УДК 004.056:323.1

д.т.н. Субач І.Ю. (ВІТІ)
к.т.н. Здоренко Ю.М. (ВІТІ)
Фесьоха В.В. (ВІТІ)

МЕТОДИКА ВИЯВЛЕННЯ КІБЕРАТАК ТИПУ JS(HTML)/SCRINJECT НА ОСНОВІ ЗАСТОСУВАННЯ МАТЕМАТИЧНОГО АПАРАТУ ТЕОРІЇ НЕЧІТКИХ МНОЖИН

У статті 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. Визначено напрямки автоматизованого уточнення вагових коефіцієнтів нечітких правил, адаптації функцій належності до умов функціонування об'єкта захисту та подальший напрямок дослідження в аспекті самонавчання системи виявлення атак на основі сучасних методів машинного навчання.

Субач И.Ю., Здоренко Ю.Н., Фесёха В.В. Методика выявления кибератак типа JS (HTML)/ScrInject на основе применения математического аппарата теории нечетких множеств. *В статье представлена методика выявления одной из самых распространенных кибератак - JS (HTML) / ScrInject на основе применения математического аппарата теории нечетких множеств и нечеткого логического вывода. Разработка методики базируется на алгоритме действий, который включает в себя этапы подготовки входных данных, фаззификации значений исследуемых параметров и осуществления процедуры нечеткого логического вывода. Определены направления автоматизированного уточнения весовых коэффициентов нечетких правил, адаптации функций принадлежности к условиям функционирования объекта защиты и дальнейшее направление исследования в аспекте самообучения системы обнаружения атак на основе современных методов машинного обучения.*

I. Subach, Y. Zdorenko, V. Fesokha Method for detecting cyber-attacks of the JS (HTML) / ScrInject type based on the use of the mathematical apparatus of the theory of fuzzy sets. *The article presents a method for identifying one of the most common cyber-attacks - JS (HTML) / ScrInject based on the use of the mathematical apparatus of the theory of fuzzy sets and fuzzy inference. The development of the methodology is based on an algorithm of actions, which includes the steps of preparing input data, fuzzing the values of the studied parameters and implementing a fuzzy inference procedure. The directions of the automated refinement of the weights of fuzzy rules, the adaptation of the membership functions to the conditions of the protected object, and the further direction of research in the aspect of self-learning of the attack detection system based on modern machine learning methods are defined.*

Ключові слова: *інформаційно-телекомунікаційна мережа, кібератака, системи виявлення атак, нечіткі множини.*

Актуальність дослідження. Постійне зростання числа нових способів та методів несанкціонованих втручань руйнівного характеру в інформаційно-телекомунікаційні мережі (ІТМ) та модифікація існуючих їх форм в умовах неконтрольованого поширення та необмеженого використання інформаційного простору є однією з найактуальніших проблем нашого часу.

На практиці, існуючі системи (засоби) захисту не тільки не здатні виявляти такого роду вторгнення, про що свідчать успішні реалізації кібератак типу вірусів-вимагачів, таких як *WannaCry*, *Petya* і *NotPetya* у 2017 році, а й не завжди ефективно запобігати деструктивному впливу дещо змінених, але уже класифікованих кібератак [1].

Так, згідно звітних даних про основні тенденції поширення комп'ютерних загроз за 2018 рік, отриманими фахівцями вірусної лабораторії *ESET* (одного з лідерів в області проактивного виявлення) за допомогою системи швидкого оповіщення *ESET Live Grid*, лідируючі позиції в рейтингу найбільш активних шкідливих програм займає програмне забезпечення (ПЗ), яке перенаправляє жертву на заражені веб-сайти, в тому числі і для прихованого видобутку криптовалюти [2].

Зокрема, найбільш високий рівень поширення (16,96 %) не тільки в Україні, але й у світі продемонструвало шкідливе програмне забезпечення (ШПЗ) *HTML/ScrInject*, яке класифікується як троянський кінь. Дана кібератака за допомогою *JavaScript*-сценаріїв перенаправляла користувачів на ресурси з ШПЗ за допомогою коду, який був вбудований в *HTML*-сторінку *HTTP-Response* (відповідь веб-серверу). Статистику поширення ШПЗ представлено у таблиці 1 [2].

Таблиця 1

Основні тенденції поширення комп'ютерних загроз за 2018 рік

№	Найменування	%
1	*HTML (JS)/ScrInject*	16,96
2	*JS/CoinMiner*	15,49
3	*JS/Adware.Agent.S*	7,44
4	*Win32/Adware.PBot*	5,74
5	*SMB/Exploit.DoublePuisar*	5,1
6	*Win32/CoinMiner*	3,0
7	*Win64/CoinMiner*	2,57
8	*Win32/AdWare.FileTour*	2,04
9	*PowerShell/Adware.Adposhel*	1,97
10	*JS/Adware.Revizer*	1,82

Представлений у таблиці перелік ШПЗ не являється новими розробками кіберзлочинців. Це свідчить про зростання останнім часом тенденції до поліморфізації вже класифікованих кібератак. Як результат, основні засоби захисту ІТМ по периметру – системи виявлення атак/вторгнень (СВА/СВВ), що побудовані на основі сигнатурних методів ідентифікування не попереджують їх вплив. За таких умов найбільш ефективним підходом до вирішення цієї задачі є застосування СВА нового покоління, які здатні не тільки виявляти кібератаки нульового дня на основі застосування підходу виявлення аномалій, а й дозволяють забезпечити прийняття ефективних рішень про стан об'єкту захисту за умов неповноти (нечіткості) інформації, яка аналізується та одночасно оперують якісними і кількісними знаннями. У зв'язку з цим для вирішення даної задачі доцільно застосувати моделі виявлення вторгнень, що побудовані на основі математичного апарату теорії нечітких множин та нечіткого логічного виводу [3 – 7].

Метою статті є розробка методики виявлення кібератак типу *JS (HTML)/ScrInject* на основі застосування математичного апарату теорії нечітких множин, яка дозволить надати управлінські рішення адміністратору з кібербезпеки для здійснення превентивних заходів щодо припинення її впливу.

Аналіз предметної області. 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.

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

Розробка методики 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*.

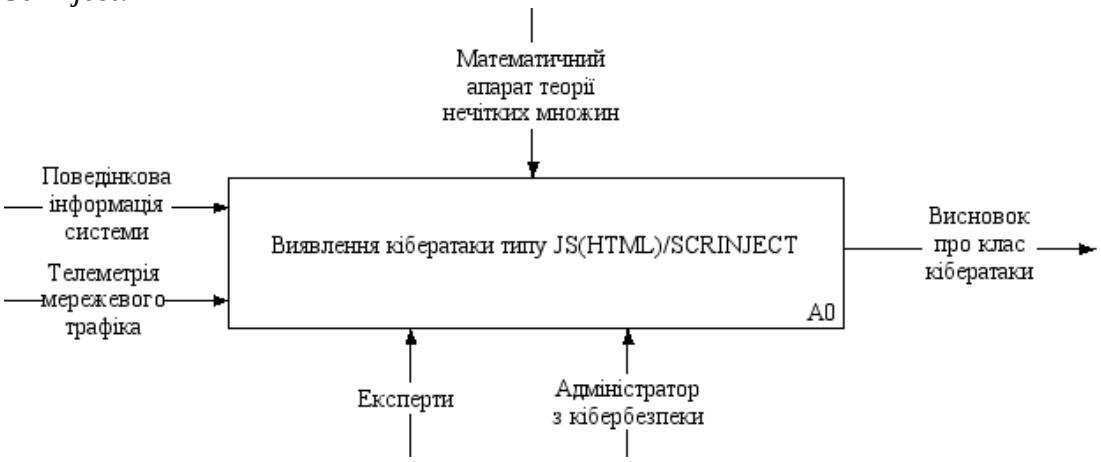

Рис. 1 Контекстна А-0 діаграма процесу визначення класу кібератаки

Вхідними даними є поведінкова інформація в ІТМ, на основі аналізу якої приймається рішення щодо виявлення кібератаки та телеметрія мережевого трафіка – 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 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.

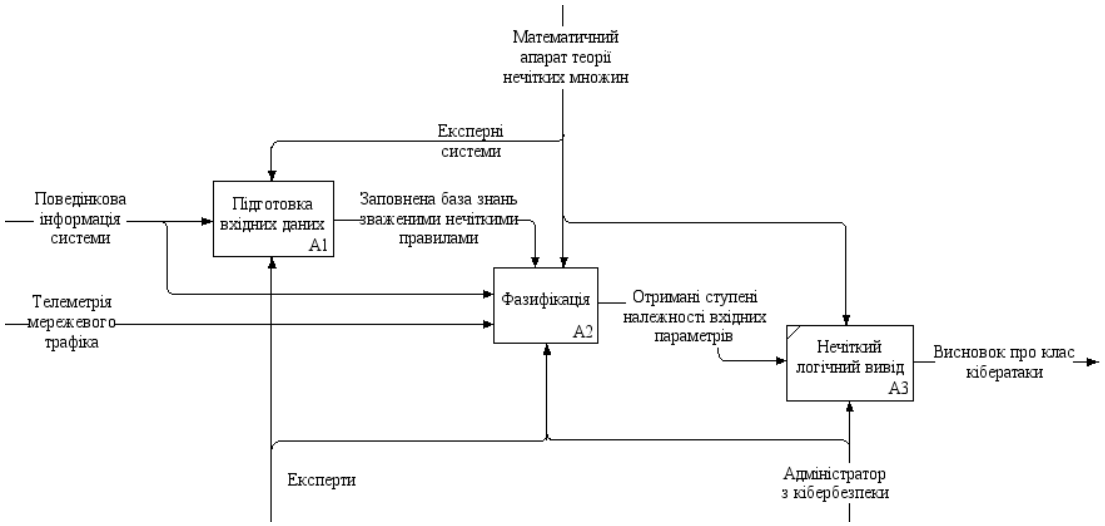

Рис. 2 Функціональна схема процесу визначення класу кібератаки типу *JS (HTML)/ScrInject*

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

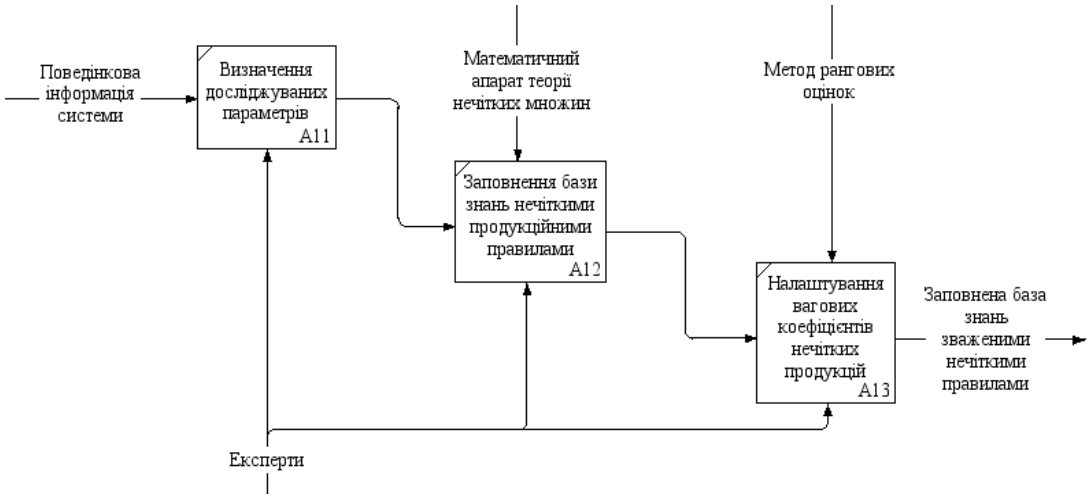

Рис. 3 Функціональна діаграма першого етапу запропонованої методики

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.

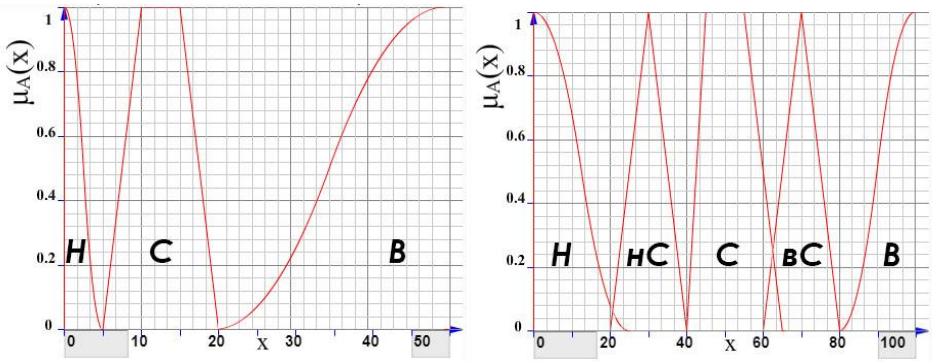

Рис. 4 Графічне зображення описаних лінгвістичних термів функцій належності

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:

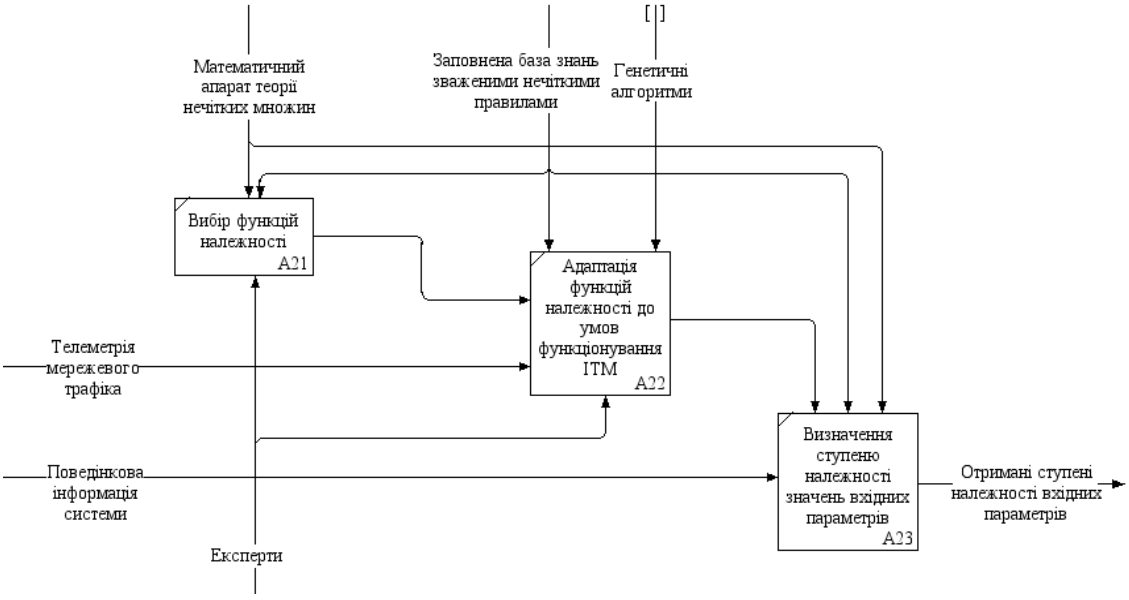

Рис. 5 Функціональна діаграма другого етапу запропонованої методики

На даному етапі запропонованої методики визначається ступінь належності значень досліджуваних параметрів терм-множинам вищевказаних лінгвістичних змінних. Врахування нечіткої мережевої активності ІТМ відбувається на основі застосування моделей запропонованих у [3, 4].

Дослідження ознак даної кібератаки будемо проводити на основі *Z,S* – подібного (початок/кінець діапазону значень), трикутного (Δ) та трапецеїдального (*T*) (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 трафіка. 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 запропонованих у [4 – 7]:

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

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

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 d 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 d_3-d_5 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*).

Висновки. У статті 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. Перспективними напрямками подальших наукових досліджень є вирішення питання наповнення бази знань шляхом застосування сучасних методів машинного навчання та інженерії знань.

ЛІТЕРАТУРА

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

2. „ТОП-10 вредоносных программ в Украине". [Электронный ресурс]. Доступно: https://eset.ua/ru/news/view/572/index0/-10-2018. Дата обращения: Сен., 10, 2018;

3. Субач І.Ю. Модель виявлення аномалій в інформаційно-телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу / І.Ю, Субач, В.В. Фесьоха // Збірник наукових праць ВІТІ. – 2017. – №3. – С.158 – 164.

4. Субач І.Ю. Модель виявлення кібернетичних атак на інформаційно-телекомунікаційні системи на основі описання аномалій їх роботи зваженими нечіткими правилами // Information technology and security, vol. 5, iss. 1, pp. 29 – 41, 2017.

5. J. Alam. Advance Cyber Security System using fuzzy logic / J. Alam, Dr. M. K. Pandey. // ACME: Journal of Management &IT, Vol: 10, Issue 1, September 2014 ISSN: 0974 – 1763.

6. Астахова Л.В. Применение самообучающейся системы корреляции событий информационной безопасности на основе нечеткой логики при автоматизации систем менеджмента информационной безопасности. // Л.В. Астахова, В.И. Цимбол // Вестник ЮУрГУ. Серия „Компьютерные технологии, управление, радиоэлектроника". 2015. Т. 16, № 1. С. 165 – 169.

7. M. Dodonov. Automated detection system of insider attacks using fuzzy logic. / Dodonov M., Dodonova N. // Information Technology and Nanotechnology (ITNT-2015).

8. Integration Definition for Function Modeling (IDEF0) – Software Standard, Modeling Techniques. Draft Federal Information Processing Standards Publication 183, 1993. – 128 p.

9. Субач І.Ю. Моделі надання знань для використання в системах підтримки прийняття рішень // Б.М. Герасимов, І.Ю. Субач, Є.В. Нікіфоров // Науково-технічна інформація. – 2005. – № 1. – С. 7 – 11.

10. Мітюшкін Ю. І. Soft Computing: ідентифікація закономірностей нечіткими базами знань / Ю. І. Мітюшкін, Б. І. Мокін, О. П. Ротштейн // Монографія. – Вінниця: УНІВЕРСУМ-Вінниця. – 2002. – 145 с.

11. E. Gandotra. Malware Threat Assessment Using Fuzzy Logic Paradigm. / Gandotra E., Divya Bansal D., Sofat S. // Cybernetics and Systems: an International Journal, 2016 – 20 p.