ЛЕКЦІЯ 3
з навчальної дисципліни
«ШТУЧНИЙ ІНТЕЛЕКТ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ»
Тема: Методи нечіткої логіки в задачах кібербезпеки

Питання лекції

Вступ
1. Теорія нечітких множин
2. Методи побудови функцій приналежності нечітких множин
3. Нечіткі оператори
4. Логіка роботи нечіткої системи
5. Практичне застосування нечіткої логіки в задачах кібербезпеки
Висновки

ВСТУП

Найбільш вражаючою властивістю людського інтелекту є здатність приймати правильні рішення в умовах неповної і нечіткої інформації. Побудова моделей, які відтворюють мислення людини і використання їх у комп'ютерних системах на сьогодні є однією з найважливіших проблем науки.

Основи нечіткої логіки було закладено наприкінці 60-х років у працях відомого американського математика Латфі Заде. Дослідження подібного роду було викликано зростаючим незадоволенням експертними системами. «Штучний інтелект», що легко справлявся із задачами керування складними технічними комплексами, був безпорадним в простих життєвих ситуаціях, типу "Якщо машиною перед тобою керує недосвідчений водій - тримайся від неї подалі".

Для створення дійсно інтелектуальних систем, здатних адекватно взаємодіяти з людиною, був потрібен новий математичний апарат, який перекладає і неоднозначні життєві твердження на мову чітких математичних формул.

Першим серйозним кроком в цьому напрямку була теорія нечітких множин, розроблена доктором Лотфі Заде. Його робота "Fuzzy Sets" з'явилася в 1965 році в журналі "Information and Control". Вона заклала основи моделювання інтелектуальної діяльності людини і стала поштовхом до розвитку нової області науки -"fuzzy logic" (fuzzy - нечіткий, розмитий, м'який).

Хоча тоді його стаття не отримала підтримки з боку деяких кіл академічної спільноти, подальші роботи професора Л.Заде і його послідовників заклали міцний фундамент нової теорії і створили передумови для впровадження методів нечіткого управління в інженерну практику. Сьогодні методи нечіткої логіки стали одним з інструментів, що використовують інженери при проектуванні вимірювально-контрольних систем.

Доктор Лотфі Заде, народився в 1921 році, вважається батьком-засновником використання нечіткої логіки. Закінчивши в 1942 році Тегеранський університет і отримавши ступінь з електротехніки, він виїхав до США, де навчався в Массачусетському технологічному інституті (1946) і в Колумбійському університеті (1949), де пізніше викладав теорію систем.

Існує легенда про те, яким чином була створена теорія "нечітких множин". Один раз Заде мав довгу дискусію зі своїм другом відносно того, чия з дружин є

більш привабливою. Термін "приваблива" є невизначеним і в результаті дискусії вони не змогли прийти до єдиної думки. Це змусило Заде сформулювати концепцію, яка здатна представити нечітке поняття типу "приваблива" в числовій формі.

Чіткі рішення нечіткої логіки

Епіменід Кноський з острова Крит - напівміфічний поет і філософ, який жив у VI ст. до н.е., одного разу заявив: «Все критяни - брехуни!». Оскільки він і сам був критянином, то його пам'ятають як винахідника так званого критського парадоксу.

У термінах аристотелевой логіки, в якій твердження не може бути одночасно істинним і хибним, і подібні самозаперечення не мають сенсу. Якщо вони істинні, то вони помилкові, але якщо вони помилкові, то вони істинні.

В нечіткій логіці змінні можуть бути частковими членами множин. Істинність або хибність перестають бути абсолютними - твердження можуть бути частково істинними і частково помилковими. Використання подібного підходу дозволяє строго математично довести, що парадокс Епіменіда рівно на 50% правдивий і на 50% хибний.

Нечітка логіка в самій своїй основі несумісна з аристотелевой логікою, особливо щодо закону Tertium non datur («Третього не дано» - лат.), який звучить так: якщо твердження не є істинним, то воно є хибним.

1. Теорія нечітких множин

Наочним прикладом нечіткої логіки можна навести відповіді людей на питання: «Чи холодно вам зараз?». В більшості випадків люди розуміють, що мова не йде про абсолютну температурі за шкалою Цельсія, а про особисте сприйняття температури. Для багатьох людей +15°С буде цілком теплою, для інших така температура буде трактуватися як прохолодна.

На відміну від людей, машини не здатні проводити таку тонку градацію. Якщо стандартом визначення холоду буде «температура нижче +15° С», то +14,99° С буде розцінюватися як холод, а +15° С - не буде.

Базові концепції нечіткої логіки є доволі простими. На рис. 1. представлено графік, що допомагає зрозуміти те, як людина сприймає температуру. Температуру в +10° С людина сприймає як холод, а температуру в +30° С - як спеку. Температура в +15° С одним здається низькою, іншим - достатньо комфортною. Назвемо цю групу визначень функцією приналежності до множин, які описують суб'єктивне сприйняття температури людиною.

Аналогічно можна створити додаткові множини, що описують сприйняття температури людиною. Наприклад, можна додати такі множини, як «дуже холодно» і «дуже жарко». Можна описати подібні функції для інших концепцій, наприклад, для станів «відкрито» і «закрито», температури в охолоджувачі або температури в теплиці.

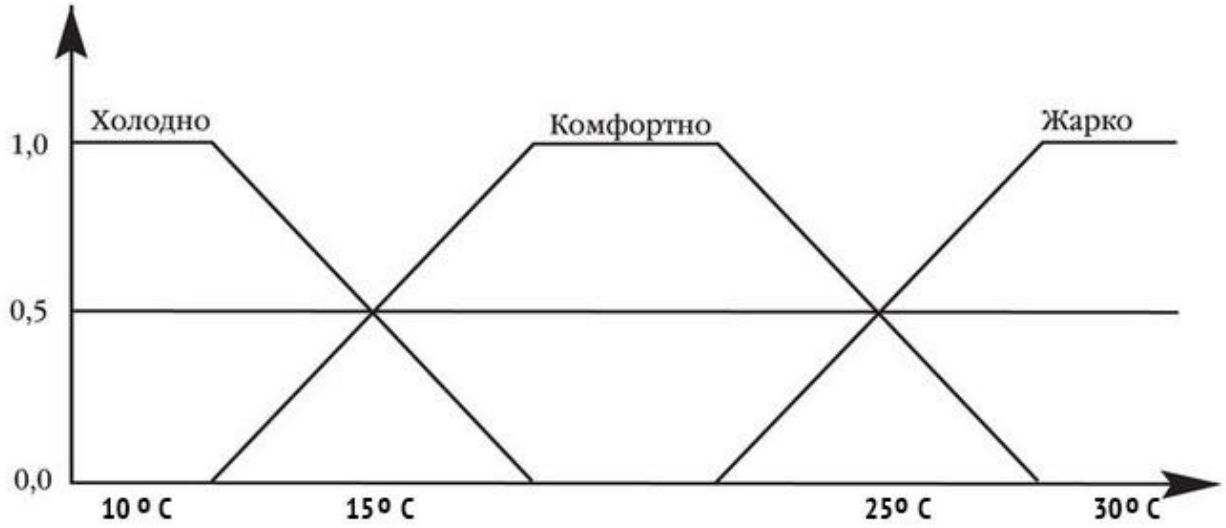


Рис.1. Нечітке визначення температури

Тобто, нечіткі системи можна використовувати як універсальний апроксиматор (усереднювач) дуже широкого класу лінійних і нелінійних систем. Це не лише робить більш надійними стратегії контролю в нелінійних випадках, але і дозволяє використовувати оцінки фахівців-експертів для побудови схем комп'ютерної логіки.

Нечіткі множини

Нехай E - універсальна множина, x - елемент E, а R - певна властивість. Звичайна (чітка) підмножина A універсальної множини E, елементи якої задовольняють властивості R, визначається як множина впорядкованої пари A = {mA (x)/x}, де mA(x) - характеристична функція, що приймає значення 1, якщо x задовольняє властивості R, і 0 - в іншому випадку.

Нечітка підмножина відрізняється від звичайної тим, що для елементів x з E немає однозначної відповіді "ні" відносно властивості R. У зв'язку з цим, нечітка підмножина A універсальної множини E визначається як множина впорядкованої пари A = {mA(x)/x}, де mA(x) - характеристична функція приналежності (або просто функція приналежності), що приймає значення в деякій впорядкованій множині M (наприклад, M = [0,1]).

Функція приналежності вказує ступінь (або рівень) приналежності елемента x до підмножини A. Множину M називають *множиною приналежностей*. Якщо M = {0,1}, тоді нечітка підмножина A може розглядатися як звичайна або чітка множина.

Розглянемо множину X всіх чисел від 0 до 10. Визначимо підмножину A множини X всіх дійсних чисел від 5 до 8.

A = [5,8]

Покажемо функцію приналежності множини A, ця функція ставить у відповідність число 1 чи 0 кожному елементу в X, у залежності від того, належить даний елемент підмножині A чи ні. Результат представлений на наступному малюнку:

Можна інтерпретувати елементи, яким поставлена у відповідність 1, як елементи, що знаходяться в множині А, а елементи, яким поставлено у відповідність 0, як елементи, що не знаходяться в множині А.

Ця концепція використовується в багатьох областях застосувань. Але можна легко знайти ситуації, в яких даній концепції буде бракувати гнучкості.

Наприклад, опишемо множину молодих людей. Формально можна записати так

B = {множина молодих людей}

Оскільки, вік починається з 0, то нижня межа цієї множини повинна бути нулем. Верхню межу визначити небагато складніше. Спочатку встановимо верхню межу, наприклад 20 років. Таким чином, маємо B як чітко обмежений інтервал, буквально: B=[0,20] . Виникає питання: чому людина в двадцятирічний ювілей - молода, а наступного дня вже не молода? Очевидно, це структурна проблема, і якщо пересунути верхню межу в іншу точку, то можна задати таке ж питання.

Більш природний шлях отримання множини B складається в послабленні строгого поділу на молодих і не молодих.

Зробимо це, виносячи не лише чіткі судження:

Так, він належить до множини молодих людей

Ні, він не належить до множини молодих людей,

але і більш гнучкі формулювання

Так, він належить до досить молодих людей

Ні, він не дуже молодий.

Розглянемо як за допомогою нечіткої множини визначити такий вираз, як він ще молодий.

В першому прикладі ми кодували всі елементи множини за допомогою 0 чи 1. Простим способом узагальнити дану концепцію є введення значення між 0 і 1. Реально можна навіть допустити нескінченне число значень між 0 і 1, в одиничному інтервалі I = [0, 1].

Інтерпретація чисел при співвідношенні всіх елементів множини стає тепер більш складною. Звичайно, знову число 1 ставиться у відповідність до того елемента, що належить множині B, а 0 означає, що елемент точно не належить множині B. Всі інші значення визначають ступінь приналежності до множини B.

Для наочності приведемо характеристичну функцію множини молодих людей, як і в першому прикладі.

Нехай E = {x1, x2, x3, x4, x5 }, M = [0,1]; A - нечітка множина, для якої mA(x1)=0,3; mA(x2)=0; mA(x3)=1; mA(x4)=0,5; mA(x5)=0,9

Тоді A можна представити у виді:

A = {0,3/x1; 0/x2; 1/x3; 0,5/x4; 0,9/x5 } або

A = 0,3/x1 + 0/x2 + 1/x3 + 0,5/x4 + 0,9/x5,

(знак "+" є операцією не додавання, а об'єднання) або

	x1	x2	x3	x4	x5
A =	0,3	0	1	0,5	0,9

2. Методи побудови функцій приналежності нечітких множин

Функції приналежності нерозривно пов'язані із нечіткими множинами. Тип функції приналежності в значному ступені визначає властивості нечіткої системи.

Задавання функцій приналежності можна здійснювати у вигляді списку з явним перерахуванням усіх елементів та відповідних ним значень функції приналежності (наприклад, використовуючи відносні частоти за даними експерименту як значення приналежності), або аналітично у вигляді формул (наприклад, використовуючи типові форми кривих для завдання функцій приналежності з уточненням їхніх параметрів відповідно до даних експерименту).

Існують прямі та непрямі *методи побудови функцій приналежності.*

У приведених вище прикладах використано прямі методи, коли експерт або просто задає для кожного $x \in E$ значення mA(x), або визначає функцію приналежності (MembershipFunction). Як правило, прямі методи завдання функції приналежності використовуються для вимірних понять, таких як швидкість, година, відстань, тиск, температура тощо, тобто коли виділяються полярні значення.

В багатьох задачах для характеристики об'єкта можна виділити набір ознак і для кожного з них визначити полярні значення, що відповідають значенням функції приналежності, 0 чи 1.

Наприклад, в задачі розпізнавання обличчя можна виділити наступні пункти:

		0	1
x1	висота чола	низький	високий
x2	профіль носа	кирпатий	горбатий
x3	довжина носа	короткий	довгий
x4	розріз очей	вузькі	широкі
x5	колір очей	світлі	темні
x6	форма підборіддя	гостра	квадратна
x7	товщина губ	тонкі	товсті
x8	колір обличчя	темний	світлий
x9	обрис обличчя	овальне	квадратне

Для конкретного обличчя А експерт, виходячи з приведеної шкали, задає mA(x) ∈ [0,1], формуючи векторну функцію приналежності { mA(x1), mA(x2),... mA(x9)}.

Непрямі методи визначення значень функції приналежності використовуються у випадках, коли немає вимірних елементарних властивостей, через які визначається нечітка множина. Як правило, це *методи попарних порівнянь.* Якщо значення функцій приналежності відомі, наприклад, $\mu_A(x_i) = w_i$, $i = 1, 2, ..., n$, то попарні порівняння можна подати матрицею відношень $A = \{a_{ij}\}$, де $a_{ij} = w_i/w_j$ (операція розподілу).

На практиці експерт сам формує матрицю А, при цьому передбачається, що діагональні елементи дорівнюють 1, а для елементів, симетричних щодо головної діагоналі, $a_{ij} = 1/a_{ji}$, тобто якщо один елемент оцінюється як в *a* разів більш значущий ніж інший, то цей останній повинний бути в *1/a* разів більш значущим, ніж перший. У загальному випадку задача зводиться до пошуку вектора *w*, що задовольняє рівнянню виду: $Aw = \lambda_{max} w$, де λ_{max} - найбільше власне значення матриці *A*. Оскільки матриця *A* позитивна за побудовою, розв'язок даної задачі існує і є позитивним.

Обмеженням методів попарного порівняння є використання суб'єктивної інформації і деяких допущень при перетворенні її в ступені приналежності нечітких множин.

Оптимізаційні методи побудови функцій приналежності засновані на параметричній ідентифікації нечітких моделей за експериментальними даними «входи - вихід», при якій оптимізують параметри функцій приналежності з метою мінімізації відхилення між експериментальними даними і результатами нечіткого моделювання. Використання оптимізаційного підходу знімає суб'єктивізм побудови функцій приналежності, однак замість цього вимагає навчаючої вибірки та нечіткої моделі «входи - вихід». Недоліком даних методів є те, що функції приналежності однакових за змістом нечітких множин виходять різними в результаті ідентифікації різних залежностей «входи -вихід». Таким чином, функція приналежності стає сильно чуттєвою до навчаючої вибірки та структури нечіткої моделі.

Візуалізувати функції приналежності нечітких множин можна шляхом побудови графіку залежності значення функції приналежності μ від значення елемента нечіткої множини ***x*.**

Виділяють такі основні *типи функцій приналежності:* кусочно-лінійні функції, Z-подібні та S-подібні функції, П--подібні функції.

3. Нечіткі оператори

Щоб застосувати алгебру для роботи з нечіткими значеннями, потрібно визначити оператори, що будуть використовуватися. Зазвичай, в булевій логіці використовується лише обмежений набір операторів, за допомогою яких і проводиться виконання інших операцій: AND (оператор «І»), OR (оператор «АБО»), NOT (оператор «НЕ»).

AND	0	1
0	0	1
1	1	1

OR	0	1
0	0	0
1	0	1

A	0	1
NOT A	1	0

Можна дати багато визначень для операторів, три базових з яких наведено в таблиці.

У булевій логіці значення FALSE («ХИБНІСТЬ») еквівалентно значенню «0», а значення TRUE («ІСТИНА») еквівалентно значенню «1». Аналогічним чином в нечіткій логіці ступінь істинності може змінюватися в діапазоні від 0 до 1, тому значення «Холод» вірно в ступені 0,1, а операція NOT («Холод») дасть значення 0,9.

Операції над нечіткими множинами

Об’єднання

Перетин

Доповнення

Концентрація

Розмивання

4. Логіка роботи нечіткої системи

Вдалим застосуванням теорії нечітких множин є контролери нечіткої логіки. Їх функціонування дещо відрізняється від роботи звичайних контролерів; для опису системи замість диференційних рівнянь використовуються знання експертів. Ці знання можуть бути виражені за допомогою лінгвістичних змінних, які описані нечіткими множинами.

Фазифікація - зіставлення множини значень x з її функцією приналежності M (x), тобто переведення значень x в нечіткий формат (приклад з терміном молодий).

Дефазифікація - процес, зворотний до фазифікації.

Всі системи з нечіткою логікою функціонують за одним принципом: показання вимірювальних приладів фазифікуються (переводяться в нечіткий формат), обробляються, дефазифікуються і у вигляді звичних сигналів подаються на виконавчі пристрої.

Ступінь приналежності - це не ймовірність, так як невідома функція розподілу, немає повторюваності експериментів. Так, якщо взяти з прикладу прогнозу погоди дві взаємовиключні події: буде дощ і не буде і присвоїти їм деякі ранги, то сума цих рангів необов'язково буде дорівнювати 1, але якщо рівність все-таки є, то нечітка множина вважається нормованою. Значення функції приналежності M (x) можуть бути взяті тільки з апріорних знань, інтуїції (досвіду), опитування експертів.

Загальна структура нечіткого мікроконтролера

Загальна структура мікроконтролера, що використовує нечітку логіку, показана на рис. Вона містить у своєму складі наступні складові:

Блок фазіфікації.

База знань.

Блок рішень.

Блок дефазіфікації.

Блок фазіфікації перетворює чіткі величини, які виміряні на виході об'єкта керування у нечіткі величини, що описані лінгвістичними змінними в базі знань.

Блок рішень використовує нечіткі умовні (if - then) правила, що закладено в базу знань, для перетворення нечітких вхідних даних в керуючі впливи, які мають також нечіткий характер.

Блок дефазіфікації перетворює нечіткі дані з виходу блоку рішень в чіткі величини, які використовуються для керування об'єктом.

Рис. 1. Загальна структура нечіткого мікроконтролера

Розглянемо випадок керування мобільним роботом, задачею якого є об'їзд перешкод. Введемо дві лінгвістичні змінні: ДИСТАНЦІЯ (відстань від робота до перешкоди) і НАПРЯМОК (кут між подовжньою віссю робота та напрямком до перешкоди).

Розглянемо лінгвістичну змінну ДИСТАНЦІЯ. Значеннями її можна визначити терми ДАЛЕКО, СЕРЕДНЬО, БЛИЗЬКО і ДУЖЕ БЛИЗЬКО. Для фізичної реалізації лінгвістичної змінної необхідно визначити точні фізичні значення термів цієї змінної. Нехай змінна ДИСТАНЦІЯ може приймати будь-які значення з діапазону від нуля до нескінченності. Відповідно до теорії нечітких множин, в такому випадку кожному значенню відстані із зазначеного діапазону може бути поставлене у відповідність деяке число від нуля до одиниці, що визначає ступінь приналежності даної фізичної відстані (припустимо 40 см) до того чи іншого терму лінгвістичної змінної ДИСТАНЦІЯ.

Ступінь приналежності визначаємо функцією приналежності M(d), де d-відстань до перешкоди. В нашому випадку відстань 40 см. Можна задати ступінь приналежності до терму ДУЖЕ БЛИЗЬКО, що дорівнює 0,7 , а до терму БЛИЗЬКО - 0,3 (рис. 2.). Конкретне визначення ступеня приналежності визначається експертами.

Рис. 2. Лінгвістична змінна і функція приналежності

Змінній НАПРЯМОК, яка може приймати значення в діапазоні від 0 до 360 градусів, задамо терми ВЛІВО, ПРЯМО і ВПРАВО.

Тепер необхідно задати вихідні змінні. У даному прикладі достатньо однієї, яку назвемо КУТ ПОВОРОТУ. Вона може містити терми: РІЗКО ВЛІВО, ВЛІВО,

ПРЯМО, ВПРАВО, РІЗКО ВПРАВО. Зв'язок між входом та виходом запам'ятовується в таблиці нечітких правил.

Таблиця нечітких правил

Кожний запис в даній таблиці відповідає своєму нечіткому правилу, наприклад: Якщо дистанція до перешкоди - «близько» і напрямок «правий», тоді кут повороту «різко вліво».

Таким чином, мобільний робот з нечіткою логікою буде працювати за наступним принципом: дані з сенсорів про відстань до перешкоди та напрямок до неї будуть фазифіковані, оброблені згідно табличних правил, дефазифіковані і отримані дані у вигляді керуючих сигналів надходять на приводи робота.

Переваги нечітких систем

Можливість оперувати вхідними даними, заданими нечітко: наприклад, дані, які неперервно змінюються в часі (динамічні задачі), значення, що неможливо задати однозначно (результати статистичних опитувань, рекламні компанії);

Можливість нечіткої формалізації критеріїв оцінки і порівняння: оперування критеріями "більшість", "можливе", переважно" тощо.;

Можливість проведення якісних оцінок як вхідних даних, так і виведених результатів: значення даних, їх ступень достовірності (не плутати з імовірністю!) та її розподілом;

Можливість проведення швидкого моделювання складних динамічних систем та їх порівняльний аналіз із заданим ступенем точності: оперуючи принципами поведінки системи, описаними fuzzy-методами:

можна швидко з'ясувати точні значення змінних і скласти правила, що їх описують,

можна оцінити різні варіанти вихідних значень.

Поширені помилкові уявлення про нечіткої логіки

Нечітка логіка є неточною: по своїй основі нечітка логіка не більше неточна, ніж стандартна арифметика. Фактично вона набагато більш точна при роботі з неточною інформацією.

В основі нечіткої логіки лежать імовірнісні міркування. Імовірність має справу з шансами виникнення тих чи інших подій, а нечітка логіка - з самими цими подіями. Зазвичай нечітка логіка має справу з двозначністю, а не з невизначеністю.

Нечітка логіка побудована на основі ряду евристичних припущень.

Хоча через інтуїтивність природи нечіткої логіки з першого погляду і може здатися, що лежать в її основі правила вибрані довільно або засновані тільки на здоровому глузді, але насправді було строго доведено, що ці правила є вірними.

5. Практичне застосування нечіткої логіки в задачах кібербезпеки

Коли тільки з'явилася теорія нечіткої логіки, в наукових журналах можна було знайти статті, присвячені її можливим областям застосування. У міру просування розробок в даній області число практичних застосувань для нечіткої логіки почало швидко зростати. В даний час цей перелік був би надто довгим, але ось кілька прикладів, які допоможуть зрозуміти, наскільки широко нечітка логіка використовується в системах управління і в задачах кібербезпеки.

Сьогодні елементи нечіткої логіки можна знайти в багатьох промислових виробах - від систем керування електропоїздами і бойовими вертольотами до побутової техніки. Без застосування нечіткої логіки немислимі сучасні ситуаційні центри керівників західних країн, в яких приймаються ключові політичні рішення і моделюються всілякі кризові ситуації.

Активними споживачами нечіткої логіки є банкіри і фінансисти, а також фахівці в області політичного й економічного аналізу, задачі яких вимагають щоденного прийняття правильних рішень у складних умовах непередбаченого ринку. Вони використовують нечіткі системи для створення моделей різних економічних, політичних, біржових ситуацій.

Слідом за фінансистами, когнітивними нечіткими схемами зацікавилися промислові гіганти США. Motorola, General Electric, Otis Elevator, Pacific Gas & Electric, Ford і інші на початку 90-х почали інвестувати в розробку виробів, що використовують нечітку логіку. Маючи солідну фінансову "підтримку", фірми, що спеціалізуються на нечіткій логіці, отримали можливість адаптувати свої розробки для широкого кола застосувань.

Пристрої для автоматичної підтримки швидкості руху автомобіля і збільшення ефективності / стабільності роботи автомобільних двигунів (компанії Nissan, Subaru).

Системи розпізнавання рукописного тексту в PDA (компанія Sony).

Поліпшення систем безпеки для атомних реакторів (компанії Hitachi, Bernard, Nuclear Fuel Div.).

Управління роботами (компанії Toshiba, Fuji Electric, Omron).

Промислові системи управління (компанії Aptronix, Omron, Meiden, Sha, Micom, Nisshin-Denki, Mitsubishi, Oku-Electronics та ін.).

Нечітка модель та засіб оцінювання ризиків інформаційної безпеки Wi-Fi мереж

Бездротові мережі на сьогоднішній день використовуються практично у всіх сферах діяльності. Широке використання бездротових мереж обумовлено тим, що вони можуть використовуватися не тільки на персональних комп'ютерах, а й в телефонах, планшетах і ноутбуках, їх зручністю і порівняно невисокою вартістю.

В наш час методи впливу на конкурентів переходять від фізичного впливу до інтелектуального. При цьому використовуються новітні способи і засоби несанкціонованого отримання інформації. Саме тому актуальним є необхідність оцінки ризиків інформаційної безпеки для побудови ефективних систем захисту інформації . Існуючі методи оцінки ризиків в більшості своїй засновані на теоріях ймовірності і класичних множин. Ці методи не дозволяють врахувати той факт, що будь-яка складна система є динамічною системою з набором невизначених даних. Системи оцінки ризиків, побудовані на застосуванні нечіткої логіки характеризуються логічністю і високою стійкістю в тому випадку, коли аналіз ризиків здійснюється в умовах нестачі даних і знань. Тому зраз є розроблені моделі нечіткі оцінки рівня захисту інформації та програмні засоби на її основі.

Методика виявлення кібератак типу JS(HTML)/SCRINJECT на основі застосування математичного апарату теорії нечітких множин **[2]**

Тут представлено методику виявлення однієї з найпоширеніших кібератак - JS (HTML)/ScrInject на основі застосування математичного апарату теорії нечітких множин та нечіткого логічного виводу. Розробка методики базується на алгоритмі дій, який включає в себе етапи підготовки вхідних даних, фазифікації значень досліджуваних параметрів та здійснення процедури нечіткого логічного виводу.

ШПЗ JS (HTML)/ScrInject – троянська програма, зазвичай завантажується з веб-сайтів, які пропонують користувачам завантажувати та/або запускати оновлення, наприклад, для таких програмних додатків, як Flash Player або Java Virtual Machine. Після запуску, ШПЗ ScrInject налаштовується на автоматичний старт та за допомогою JavaScript-сценаріїв перенаправляє користувача на небезпечні ресурси, що дозволяє кіберзлочинцям у подальшому здійснювати інформаційно-руйнівні впливи на інфіковану систему.

Послідовність характерних дій даного ШПЗ зводиться до:

спроб звернення до Інтернет-ресурсів із шкідливим вмістом з погодженням користувача або без такого, при чому користувачеві виводиться повідомлення із запитом зовсім іншого контексту;

автоматичного запуску сценаріїв на завантаження іншого ПЗ без згоди користувача;

ініціювання запису ПЗ до автоматичного запуску із завантаженням системи;

помітного для користувача додаткового навантаження на систему (ресурси оперативної пам’яті, завантаження процесора, повільний відклик системи на дії);

ініціювання завантаженими сценаріями досить великої кількості запитів до різноманітних Інтернет-ресурсів (сервісів) під виглядом оновлень.

Оскільки модель даної кібератаки є не параметричною, а поведінковою, то доцільно на етапі її виявлення опиратися саме на шаблон/паттерн поведінки.

Методика виявлення передбачає визначення функцій системи, а також потоків інформації, які пов'язують між собою вказані функції. Відповідно до методології функціонального моделювання IDEF0 [8], на рис. 1 представлено контекстну діаграму рівня А-0, на якій згідно аналізу цілей та функцій СВА визначено вхідні та вихідні дані, управляючі компоненти та механізми (суб'єкти), що впливають на результат. Контекст системи обмежено однією ітерацією процесу визначення належності кібератаки до типу JS (HTML)/ScrInject.

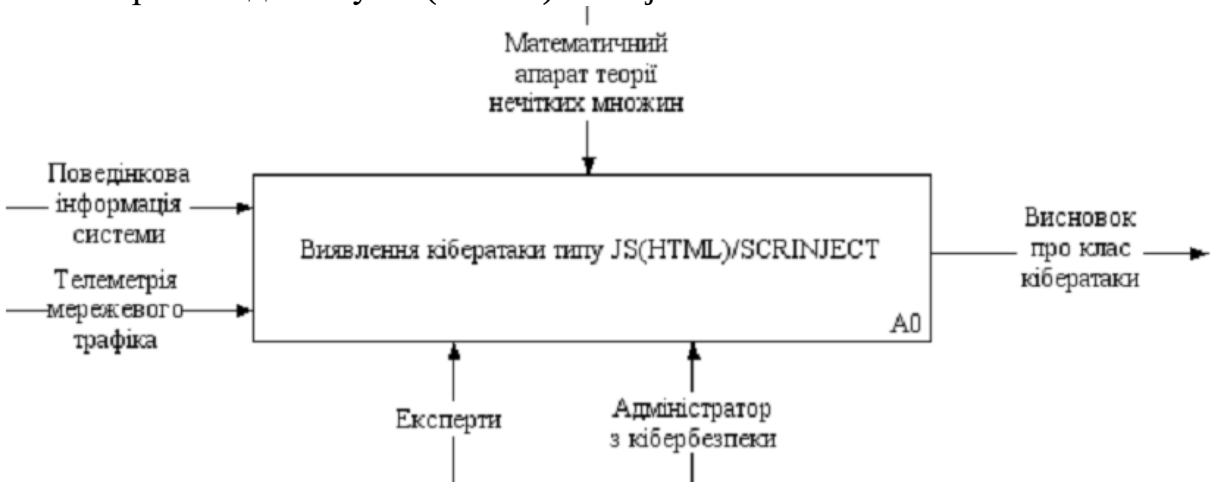


Рис.1. Контекстна А-0 діаграма процесу визначення класу кібератаки

Вхідними даними є поведінкова інформація в інформаційно-телекомунікаційній мережі (ІТМ), на основі аналізу якої приймається рішення щодо виявлення кібератаки та телеметрія мережевого трафіку – статистичні дані для уточнення (адаптації) функцій належності з метою врахування особливостей та умов функціонування системи – об'єкта захисту.

Управляючим компонентом є математичний апарат теорії нечітких множин.

Суб'єкти, за допомогою яких відбувається даний процес: експерти – на етапі налаштування системи виявлення атаки (СВА), зокрема заповнення бази знань (БЗ) правилами та адміністратор з кібербезпеки – особа, якій надаються управлінські рішення системою про стан ІТМ для здійснення подальших превентивних заходів у разі необхідності.

Вихідними даними є перевірена на відповідність описаному шаблону поведінки кібератаки інформація у вигляді логічного висновку, який характеризує поточний стан безпеки ІТМ щодо наявності досліджуваної кібератаки у режимі реального часу RTC (Real-Time Clock).

Отже методика виявлення кібератаки типу JS (HTML)/ScrInject складається з наступних етапів, що визначають порядок дій для своєчасного та достовірного її виявлення, які представлено у вигляді функціональної схеми на рис. 2.

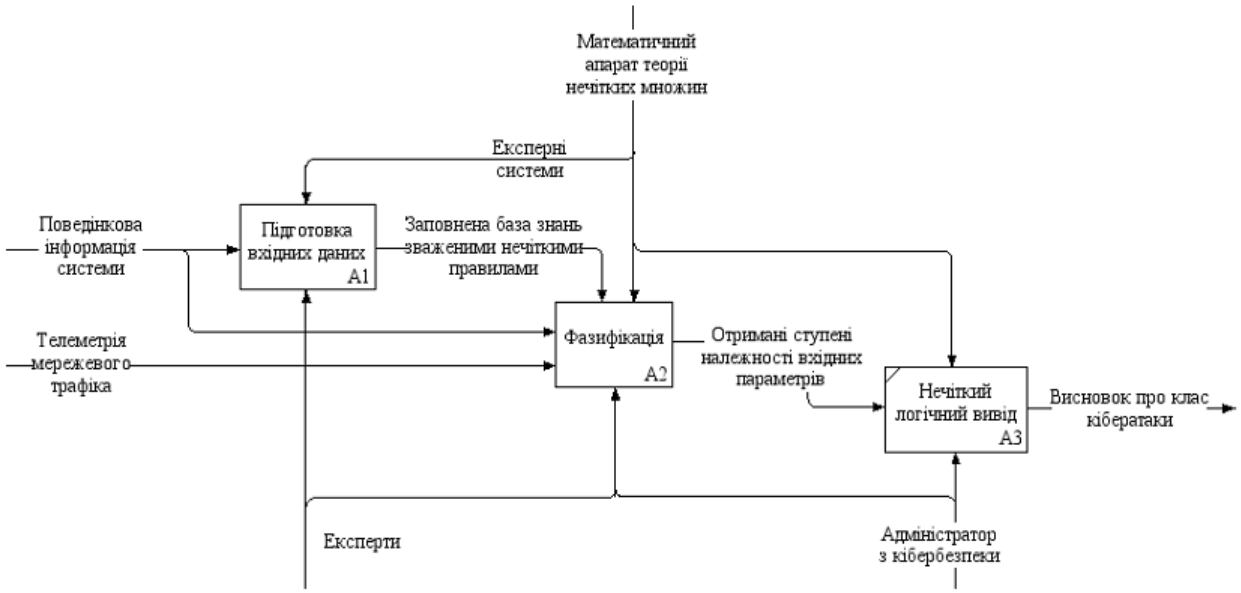
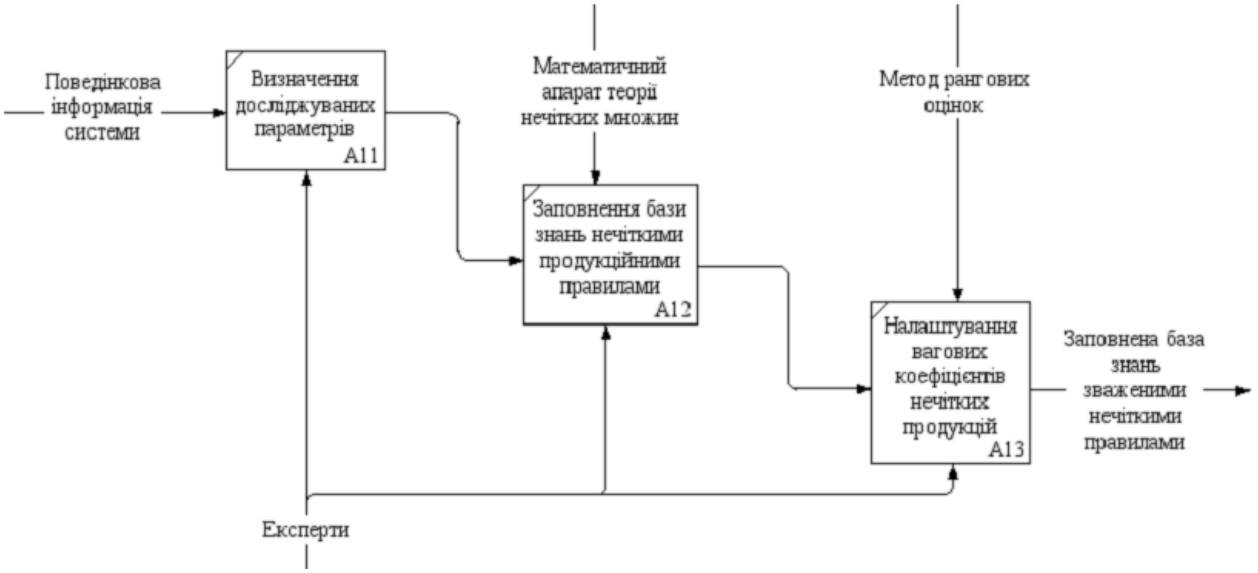


Рис. 2 Функціональна схема процесу визначення класу кібератаки типу JS (HTML)/ScrInject

1 етап – підготовка вхідних даних. Виконання цього етапу характеризуються послідовністю дій, які представлені наступною функціональною діаграмою на рис. 3.



Вхідними даними на даному етапі є поведінкова інформація процесів в ІТМ, яка представлена наступними ***лінгвістичними змінними*** на основі аналізу характерних дій кібератаки JS (HTML)/ScrInject:

GET_NET – звернення до Інтернет-ресурсів із шкідливим вмістом з погодженням користувача або без такого;

AUTOSTART_BOOT – автоматичний запуск сценаріїв на завантаження іншого ПЗ без згоди користувача;

AUTOSTART – ініціювання запису ПЗ до автоматичного запуску із завантаженням операційної системи;

BOOT_LEVEL – рівень завантаженості операційної системи у відсотках;

REQUEST – ініціювання досить великої кількості запитів до різноманітних Інтернет-ресурсів (сервісів) під виглядом оновлень.

Наступним процесом є заповнення БЗ нечіткими правилами, що описують стани поведінки в ІТМ з наступними лінгвістичними термами та відповідними значеннями:

GET_NET, AUTOSTART_BOOT, AUTOSTART, REQUEST – {„Н – низька [до 5]”, „С – середня [5,10,15,20]”, „В – велика [від 20 і вище]”} на універсумі [0,50];

BOOT_LEVEL – {„Н – низький [до 25]”, „нС – нижче середнього [20, 30, 40]”, „С – середній [40, 45, 55, 65]”, „вС – вище середнього [60, 70, 80]”, „В – високий [від 80 і вище]”} на універсумі [0, 100].

На рис. 4 представлено графічне зображення описаних лінгвістичних термів функцій належності.

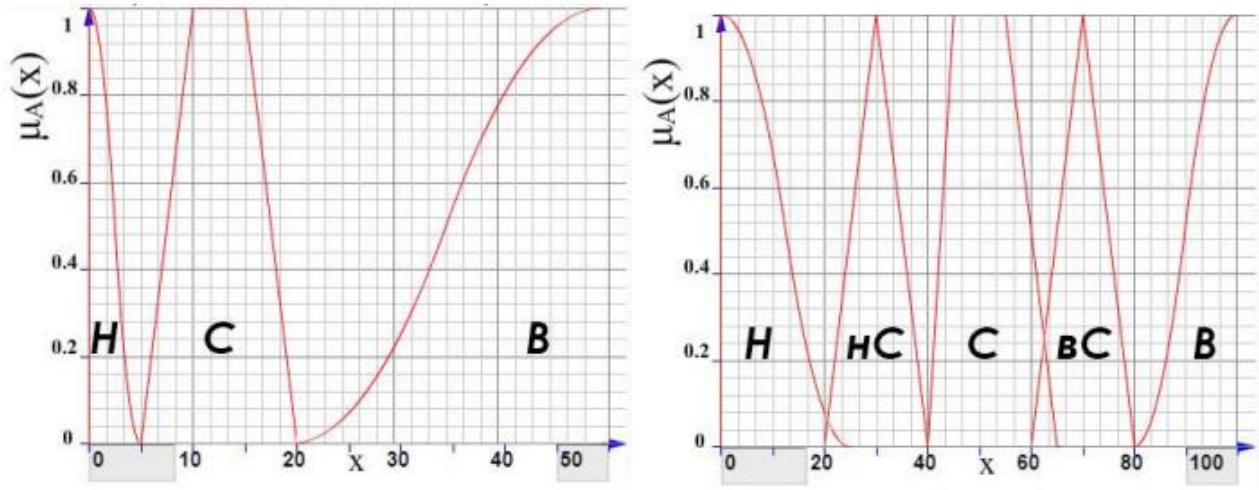


Рис. 4 Графічне зображення описаних лінгвістичних термів функцій належності

У зведеній таблиці 2 представлено правила з БЗ та відповідні їм експертні рішення.

Таблиця 2

Стани ІТМ описані нечіткими зваженими правилами

Вхідні лінгвістичні змінні (ознаки атаки „*back*”)					Ваговий коефіцієнт	Висновок
GET_NET	*AUTOSTART_BOOT*	*AUTOSTART*	*BOOT_LEVEL*	*REQUEST*		*y*
Н	Н	Н	Н	Н	w_1	d_1
Н	Н	Н	В	Н	w_2	d_2
В	С	С	вС	В	w_3	d_3
В	В	В	вС	В	w_4	d_4
В	В	В	В	В	w_5	d_5

Де $d_1 - d_5$ – варіанти експертних рішень щодо станів ІТМ:

$d_1 - d_2$ – нормальний стан ІТМ;

$d_3 - d_5$ – наявність кібератаки в ІТМ класифікованої як JS (HTML)/ScrInject.

Управляючими компонентами є математичний апарат теорії нечітких множин та нечіткого логічного виводу, а також вагові коефіцієнти правил w, отримані на основі застосування методу рангових оцінок з метою ранжування (впорядкування) нечітких правил, визначених експертами з кібербезпеки, що характеризують їх впевненість у кожному прийнятому рішенні [9, 10, 11]. Так, $w_1 - w_5$ - – вагові коефіцієнти нечітких правил у БЗ. Такий підхід дозволяє підвищити ефективність нечіткого логічного виводу, оскільки враховується відносна значущість (перевага) нечітких правил.

Суб'єкти, за допомогою яких відбувається даний процес – експерти з кібербезпеки.

Вихідні дані – заповнена нечітка база зважених правил про стани ІТМ.

2 етап – фазифікація. Виконання даного етапу характеризуються послідовністю дій, які представлені наступною функціональною діаграмою на рис. 5:

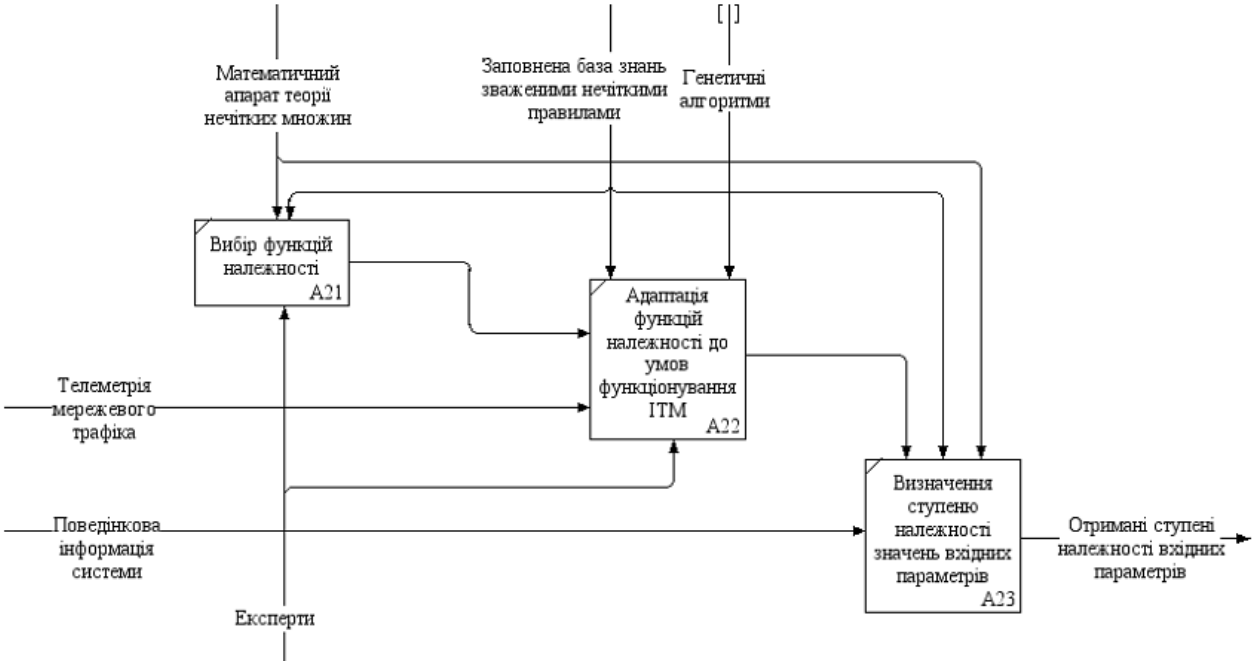


Рис. 5 Функціональна діаграма другого етапу запропонованої методики

На даному етапі запропонованої методики визначається ступінь належності значень досліджуваних параметрів терм-множинам вищевказаних лінгвістичних змінних.

Дослідження ознак даної кібератаки проводилось на основі Z,S – подібного (початок/кінець діапазону значень), трикутного (Δ) та трапецеїдального (Т) (проміжні значення діапазону значень) типу функцій належності з наступними значеннями (1, 2):

GET_NET, AUTOSTART_BOOT, AUTOSTART, REQUEST – {„Н – низька [до 5]", „С – середня [5, 10, 15, 20]", „В – велика [від 20 і вище]"} на універсумі [0, 50];

BOOT_LEVEL – {„Н – низький [до 25]", „нС – нижче середнього [20, 30, 40]", „С – середній [40, 45, 55, 65]", „в С – вище середнього [60, 70, 80]", „В – високий [від 80 і вище]"}

на універсумі [0,100].

З метою забезпечення ефективного виявлення кібератак типу JS (HTML)/ScrInject у різних ІТМ за призначенням, топологією та специфікою доцільно враховувати умови та особливості їх функціонування. Так, налаштовані експертами значення термів функцій належності, від яких багато в чому залежить точність та достовірність отриманого логічного висновку потребують уточнення (адаптації) на основі статистичних даних телеметрії мережевого трафіку. Ця задача може бути вирішена шляхом застосування математичного апарату генетичних алгоритмів, на кожній ітерації якого діапазони терм-множин функцій належності підлягають оцінці функцією відповідності, яка в свою чергу приймає участь у формуванні нової їх популяції [10]. В результаті розвитку такої популяції алгоритм зводиться до вибору оптимальних або субоптимальних значень термів.

Визначення ступеню належності значень досліджуваних параметрів, що описують поведінку процесів у ІТМ здійснюється на основі моделей:

$$\mu_Z(x;a,b)=\begin{cases}1, x\le a\\ \frac{1}{2}+\frac{1}{2}\cos\left(\frac{x-a}{b-a}\pi\right), a\le x\le b\\ 0, x>b\end{cases}\quad \mu_S(x;a,b)=\begin{cases}0, x<a\\ \frac{1}{2}+\frac{1}{2}\cos\left(\frac{x-b}{b-a}\pi\right), a\le x\le b\\ 1, x>b\end{cases} \quad (1)$$

$$\mu_\Delta(x;a,b,c)=\begin{cases}0, x\le a\\ \frac{x-a}{b-a}, a\le x<b\\ \frac{c-x}{c-b}, b\le x\le c\\ 0, c\le x\end{cases}\qquad \mu_T(x;a,b,c,d)=\begin{cases}\frac{x-a}{b-a}, a\le x<b\\ 1, b\le x<c\\ \frac{d-x}{d-c}, c\le x\le d\\ 0, x\notin(a,d)\end{cases} \quad (2)$$

Управляючими компонентами є математичний апарат теорії нечітких множин та нечіткого логічного виводу, БЗ та штучні генетичні алгоритми.

Суб’єкти, за допомогою яких відбувається даний процес – експерти з кібербезпеки та адміністратор, який має змогу приймати участь в налаштуванні СВА у зв’язку з безпосереднім виконанням посадових інструкцій на конкретній ІТМ.

Вихідні дані – розраховані ступені належності значень досліджуваних параметрів щодо стану ІТМ.

3 етап – нечіткий логічний вивід. Виконання даного етапу передбачає проведення розрахунків над отриманими ступенями належності на попередньому етапі для всіх експертних рішень у нечіткій БЗ з метою визначення найбільш відповідного висновку на основі застосування нечітких максимінних операцій. Описаний процес можливо представити у вигляді наступної системи нечітких логічних рівнянь:

$$\mu^{d_j}(x_1,x_2,...,x_n)=\max_{p=\overline{1,k_j}}\left\{w_{jp}\min_{i=\overline{1,n}}\left[\bigwedge_{i=1}^{n}\mu^{jp}(x_i)\right]\right\}, j=\overline{1,m} \quad (3)$$

Так, при отриманні значень у режимі RTC, що відповідають експертним висновкам -адміністратору з кібербезпеки буде виведено рішення про наявність в ІТМ кібератаки, класифікованої як JS (HTML)/ScrInject.

Вхідними даними є ступені належності значень вхідних параметрів терм-множинам обраних функцій належності. Управляючим компонентом є математичний апарат теорії нечітких множин та нечіткого логічного виводу.

Суб'єкти, за допомогою яких відбувається даний процес: адміністратор з кібербезпеки – особа, якій надаються управлінські рішення системою про стан ІТМ для здійснення подальших превентивних заходів у разі необхідності.

Вихідними даними є перевірена на відповідність описаному шаблону поведінки кібератаки інформація у вигляді логічного висновку, який характеризує поточний стан безпеки ІТМ щодо наявності досліджуваної кібератаки у режимі реального часу RTC (Real-Time Clock).

Таким чином, представлено методику виявлення кібератак типу JS (HTML)/ScrInject, яка на відміну від існуючих, забезпечує їх виявлення в умовах режиму реального часу функціонування ІТМ на основі дослідження параметрів, якими характеризується кібератака. Експериментальна перевірка застосування запропонованої методики на практиці дозволяє зробити висновок про підвищення точності та достовірності виявлення розглянутої кібератаки СВА. Практична цінність методики полягає у можливості виявлення кібератак як в умовах невизначеності та нечіткості управляючої інформації, так і з врахуванням умов та особливостей функціонування об'єкта захисту.

ЛІТЕРАТУРА

1. ТЗІ 1.1-003–99. Термінологія в галузі захисту інформації в комп'ютерних системах із несанкціонованого доступу – Київ: ДСТСЗІ СБУ, 1999. – 38 с.

2. Субач І.Ю. Здоренко Ю.М. Фесьоха В.В. МЕТОДИКА ВИЯВЛЕННЯ КІБЕРАТАК ТИПУ JS(HTML)/SCRINJECT НА ОСНОВІ ЗАСТОСУВАННЯ МАТЕМАТИЧНОГО АПАРАТУ ТЕОРІЇ НЕЧІТКИХ МНОЖИН.

Київ. Збірник наукових праць ВІТІ № 4 – 2018, с. 125-131.