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників з розробки ПЗ комп'ютерних систем, в тому числі і фахівців зі створення ШІС в ІБ та способи детектування порушень, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці [30]. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Згідно Вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до цих вимог;

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

– Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від 28.10.98 N 247 (далі - ДБН В.2.5-56:2014, з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, ДБН В.2.5-56:2010, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп'ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п'ять комп'ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп'ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при відключенні має бути зворотним. Не допускається підключати комп'ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп'ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При підвищенні ефективності контролю доступу в приміщення, де для забезпечення безпеки мешканців, співробітників і збереження майна використовуються ДС, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-7.15-18.

Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів на основі ГА повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги». Відстань від екрана до ока фахівців, які працюють за комп'ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп'ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп'ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи фахівців з дослідження можливостей створення ШІС в ІБ та способи детектування порушень.

4.2. Комп'ютерне забезпечення процесу оцінки радіаційної та хімічної обстановки

Екологічне співтовариство розробило сімейство інструментів комплексної екологічної оцінки. Програмне забезпечення і послуги (ESS), комерційна група IIASA, включаючи AirWare (для повітряних проблеми якості), WaterWare (для якості води), CityWare (якість повітря і води в контексті великих міст) і EIAxpert (для надання допомоги із загальним впливом на навколишнє середовище). Функціональність в цілому схожа на RAISON, хоча з великим акцентом на моделювання і меншим акцентом на керування даними. Знову ж таки, інструменти ESS розроблені як модульні набори інструментів (доступні спеціальні системи для вирішення конкретних завдань). Компоненти включають стандартні імітаційні моделі, включаючи моделі ISC і PBM Агентства з охорони навколишнього середовища США, управління даними, в тому числі ГІС, аналіз даних (наприклад, аналіз часових рядів даних спостережень), візуалізація, а також оптимізація [31].

Іноді немає готових моделей, придатних для конкретного застосування, але тягар розробки нової програми на Фортрані або C / C ++ є надмірним. Розробка моделі оточення може відносно легко реалізувати власні моделі комп'ютерів і не турбуватися про включення процедур для вирішення рівнянь, візуалізації і т. д. Як правило, за допомогою цих інструментів користувач просто повинен вказати свою модель, використовуючи або математичні рівняння, або спеціальні графічні символи або значки, які безпосередньо представляють поведінку системи.

На даний момент є розроблені моделі комп'ютерного забезпечення процесу для оцінки радіаційної та хімічної обстановки.

GEMS – це система на основі моделей, яка підтримує оцінки схильності і

ризику, надаючи доступ до одиночних і мультимедійних моделям експозиції, фізико-хімічні властивості методи оцінки, статистичний аналіз, графічні та картографічні програми з відповідними даними на навколишнє середовище, джерела, рецептори і популяції. У розробці з 1981 року, GEMS надає аналітикам 84 84 інтерактивний, легко досліджуваний інтерфейс для різних моделей, програм і даних, які необхідні для оцінки хімічного впливу і ризику [31].

HSPF – це комплексний пакет для моделювання кількості і якості стоків з багатоцільових водозборів і процесів радіації, що відбуваються в потоках або повністю змішаних озерах. Це дозволяє інтегроване моделювання землі і грунту, процесів забруднення при гідравлічній і осадово-хімічній взаємодії. Результатом моделювання є тимчасові дані витрати стоку, концентрація поживних речовин і пестицидів, а також дані кількості і якості води в будь-якій точці водозбору. Алгоритми якості води включають динаміку BOD / DO, вуглець, азот і фосфор. Процеси трансформації, які включені в модель це: гідроліз, фотоліз, окислення, випаровування, сорбція і биодеградація. Вторинні або «дочірні» хімічні речовини також моделюються.

Вимоги до даних для моделі можуть бути досить широкими в залежності від конкретного застосування.

Модель MMSOILS – це методологія оцінки впливу на людину і ризику для здоров'я, пов'язаних з викидами забруднень з небезпечних відходів. Мультимедійна модель, що стосується перенесення хімічної речовини в ґрунтові води, поверхневі води, атмосферу і накопичення в їжі. Шляхи впливу на людину, які розглянуті в методології включають: потрапляння в грунт, вдихання летких речовин в повітря і тверді частинки, шкірний контакт, прийом питної води і т.д. Ризик, пов'язаний із загальною дозою опромінення, розраховується на основі хімічної токсичності [31].

4.3. Висновки до розділу

В цьому розділі проаналізовано важливі питання охорони праці та безпеки

в надзвичайних ситуаціях, висвітлено питання комп’ютерного забезпечення процесу оцінки радіаційної та хімічної обстановки.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи магістра проаналізовано теоретичне підґрунтя досліджень ШІС в ІБ, проведено огляд перспектив побудови моделей ШІС, наведено специфіку виявлення порушень (вторгнень) ІБ та формування способів впливів на них.

В результаті виконання кваліфікаційної роботи було досліджено:

– необхідні умови та допустимість побудови моделей імунних систем в ІБ;

– керування стосунками захищеної системи із навколишнім середовищем;

– способи детектування відхиленням від правил ІБ та призначення норм реагування на них;

– стан та тенденції розвитку ІП в ІБ;

– головні сфери застосування ІП.

Також було проаналізовано використання принципів роботи механізмів імунної системи у завданнях створення ЗЗІ.

За результатами виконання практичної складової роботи було створено моделі ШІС:

– функціональну;

– принципу дії;

– структурну.

Таким чином, завдання на дипломне проектування виконане повністю.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Грицик В.В., Литвиненко В.І., Цмоць І.Г., Стех С.М. Теоретичні і прикладні проблеми застосування штучних імунних систем // Інформаційні технології і системи. – 2003 – Т. 6. – № 1-2. – С. 7-45.

2 Литвиненко В.І. Побудова штучних імунних систем // Наукові праці. Комп'ютерні технології . – 2010. – Вип. 121. – Т.134. – С. 166 – 178.

3 Литвиненко В.І. Вирішення задач класифікації з використанням механізмів ідеопатичної мережі // Наукові праці: науково-методичний журнал. Т. 57. Вип. 44. Компютерні технології. – Миколаїв: Вид-во МДГУ ім. Петра Могили, 2006. – С. 136-146.

4 Гангала О.М. Вимоги та умови до побудови моделей штучних імунних систем в інформаційній безпеці // Інформаційні моделі, системи та технології: Праці XI наук.-техн. конф. (Тернопіль, ТНТУ ім. І. Пулюя, 13-14 грудня 2023 р.) – Тернопіль, 2023. – С. 30.

5 Бідюк П.І., Литвиненко В.І., Фефелов. А.О. Формалізація методів побудови штучних імунних мереж // Наукові НТУУ 2007 р. – С. 29-41.

6 Сучасна імунологія (курс лекцій) / І.А.Іонов, Т.Є.Комісова, О.М. Сукач, О.О. Катеринич. – ПП Петров В.В. , 2017 .– 107 с.

7 Литвиненко В. І. Методи та засоби гібридних штучних імунних систем в задачах інтелектуального аналізу даних. – Дис… докт.техн.н. – Львів, 2010.

8 Корабльов, М. М. Гібридні методи і моделі обробки нечіткої інформації на основі штучних імунних систем: автореф. дис. ... д-ра техн. наук: 05.13.23 Харків, 2012. 38 с.

9 Кухарська Н.П., Полотай О.І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. Information Technology and Security. July-December 2019. Vol. 7. Iss. 2 (13), pp. 126-136.

10 O.Polotai, O.Belej, K.Kolesnyk Application of neural networks in intrusion monitoring system for wireless sensor networks. Conference on computer science and information technologies. CSIT 2020: advances in intelligent systems and computing, vol 1293, Springer, Cham. – pp.1101-1115.

11 Dudek G. Artificial immune system for classification with local feature selection, IEEE Trans. on Evolutionary Computation, vol. 16, issue 6, pp. 847- 860, 2012.

12 Forrest S. and S. A. Hofmeyr. Engineering an immune system. Graft, Vol. 4:5, P. 5-9, 2001.

13 Forrest S. and S. A. Hofmeyr. Immunology as information processing. In Design Principles for the Immune System and Other Distributed Autonomous Systems, edited by L. A. Segel and I. Cohen. Santa Fe Institute Studies in the Sciences of Complexity. New York: Oxford University Press, 2000.

14 Dasgupta D. and F. A. Gonzalez. An Immunogenetic Approach to Intrusion Detection, CS Technical Report (No. CS-01-001), The University of Memphis. May, 2001.

15 Dasgupta. Immunity-Based Intrusion Detection Systems: A General Framework In the proceedings of the 22nd National Information Systems Security Conference (NISSC), October 18-21, 1999.

16 Dasgupta D. An Overview of Artificial Immune Systems and Their Applications. Chapter 1 in the book entitled Artificial Immune Systems and Their Applications, Publisher: Springer-Verlag, Inc., pp 3-23, January 1999.

17 Castro De, L.N. & Timmis, J.I. Artificial Immune Systems: A New Computational Intelligence Approach, London: Springer-Verlag 2000), September, – 357 p.

18 De Castro Leandro N. Artifical Immune Systems: New Computational Intelligence Approach. – Springer, 2002. – P.57 – 58.

19 Timmis J., Knight T., de Castro L. N. Hart E. An Overview of Artificial Immune Systems, Computation in Cells and Tissues, R. Paton, H. Bolouri, M. Holcombe, J. H. Parish, и R. Tateson, Ред. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 51–91.

20 Read M., Andrews P. S., Timmis J. An Introduction to Artificial Immune Systems, Handbook of Natural Computing, G. Rozenberg, T. Bäck, и J. N. Kok, Ред. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 1575– 1597.

21 Chelly Z. and Elouedi Z. A survey of the dendritic cell algorithm, Knowl Inf

Syst, vol. 48, issue. 3, pp. 505–535, sept. 2016.

22 Malim M. R., Halim F. A. IMMUNOLOGY AND ARTIFICIAL IMMUNE SYSTEMS, Int. J. Artif. Intell. Tools, t. 21, ed. 06, p. 1250031, dec. 2012.

23 Cohen I. R. Real and artificial immune systems: computing the state of the body, Nat Rev Immunol, vol. 7, issue. 7, pp. 569–574, jul. 2007.

24 McEwan C., Hart E. Representation in the (artificial) immune system, J. Math. Model. Algorithms, vol. 8(2), pp. 125-149, 2009.

25 Mendao M., Timmis J., Andrews P.S., M. Davies The immune system in pieces: Computational lessons from degeneracy in the immune system, in Proc. Foundations of Computational Intelligence (FOCI 2007), 2007, pp. 394-400.

26 Katsikis, Peter D., Stephen P. Schoenberger, and Bali Pulendran, eds. Crossroads between Innate and Adaptive Immunity. Boston, MA: Springer US, 2007.

27 Ямпольський, Л. С. Нейротехнології та нейрокомп’ютерні системи / Л. С. Ямпольський, О. І. Лісовиченко, В. В. Олійник; НТУУ «КПІ». – Київ : Дорадо-друк, 2016. – 631 с.

28 Korablev N. M., Ivaschenko G. S. Parallel immune algorithm of short-term forecasting based on model of clonal selection, Radio Electronics, Computer Science, Control, vol. 0, issue. 2, nov. 2014.

29 Development of methods for adaptive protection and computer security based on the theory of artificial immune systems / A. V. Skatkov, A. A. Bruhoveckiy, V. S. Loviahin // Радіоелектронні і комп’ютерні системи. - 2012. - № 5. - С. 62–66.

30 Толок А.О. Крюковська О.А. Безпека життєдіяльності: Навч. посібник. 2011. 215 с.

31 Зеркалов Д.В. Охорона праці в галузі: Загальні вимоги. Навчальний посібник. К.: Основа. 2011. 551 с.

ДОДАТКИ

Додаток А
Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

УДК 519.71
О.М. Ганжа
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ВИМОГИ ТА УМОВИ ДО ПОБУДОВИ МОДЕЛЕЙ ШТУЧНИХ ІМУННИХ СИСТЕМ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

O.M.Hanhala

REQUIREMENTS AND CONDITIONS FOR THE CONSTRUCTION OF ARTIFICIAL IMMUNE SYSTEM MODELS IN INFORMATION SECURITY

Основне питання у забезпеченні інформаційної безпеки (ІБ) – це створення системи захисті інформації (СЗІ), при якій головною проблемою є безперервна поява нових, раніше незвіданих загроз. Тому для ефективної роботи СЗІ повинна вміти навчатися і сама здійснювати заходи боротьби та захисту. Така СЗІ повинна саморозвиватися, вона могла б самостійно реагувати на загрози ІБ. Також СЗІ повинна бути адаптивною системою, що зберігає працездатність за будь-яких змін внутрішнього чи зовнішнього середовища. Принцип роботи таких систем полягає в застосування імунної системи людини, котра забезпечує захист організму від різноманітних загроз і є складною адаптивною системою. Головним завданням імунної системи є принцип поділу на «своїх» та «чужих».

При виявленні чужорідних клітин активуються захисні механізми людини. Надалі відбувається розпізнавання цієї загрози, після чого формується пам'ять до неї, щоб надалі при зустрічі такої ж загрози негайно протидіяти їй. Принципи штучних імунних систем (ШІС) активно використовуються при вирішенні завдань, пов'язаних з ІБ, наприклад:

- виявлення комп'ютерних вірусів;
- організація парольного захисту;
- моніторинг процесів у системі UNIX та ін.

ШІС необхідна для автоматизації процесу реагування системи на зовнішні та внутрішні порушення функціонування.

У сфері ІБ ШІС можуть вирішувати такі завдання:

- протидія розповсюдженню шкідливої активності;
- виявлення неавторизованого використання інформаційних ресурсів;
- виявлення порушень у інформаційних системах (ІС);
- виявлення аномалій в інформаційних процесах;
- збереження цілісності інформації;
- управління інцидентами ІБ та ін.

Більшість із перелічених вище завдань зводиться до проблеми знаходження відмінностей «свого» від потенційно небезпечного «чужого».

Імунологічний підхід дозволяє системам навчатися під час їх роботи, самостійно виявляти порушення та продукувати способи боротьби з ними. Внаслідок здатності до навчання під час функціонування, ШІС відносяться до систем штучного інтелекту, які знаходять все більше застосування в СЗІ. До найбільш розвинених інформаційних технологій, придатних для вирішення завдань ІБ, можна віднести штучні нейромережі (ШНМ) та генетичні алгоритми(ГА), а до найбільш перспективних - ШІС та імунокомп'ютинг.

Режим функціонування ШІС – безперервний системний процес перевірки ІС на відповідність декларованим цілям політики безпеки, організації обробки даних, норм експлуатації засобів обчислювальної техніки, а також автоматичного реагування на виявлені відхилення. Виділяючи імунологічні системи, можна сказати, що їхня суттєва перевага над ГА та ШНМ - це здатність до навчання та наявність пам'яті.