УДК 004.056.5

О.М. Юдін[1], Ю.І. Хлапонін[2]

[1] *Полтавський університет економіки і торгівлі, Полтава*
[2] *Національний авіаційний університет, Київ*

КОНТРОЛЬ ЗАХИЩЕНОСТІ БЕЗПРОВІДНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

У статті розглядається рішення задачі організації контролю захищеності вузлів безпровідної комп'ютерної мережі, яке базується на використанні апарату теорії нечітких множин. Особливість запропонованого підходу полягає в тому, що враховується динамічний характер безпровідної комп'ютерної мережі. Наданий в статті підхід служить основою для його автоматизації, що дозволить підвищити ефективність контролю вузлів і оперативність дій адміністратора мережі.

Ключові слова: *безпровідна комп'ютерна мережа, терми, уразливості, нечітка база знань.*

Вступ

Одним з ключових завдань у досягненні необхідного рівня безпеки комп'ютерних мереж є організація і проведення контролю захищеності, який передбачає пошук уразливостей у програмному та апаратному забезпеченні вузлів мережі. Необхідність постійного виконання пошуку уразливостей, з одного боку, обумовлена їх різким зростанням – тільки за дев'ять місяців 2014 року було знайдено понад 5000 уразливостей (рис. 1), з іншого боку – збільшенням шкідливого програмного забезпечення, кількість якого зросла на 76% у порівнянні з минулим роком, а мобільного – на 112% [1].

Контроль захищеності у комп'ютерної мережі здійснюється адміністратором за допомогою мережевих сканерів (сканерів безпеки) [2]. На даний час запропоновано підходи вдосконалення контролю захищеності провідних комп'ютерних мереж, метою яких є підвищення оперативності дій адміністратора мережі за рахунок автоматизації процесу підготовки і проведення контролю захищеності [3, 4]. Проте, аналіз вище зазначених підходів до організації контролю захищеності показує, що вони не враховують особливості безпровідних комп'ютерних мереж, хоча прогнозується зростання частоти і різноманітності атак саме на мобільні пристрої: для безпровідних мереж вже почали активно створювати генератори шкідливих додатків і поширювати готові зразки шкідливого коду [1]. Таким чином, вдосконалення процесу проведення контролю захищеності безпровідних комп'ютерних мереж є актуальною задачею.

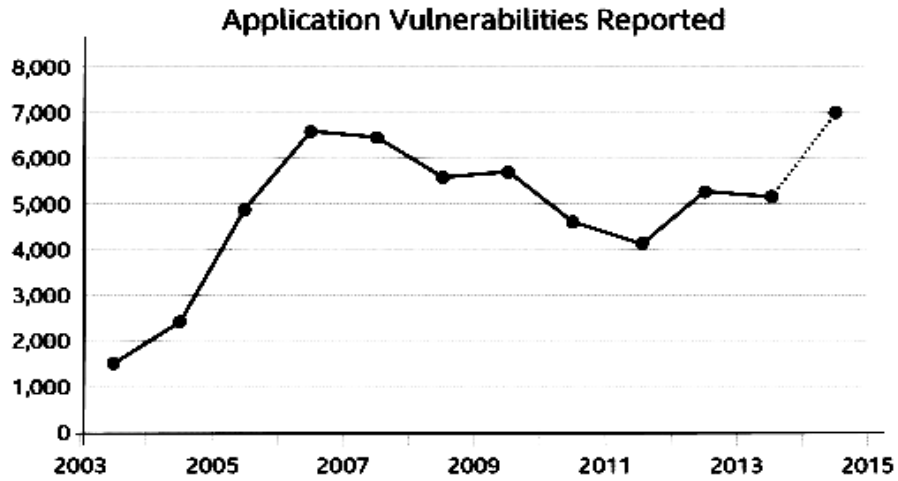

Рис. 1. Зростання кількості знайдених уразливостей

Основна частина

Принциповими особливостями безпровідної комп'ютерної мережі, що оказують суттєвий вплив на організацію контролю захищеності, є такі:

– певний ступень автономності вузла, кожен вузол працює від свого власного джерела живлення, акумуляторної батареї, заряд якої є обмеженим;

– якість зв'язку у межах зони покриття є залежною від багатьох умов і може сильно змінюватися у межах зони;

– можливість вузлів мережі вільно рухатися в межах зони покриття і, навіть, виходити за межі зони, потрапляючи в «мертву зону», де зв'язок відсутній.

Першим кроком при організації контролю захищеності вузлів мережі є визначення порядку їх перевірки, який може визначатися важливістю вузла. Для визначення важливості вузла провідної комп'ютерної мережі було запропоновано фактори, значення яких суттєво не змінювались для окремого вузла протягом тривалого часу. Для вузла безпровідної мережі, враховуючі зазначені вище особливості, фактори, що визначають його важливість, навпаки будуть змінюватися у часі. До таких факторів, наприклад, відносяться: автономність вузла, якість зв'язку (з окремим вузлом мережі), близькість вузла до «мертвої зони» (ділянки мережі, де зв'язок відсутній) тощо.

Для успішного вирішення завдання організації контролю захищеності безпровідної комп'ютерної мережі робота системи має спиратися на знання і досвід грамотного адміністратора, які він застосовує під час проведення контролю. Отже, рішення даної Введемо три лінгвістичні змінні: «автономність вузла», «якість зв'язку» і «важливість». Для термножиною першої лінгвістичної змінної буде T_1 = {«дуже низька», «низька», «середня», «висока», «дуже висока»}; другій – T_2 = {«дуже неякісний», «неякісний», «середній», «якісний», «дуже якісний»}; третій – T_3 = {«дуже низька», «низька», «середня», «висока», «дуже висока»}. Лінгвістичні змінні «автономність вузла» і «якість зв'язку» є вхідними змінними, а лінгвістична змінна «важливість» – вихідна змінна. Задамо фізичні значення термів для кожної лінгвістичної змінної. Змінна «автономність вузла» може приймати значення від 0 до 10 годин автономної роботи вузла від джерела живлення. Змінна «якість зв'язку» може приймати значення від 0 до 100%, «важливість» – від 0 до 1.

Побудуємо функції приналежності для кожного терму, кожної лінгвістичної змінної. При цьому для вхідних змінних застосуємо функції приналежності стандартного виду: S-функція, Z-функція, П-функція (рис. 2 – 4), для вихідної змінної – функція Гаусу.

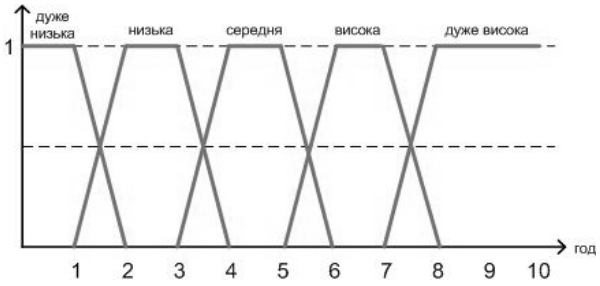

Рис. 2. Функції приналежності термів лінгвістичної змінної «автономність вузла»

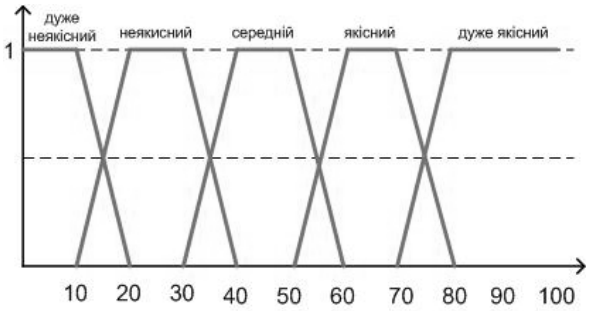

Рис. 3. Функції приналежності термів лінгвістичної змінної «якість зв'язку»

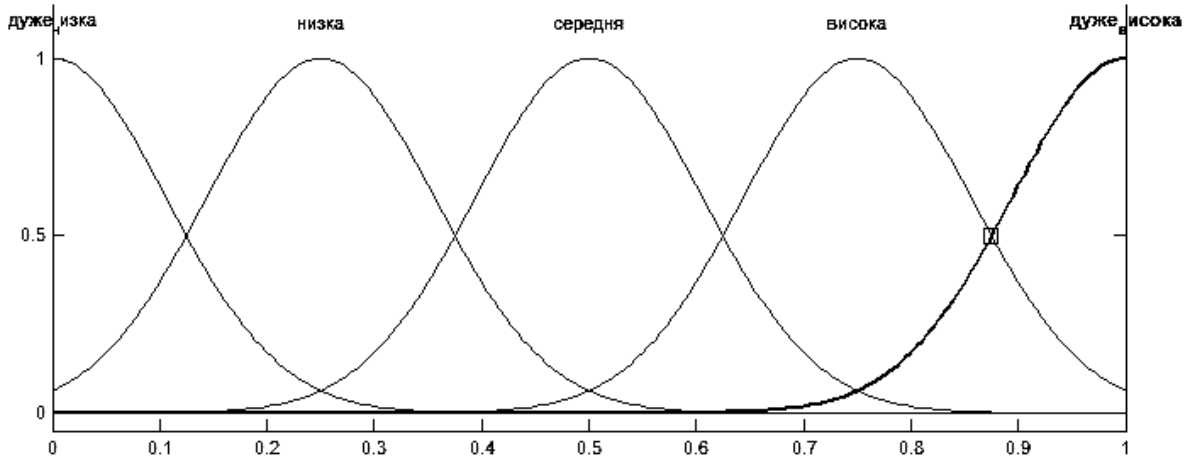

Рис. 4. Функції приналежності термів лінгвістичної змінної «важливість»

Формування нечіткої бази знань, за допомогою якої буде здійснюватися визначення важливості вузла, зробимо на основі продукційних правил. Доцільність використання продукційної моделі опису знань в системах нечіткого логічного висновку обумовлюється необхідністю обліку такої важливої специфіки роботи системи управління контролем захищеності, як реальний масштаб часу і зручність подання інформації про процедури і умови їх виконання. Будь-яке правило в базі знань може бути представлено таким чином:

$$\text{ЯКЩО } (\varepsilon \in \varepsilon_1^*) \text{ ТА } (\dot{\varepsilon} \in \dot{\varepsilon}_1^*), \text{ ТО } (u \in u_1^*),$$

де ε, $\dot{\varepsilon}$, u – змінні, а ε_1^*, $\underline{\dot{\varepsilon}_1^*}$, u_1^* – їх лінгвістичні оцінки.

Для зручності представимо правила у вигляді таблиці (табл. 1). Заголовки стовпчиків – назви термів лінгвістичної змінної «автономність вузла», заголовки рядків – назви термів лінгвістичної змінної «якість зв'язку». На перетині стовпчику і рядку знаходиться значення вихідної змінної.

Таблиця 1

Правила нечіткої бази знань

	Дуже низька	**Низька**	**Середня**	**Висока**	**Дуже висока**
Дуже неякісний	дуже висока	дуже висока	висока	середня	низька
Неякісний	дуже висока	висока	середня	середня	низька
Середній	висока	середня	середня	низька	низька
Якісний	висока	низька	середня	низька	дуже низька
Дуже якісний	середня	низька	низька	дуже низька	дуже низька

Приклад правила нечіткої бази знань:

Якщо АВТОНОМНІСТЬ ВУЗЛА = НИЗЬКА ТА ЯКІСТЬ ЗВ'ЯЗКУ = НЕЯКІСНИЙ, то ВАЖЛИВІСТЬ = ДУЖЕ ВИСОКА.

Виконаємо моделювання роботи системи нечіткого логічного висновку в середовищі MATLAB. Припустимо, що потрібно визначити порядок проведення контролю захищеності безпровідних вузлів, які працюють в межах виставкового павільйону розміром 60×60 м. Робота безпровідних пристроїв забезпечується 5 точками доступу, розташованими так, як показано на рис. 5.

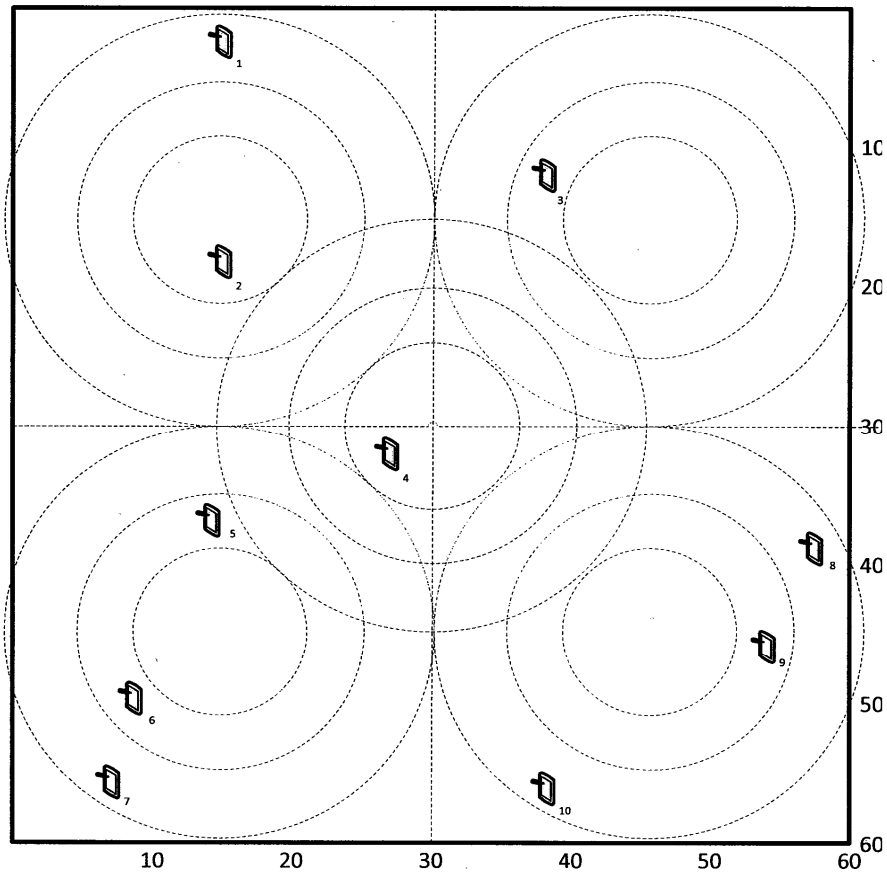

Рис. 5. Схема розташування точок доступу
та безпровідних пристроїв в межах виставкового павільйону

Вхідні значення лінгвістичних змінних «автономність вузла» (АВ) і «якість зв'язку» (ЯЗ) для розташування вузлів, зазначеного на рис. 5, в початковий момент часу надані в табл. 2.

Введемо вхідні значення по черзі у програму перегляду правил (рис. 6) для визначення важливості вузлів відповідно до правил, отримуємо значення, що надані в табл. 3.

Таблиця 2

Вхідні значення лінгвістичних змінних

	1	2	3	4	5	6	7	8	9	10
АВ	2	3	6	5	4	7	8	3	2	9
ЯЗ	20	75	45	60	40	50	10	25	50	15

Таблиця 3

Важливість вузлів

	1	2	3	4	5	6	7	8	9	10
АВ	2	3	6	5	4	7	8	3	2	9
ЯЗ	20	75	45	60	40	50	10	25	50	15
Важливість	0,748	0,253	0,252	0,5	0,506	0,252	0,252	0,748	0,5004	0,253

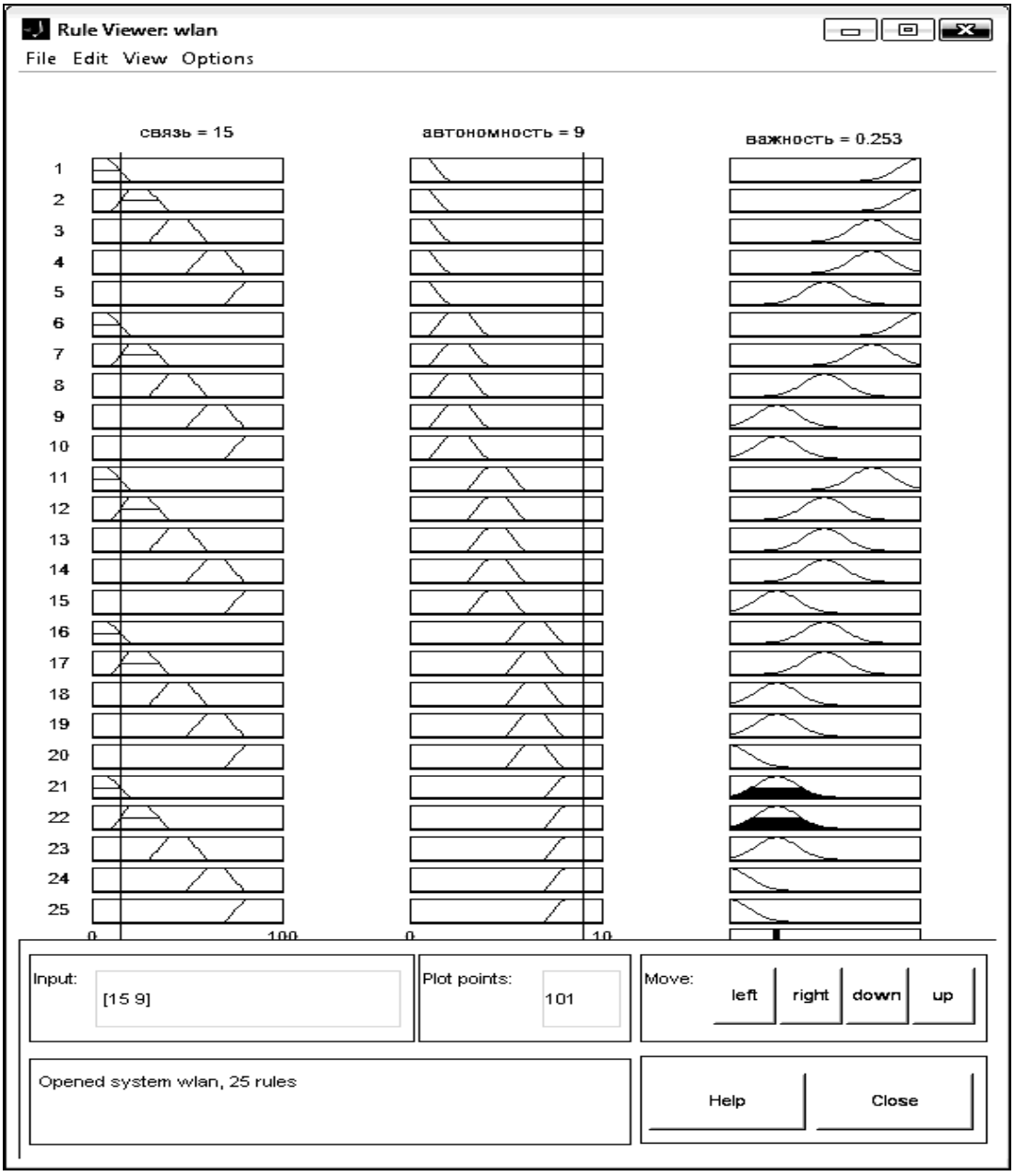

Рис. 6. Програма перегляду правил системи нечіткого логічного виводу

Для остаточного визначення порядку проведення контролю припустимо, що у випадку однакових значень важливості, першім буде перевірятися вузол з найменшим порядковим номером. Тоді аналіз значень важливості вузлів безпровідної мережі, отриманих в результаті моделювання дозволяє зробити наступний висновок стосовно порядку проведення контролю захищеності (табл. 4).

Таблиця 4

Порядок проведення контролю захищеності

Вузол	1	8	5	9	4	2	10	3	6	7
Важливість	0,748	0,748	0,506	0,504	0,5	0,253	0,253	0,252	0,252	0,252

Отже, першим буде перевірений перший вузол, потім – восьмий, далі – п’ятий тощо. Якщо перевірку вузла розпочато, то вона не переривається до її повного закінчення і вузол виключається з подальшого уточнення порядку проведення контролю, який здійснюється з визначеною періодичністю для інших вузлів мережі. Це необхідно робити тому, що безпровідна комп’ютерна мережа є дуже динамічним

середовищем. Власники безпровідних пристроїв можуть пересуватися в межах зони покриття, відповідно, зв'язок з ними може як покращуватися, так і погіршуватися. Крім того, вони можуть користуватися додатками, робота яких значно впливає на автономність пристрою.

Висновки

Таким чином, в роботі розглядається рішення задачі організації контролю захищеності вузлів безпровідної комп'ютерної мережі. Рішення задачі визначення порядку контролю захищеності вузлів безпровідної мережі базується на використанні апарату теорії нечітких множин.

Особливість запропонованого підходу полягає в тому, що враховується динамічний характер безпровідної комп’ютерної мережі. Наданий в статті підхід рішення задачі визначення контролю захищеності вузлів безпровідної комп'ютерної мережі служіть основою для його автоматизації, що дозволить підвищити ефективність контролю вузлів і оперативність дій адміністратора мережі.

Список літератури

1. Дериев Игорь. Киберугрозы 2015: прогноз от McAfee [Електронний ресурс] / Игорь Дериев. – Режим доступу до ресурсу: http://ko.com.ua/kiberugrozy _2015_prognoz_ot_ mcafee_108428 – Назва з екрана. – Дата звернення: 06.04.15.

2. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий. – СПб.: БХВ – Петербург, 2003. – 624с.

3. Юдін О.М. Вибір стратегії і тактики контролю захищеності вузлів комп'ютерної мережі на основі нечіткої логіки / О.М. Юдін // Зб. наук. пр. ВІТІ НТУУ «КПІ». – К.: ВІТІ НТУУ «КПІ», 2005. – № 1. – С. 172-177.

4. Мазулевский О.Е. Методика организации контроля защищенности компьютерной сети / О.Е. Мазулевський // Радіоелектронні і комп’ютерні системи – Х.: «ХАІ». – 2006. – № 5. – С. 122-127.

5. Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети / А.П. Ротштейн. – Винница: УНИВЕРСУМ – Винница, 1999. – 320 с.

Надійшла до редколегії 9.04.2015

Рецензент: д-р техн. наук проф. О.А. Смірнов, Кіровоградський національний технічний університет, Кіровоград.

КОНТРОЛЬ ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

А.Н. Юдин, Ю.И. Хлапонин

В статье рассматривается решение задачи организации контроля защищенности узлов беспроводной компьютерной сети, основанное на использовании аппарата теории нечетких множеств. Особенность предложенного подхода заключается в том, что учитывается динамический характер беспроводной компьютерной сети. Представленный в статье подход служит основой для его автоматизации, что позволит повысить эффективность контроля узлов и оперативность действий администратора.

Ключевые слова: *беспроводная компьютерная сеть, термы, уязвимости, нечеткая база знаний.*

MONITORING THE SECURITY OF WIRELESS COMPUTER NETWORKS

A.N. Yudin, Yu.I. Hlaponin

In the paper the solution of the problem of security control node wireless computer network, based on the use of the apparatus of fuzzy sets. The peculiarity of the proposed approach is taken into account the dynamic nature of the wireless computer network. Powered article in approach is the basis for its automation that will improve the effectiveness and efficiency of control nodes Action Network Administrator.

Keywords: *wireless computer network terms, vulnerability, fuzzy knowledge base.*