УДК 004.891

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц. **Красильников С.Р.** (ХмНУ)
Крижанський Р.О. (ХмНУ)

ОЦІНКА СТАНУ БЕЗПЕКИ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ НА ОСНОВІ ЛОГІКО-ЛІНГВІСТИЧНОГО ПІДХОДУ

У статті розглянутий метод оцінки стану безпеки інформації в комп'ютерних системах оснований на логіко-лінгвістичному підході. Процес оцінювання стану захищеності комп'ютерних систем складається з декількох етапів. Це формування еталонних значень, оцінка і формування поточного значення та порівняння отриманого значення з еталонними і на основі чого формування висновку про рівень захищеності оцінюваної комп'ютерної системи. Приведено відповідні розрахунки щодо оцінювання стану захищеності комп'ютерних систем. Логіко-лінгвістичний підхід можна застосувати для побудови моделі формування нечітких параметрів, які можна використовувати для підвищення ефективності технологій в системі виявлення атак. Проблема захисту інформації в комп'ютерних системах є відносно новою, проте із розвитком інформаційних технологій і тотального використання комп'ютерних систем та мереж у всіх галузях життя людей ця проблема потребує все більшої уваги. На сьогодні в сфері захисту інформації сформувалась досить потужна індустрія, що орієнтована на вирішення основних питань безпеки. Безпека інформації залежить від стану базових характеристик безпеки інформації та від успішності реалізації тієї чи іншої загрози.

Ключові слова: логіко-лінгвістичний підхід, еталонні значення, захист інформації, комп'ютерні системи.

Вступ. Проблема захисту інформації в комп'ютерних системах є відносно новою, проте із розвитком інформаційних технологій і тотального використання комп'ютерних систем та мереж у всіх галузях життя людей ця проблема потребує все більшої уваги. На сьогодні в сфері захисту інформації сформувалась досить потужна індустрія, що орієнтована на вирішення основних питань безпеки.

Стан безпеки інформації, відповідно до його базових характеристик, залежить від успішності реалізації тієї чи іншої загрози. Під час побудови комплексних систем захисту (СЗ) інформації аналіз загроз є одним з обов'язкових етапів. На цьому етапі формується найбільш повна множина загроз з врахуванням факторів ризику та їх властивостей.

Найбільш розповсюдженою та найбільш повною класифікацією загроз є розподіл їх за такими ознаками [1, 2, 3, 4]:

- за впливом на характеристики безпеки інформації: К-тип (загроза конфіденційності); Ц-тип (загроза цілісності); Д-тип (загроза доступності); КЦ-тип (загроза конфіденційності та цілісності); КД-тип (загроза конфіденційності та доступності); ЦД-тип (загроза цілісності та доступності); КЦД-тип (загроза конфіденційності, цілісності та доступності);
- за природою джерела: об'єктивна, виникнення якої не залежить від прямої діяльності людини і пов'язана з різними стихійними природними проявами; суб'єктивна, виникнення якої залежить від діяльності людини.

В свою чергу суб'єктивну загрозу за мотивом поділяють на активну, таку що пов'язана з діями людини, які направленні на отримання певної вигоди та пасивну, тобто ту, яка виключає вказану складову і пов'язана з помилками людини.

Індустрія сучасних засобів захисту інформації визначається широким номенклатурним арсеналом. Такі засоби з практичної точки зору можна розподілити на наступні класи [1,5,7]: апаратні; програмні; програмно-апаратні; криптографічні; стеганографічні; організаційні; законодавчі; морально-етичні.

Як показує практика, найбільш дорогою складовою комп'ютерних систем **(**КС) є її програмне забезпечення (ПЗ). Тому розробка програмних засобів захисту інформації для захисту ПЗ з практичної точки зору є найбільш привабливим завданням. Питання захисту ПЗ (щодо його копіювання, а також динамічних і статичних методів дослідження), від хакерів, найгостріше стоїть перед його розробниками і власниками. Із системних позицій, захист ПЗ

забезпечується цілим комплексом засобів, який починається законодавчими актами і закінчується конкретними апаратурними розробками. Серед засобів захисту ПЗ можна виділити такі категорії: власні, у складі КС, із запитом інформації, активні, пасивні.

Останнім часом інтенсивно розвиваються стеганографічні засоби (стеганографія – приховування інформації в такій формі, коли сам факт наявності інформації не очевидний, наприклад приховування даних у звукових або графічних файлах), але широкого практичного застосування (особливо на державному рівні) вони поки не отримали. Організаційні засоби [1] – організаційно-технічні та організаційно-правові заходи (наприклад, організація розробки та використання СЗ інформації, контроль за знищенням носіїв та інформації з обмеженим доступом, аудит СЗ, експертизи і т.п.), які здійснюються впродовж всіх технологічних етапів (проектування, виготовлення, модифікація, експлуатація, утилізація тощо) існування КС з метою вирішення завдань захисту інформації.

Постановка задачі. Питання прийняття рішень – одна з найбільш розповсюджених задач. В багатьох випадках рішення приймаються в умовах певних обмежень, а результати зумовлені можливими діями точно не відомі [1]. В теорії інформації, як і в багатьох інших областях науки, неточність та невизначеність зазвичай визначаються за допомогою методів та понять теорії вірогідності. При цьому поняття нечіткості ототожнюють з випадковістю. Проте в більшості випадків джерелом неточності виступає не наявність яких-небудь випадкових величин, а поява в задачі, яка розглядається, якого-небудь класу або класів величин, що не мають чітко визначених меж [1,6]. Більшість класів об'єктів, з якими доводиться стикатися в реальному світі, являються класами саме нечіткого типу. В такому випадку елемент може належати або ж не належати до певного класу, але, крім того, можливим є також і проміжна градація належності, тому тут для опису степені належності елементу до класу (певної множини значень) необхідно використовувати багатозначну логіку. Тобто людина, яка вирішує задачі, що не піддаються строгій формалізації використовує суб'єктивні та розмиті уявлення. Усвідомлення даного факту призвело до появи нової математичної дисципліни – нечіткої логіки [1], яка усунула розбіжності між суворістю математики та невизначеностями реального світу.

Центральним поняттям нечіткої логіки є поняття нечітких множин. Нечітка множина (НМ) [6] – певний клас з множиною різних ступенів належності до нього, що може бути безперервною нескінченою множиною. Точніше кажучи, нехай X - сукупність об'єктів x, де $X = \{x\}$. Тоді нечітка множина A на X задається функцією належності (ФН) $\mu_A(x)$ (або просто μ_A), котра ставить у відповідність кожному x числа з інтервалу [0, 1], що являються ступенем належності x до A. Чим ближча величина $\mu_A(x)$ до одиниці, тим вища степінь належності x до A і, навпаки, чим меша величина $\mu_A(x)$ тим нижча степінь належності x до A. Формально нечітку множину A на універсальній множині X можна задати як сукупність пар $A = \left\{ \left\langle \underset{\sim}{\mu}_A(x)/x \right\rangle \right\}$.

Основним поняттям теорії НМ є ФН [1,6], тому визначення ступені належності елементів множині та побудова на їх основі ФН – основне питання практичної реалізації незалежно від того, до якої предметної галузі вони належать. При вирішенні задач захисту інформації, моделювання процесів прийняття рішень в нечітких умовах можна використати багаточисельні методи формування ФН.

Серед відомих методів формування ФН виділяють наступні [1, 2, 4, 5]: метод опитування (МО); чисельний метод (ЧМ); метод лінгвістичних термів (МЛТС); метод кількісного парного порівняння (КПП); метод порівняння зі знаходженням квадратного кореня (ПЗК); метод порівняння зі знаходженням частки (ПЗЧ); метод попарного порівняння найменших квадратів (ППНК); метод попарного порівняння на рангових оцінках (ППРО); метод призначення параметрів (МПП); метод корегування параметрів (КП); метод побудови експоненціальної функції (ЕФН); метод прямого та зворотного оцінювання (ПЗО); метод

інтервальних оцінок (МІО); метод рівневих множин (МРМ). Методи побудови ФН відрізняються один від одного способом отримання та опрацювання вхідних даних.

Метод лінгвістичних термів. В МЛТС в якості ступені належності елемента множині приймається оцінка частоти використання поняття, що задається НМ для характеристики елементу. На шкалі [0, 1] розміщуються значення логічних змінних (ЛЗ). Причому в ідеалі метод базується на тому, що в кожний інтервал шкали попадає однакова кількість експериментів, що на практиці відбувається досить рідко. В такому випадку дані опрацьовуються з використанням матриці підказок. Коли вже отримано результати експериментів, вони заносяться в таблицю і опрацьовуються так, щоб максимально зменшити погрішності, внесені в процесі експерименту (з таблиці видаляються окремі елементи, по ліву і по праву сторону від яких стоять нулі). Матриця підказок являє собою строку, елементи якої обчислюються за формулою (1).

$$k_j = \bigcup_{i=1}^{n} \sum_{i=1}^{n} b_{ij}, j = \overline{1,n}, \quad (1)$$

де n – кількість значень ЛЗ, b_{ij} – елемент таблиці результатів.

Далі в отриманому рядку обирається максимальне значення k_j і всі елементи таблиці результатів експериментів перетворюються за виразом (2)

$$c_{ij} = b_{ij} k_{\max} / k_j, i = \overline{1,n}; j = \overline{1,n}, \quad (2)$$

а для стовпців, де $k_j = 0$ застосовується лінійна апроксимація $c_{ij} = (c_{ij-1} + c_{ij+1})/2, i = \overline{1,n}; j = \overline{1,n}$. Наступним кроком методу є обчислення значення ФН за формулою (3)

$$\mu_{ij} = c_{ij} / c_{i\max}, \text{ де } c_{i\max} = \max_j c_{ij}, i = \overline{1,n}; j = \overline{1,n}. \quad (3)$$

В МЛТС використовуються статистичні дані і їх обробка та отримання ФН є досить трудомістким процесом, так як для побудови ФН одного терму необхідно провести статистичні дослідження і для всіх останніх термів.

Можливості кожного з існуючих методів побудови ФН обмежуються класом отриманих в результаті НЧ, що в подальшому впливає на вибір методів реалізації операцій нечіткої арифметики.

Розробляючи організаційні засоби, необхідно враховувати, щоб в загальній множині механізмів захисту вони могли самостійно або й у комплексі з іншими засобами вирішувати завдання захисту, забезпечувати ефективне використання засобів інших класів, а також раціонально об'єднувати всі засоби в єдину цілісну СЗ. Слід зазначити, що безліч всіх потрібних і потенційно можливих організаційних засобів невизначена і не існує формальних методів формування їх переліку та змісту. Виходячи з цього можна вважати, що основними методами формування організаційних засобів є неформально-евристичні.

Оцінка стану безпеки інформації в комп'ютерних системах. Оцінка рівня безпеки КС трудомістка та важко-структурована задача, вирішення якої вимагає глибоких предметних знань та великого практичного досвіду. Вирішення задачі грунтується на знаннях експертів і пов'язане з високою трудомісткістю процедур аналізу. Під час вирішення такої задачі виникає потреба в обробці даних представлених в різних формах. Тому для забезпечення ефективного вирішення проблеми оцінки захисту інформації в КС необхідні спеціальні інтелектуальні засоби. Традиційними математичними методами не завжди можливо ефективно і коректно вирішити дане питання, тому тут доцільніше використовувати методи, основані на НМ та логічних змінних (ЛЗ), неформальному оцінюванні та пошуку оптимальних рішень.

Стан безпеки в системі характеризується, зазвичай, лінгвістичними даними і для їх формалізації найкраще використовувати поняття ЛЗ. ЛЗ спочатку використовувались як засіб моделювання нечіткості людської мови, а з часом це поняття набуло ширшого значення і тепер використовується як засіб для опису складних систем, що містять

параметри, представлені не тільки в кількісному, але і в якісному вигляді. При цьому ЛЗ дозволяють співвіднести якісним значенням певну кількісну характеристику і таким чином формалізувати їх.

Лінгвістична змінна характеризується набором $(X,T(X),U,G,M)$ [1], де X – назва змінної; $T(X)$ – терм-множина змінної X, тобто це множина назв лінгвістичних значень змінної A, причому кожне з таких значень являє собою нечітку змінну X із значеннями з універсальної множини U з базовою змінною u; G – синтаксичне правило (зазвичай має форму граматики), що породжує назву A значень змінної X, а M – семантичне правило, яке ставить у відповідність кожній нечіткій змінній A її зміст $M(X)$. Конкретна назва X, що породжена синтаксичним правилом G, називається термом. Терм, який складається з одного або декількох слів, що завжди фігурують одне з одним, називається атомарним термом. Терм, який складається з одного або декількох атомарних термів називається складеним термом. Результат приписування один до одного ланцюжків-компонентів складеного терму являється підтермом.

Безпосередньо до назв ЛЗ та їх термів вимог не ставлять [1]. Терми ЛЗ повинні бути впорядковані, а ФН НМ, що визначає базовий терм повинна задовольняти ряду умов. А саме:

- значення ФН термів на границях впорядкованої множини X повинні бути одиничними: $\mu_{T1}(x_{\min})=1, \mu_{TN}(x_{\max})=1.$

- одна і та ж точка не може одночасно з ступенем належності 1 належати більше ніж одному терму і відповідно кожне значення з області визначення ЛЗ повинно описуватись хоча б одним термом: $\forall i, i+1=\overline{1,n}: 0<\max\limits_{x\in X} \mu_{Ti\cap Ti+1}(x)<1.$

- кожне поняття в ЛЗ повинно мати хоча б одне еталонне визначення, тобто таку точку, де ФН базового терма рівне одиниці: $\forall i=\overline{1,n}\ \exists x\in: X\ \ \mu_T(x)=1.$

- будь-яке поняття, що описується ЛЗ має фізичне обмеження на числові значення параметрів. Для неперервної універсальної множини X додатково існує умова неперервності ФН базових термів: $\forall i=\overline{1,n}\ \ 0<\int\limits_x \mu_T(x)dx<\infty$.

Процес формування ЛЗ починається з визначення кількості термів та їх впорядкування, визначення граничних значень ЛЗ, далі визначається метод формування ФН та проведення експертного опитування і як результат побудова ФН для будь-якого з термів ЛЗ.

Логіко-лінгвістичний підхід можна застосувати для побудови моделі формування нечітких параметрів, які можна використовувати для підвищення ефективності технологій в системі виявлення атак. Така модель представляє собою сукупність дій, представлених у кілька етапів: визначення нечітких понять, формування нечітких еталонів, формування поточних нечітких параметрів та оцінка стану безпеки на основі порівняння еталонних та поточних параметрів.

Визначення нечітких величин. При спробі будь-якого порушника здійснити атаку на об'єкт першими його діями буде обрання об'єкту атаки та зібрання про нього детальної інформації. Отримання інформації про об'єкт, що атакується, можна здійснити шляхом сканування портів (ідентифікація сервісів). Оскільки конкретний відкритий порт говорить про присутність певного сервісу (наприклад, 80-тий порт свідчить про наявність Web-серверу). Виявити факт сканування портів можна на основі аналізу мережевого трафіку. Для чого слід виділити окремі його характеристики, які і будуть надалі використані для визначення набору нечітких величин. Однією з таких характеристик буде поняття "віртуального каналу". Віртуальний канал (ВК) – це канал, що утворюється в момент отримання (по заданому порту) IP-пакету і після чого існує деякий час. Максимальна кількість таких каналів ($\max_{КВК}$) обумовлена апаратними та програмними можливостями КС. Будь-який ВК характеризується параметрами "час життя" (ЧЖ) та "вік" (ВВК). За параметром ЧЖ можна визначити скільки каналу залишилось існувати. При створенні ВК

присвоюється початкове значення ЧЖ$_0$ по закінченні цього терміну канал припинить своє існування, а при повторному проходженні трафіку через канал параметр ЧЖ збільшується на значення ΔЧЖ. ВВК – це час, що пройшов від моменту створення ВК. Виходячи з властивостей ВК, чим інтенсивніший трафік, тим живучіший канал, при цьому значення ВВК постійно збільшується, а значення ЧЖ більше за нуль. Отже, для оцінки стану безпеки будуть використовуватись дві ЛЗ "Кількість віртуальних каналів" (КВК) та "Вік віртуального каналу" (ВВК), які відповідно визначаються кортежами $\langle KBK, T_{KBK}, X_{KBK} \rangle$ та $\langle BBK, T_{BBK}, X_{BBK} \rangle$, для яких синтаксичне правило та семантична процедура не задаються.

Формування нечітких еталонів. Тепер введені ЛЗ необхідно визначити. Для обох ЛЗ цей процес однаковий і включає в себе наступні стадії: формування базової терм-множини, формування ФН і формування нечітких еталонів.

Для КВК *базову* терм-множину задамо п'ятьма термами $T_{KBK} = \bigcup_{i=1}^{5} T_{KBKi}$ = {"дуже мала" (ДМ), "мала" (М), "середня" (С), "велика" (В), "дуже велика" (ДВ)}, що може бути відображена на універсальній множині $X_{KBK} \in \{0, \max_{\text{КВК}}\}$. Терм-множина визначається нечіткими числами, для яких необхідно визначити ФН.

ФН для *термів* КВК визначаємо за допомогою МЛТС. Для цього в емпіричну таблицю (таблиця 1) заносимо статистичні дані (за 24 години роботи) відносно ВК (в таблиці як N1, N2, N3, N4, N5 інтервали відповідно [0; 2], [3; 8], [9; 16], [17; 64], [65; 256], $\max_{KBK} = 256$).

Таблиця 1

Статистичні дані для формування термів T_{KBKI}

Значення ЛЗ	Інтервал				
	N1	N2	N3	N4	N5
ДМ	3	1	0	0	0
М	1	2	1	0	0
С	0	1	3	0	0
В	0	0	2	4	1
ДВ	0	0	0	3	5

Згідно статистичних даних за формулою (1) формуємо матрицю підказок. Далі за (3) знаходимо ФН. Для $\bigcup_{i=1}^{5} \mu_{ij}$, відповідно до технології МЛТС, знаходимо оцінювані відношення $\bigcup_{i=1}^{5} \Delta B/B = \{2/256 \quad 8/256 \quad 18/256 \quad 64/256 \quad 256/256\} = \{0{,}008 \quad 0{,}031 \quad 0{,}063 \quad 0{,}25 \quad 1\}$ (де $\Delta B/B$ – відхилення параметру $\Delta B_{KBK} \in [0, \text{B}_{\text{КВК}}]$, а $\text{B}_{\text{КВК}}$ – максимально можливе значення, що характеризує поточне вимірювання) і отримуємо НЧ. Для формування нечітких еталонів необхідно щоб для $\forall T_{KBKI}$ виконувалось співвідношення порядку, наприклад, при $i = 1, \forall X_{ДМ} : X_{ДМК} < X_{ДМК+1}$. Далі отримані T_{KBK} представляються в приведеній формі T^{e}_{KBK}, яка і використовується як еталон:

$$ДМ^e = \left\{ 0/0{,}008;\ 1/0{,}008;\ 0{,}33/0{,}031;\ 0/0{,}063 \right\}$$
$$M^e = \left\{ 0/0{,}008;\ 0{,}5/0{,}008;\ 1/0{,}031;\ 0{,}5/0{,}063;\ 0/0{,}25 \right\}$$
$$C^e = \left\{ 0/0{,}008;\ 0{,}33/0{,}031;\ 1/0{,}063;\ 0{,}67/0{,}25;\ 0/1 \right\}$$
$$B^e = \left\{ 0/0{,}063;\ 1/0{,}25;\ 0{,}75/1;\ 0/1 \right\}$$
$$ДВ^e = \left\{ 0/0{,}063;\ 0{,}2/0{,}25;\ 1/1;\ 0/1 \right\}$$

Графічне зображення яких представлене на рис. 1.

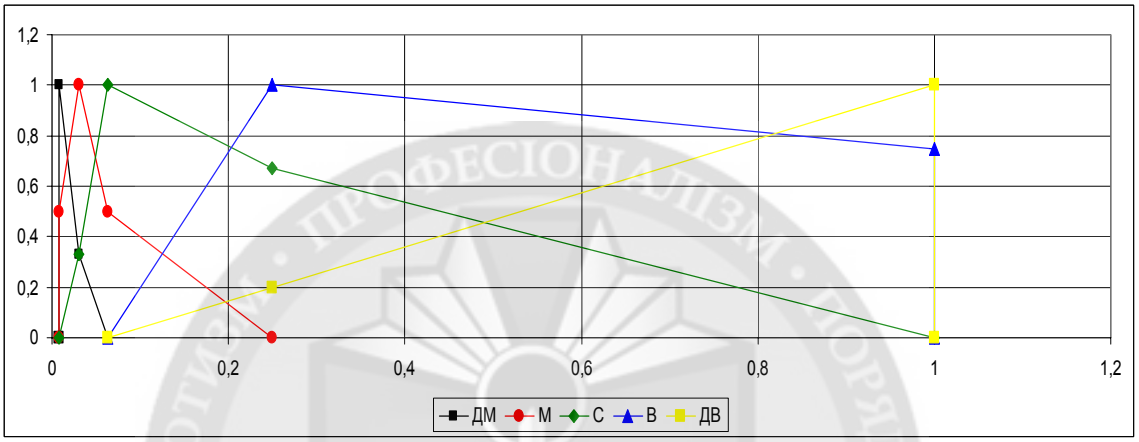

Рис. 1. Еталонні НЧ для КВК

Для ВВК базову терм-множину задамо трьома термами $T_{ВВК} = \bigcup_{i=1}^{3} T_{ВВКi}$ = {“молодий” (М), “середній” (СР), “старий” (СТ)}, що може бути відображена на універсальній множині $X_{ВВК} \in \{0, \max_{ВВК}\}$.

Терм-множина визначається нечіткими числами (М, СР, СТ), для яких за методом МЛТС визначаємо ФН. Для чого по роботі комп’ютера в мережі збираємо статистичну інформацію (за 24 години роботи), яка представлена в таблиці 2, де N1, N2, N3 інтервали (в хвилинах) відповідно [0; 30], [30; 100], [100; 250], а $\max_{ВВК} = 250$.

Таблиця 2

Статистичні дані для формування термів $T_{КВКІ}$

Значення ЛЗ	Інтервал		
	N1	N2	N3
М	4	1	0
СР	2	5	1
СТ	1	2	6

Згідно цих даних за формулою (1) формуємо, як і для випадку з КВК матрицю підказок $k_j = \bigcup_{i=1}^{3} \sum_{i=1}^{3} b_{ij} = \{(4+2+1),(1+5+2),(0+1+6)\} = \{7,8,7\}$ (тут $k\max = 8$).

При формуванні еталонних значень для ВВК приводимо отримані НЧ аналогічним чином як і у випадку з КВК (рис. 2):

$$M^e = \left\{ \frac{1}{0} \quad \frac{1}{0,12} \quad \frac{0,5}{0,4} \quad \frac{0,25}{1} \right\}$$

$$CP^e = \left\{ \frac{0,2}{0} \quad \frac{0,2}{0,12} \quad \frac{1}{0,4} \quad \frac{0,4}{1} \right\}$$

$$CT^e = \left\{ \frac{0}{0,12} \quad \frac{0,17}{0,4} \quad \frac{1}{1} \right\}$$

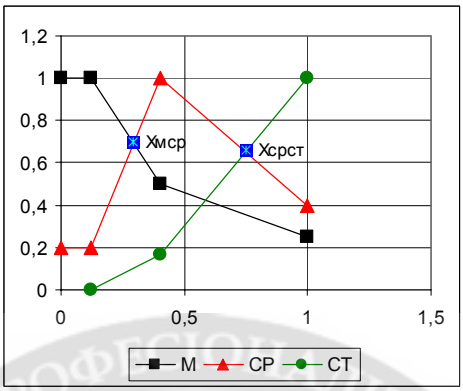

Рис. 2. Еталонні НЧ для ВВК

Формування поточних параметрів. На основі КВК та ВВК з еталонними термами, поточні параметри (значення КВК відносно ВВК) формуємо для заданих моментів часу T. При формуванні поточних значень для КВК та ВВК проводимо розрахунки аналогічним чином як і у випадку формування еталонних параметрів. На рисунку 3 зображено поточне значення $КВК(M)$ відносно еталонних.

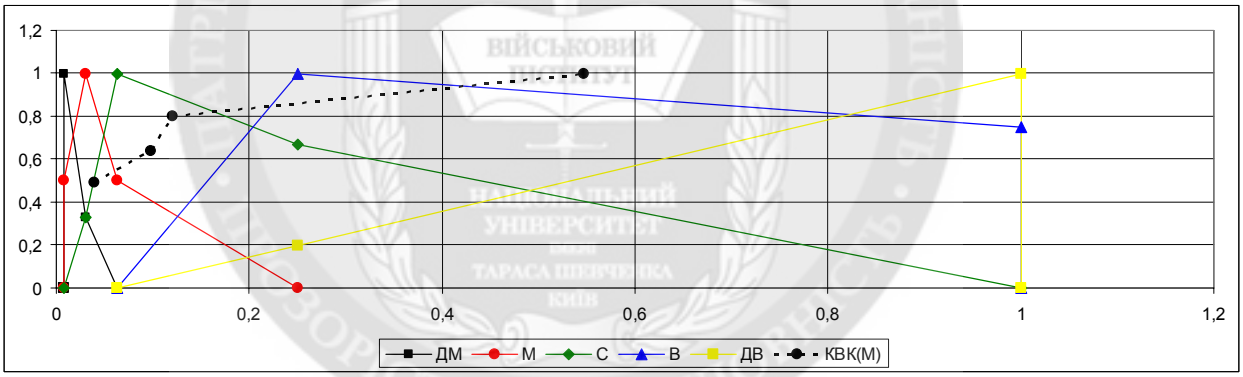

Рис. 3. Поточне значення КВК(М) та еталонних НЧ для КВК

Оцінка стану безпеки. Для того, щоб оцінити стан безпеки необхідно порівняти поточне значення з еталонними. Для порівняння НЧ використовується функція впорядкування (ФУП) [1]. ФУП дає змогу зрівнювати будь-які нечіткі підмножини вказаного інтервалу, а висновок щодо стану захищеності комп'ютерної системи визначимо згідно набору евристичних правил:

Правило 1. Якщо $КВК(M)$ ближче до $ДМ^e$, то можливість сканування $Н$;

Правило 2. Якщо $КВК(M)$ ближче до M^e, то можливість сканування $БНВ$;

Правило 3. Якщо $КВК(M)$ ближче до C^e, то можливість сканування $БВН$;

Правило 4. Якщо $КВК(M)$ ближче до B^e, то можливість сканування $В$;

Правило 5. Якщо $КВК(M)$ ближче до $ДВ^e$, то можливість сканування $ДВ$,

де $Н$ – низька, $БНВ$ – більш низька ніж висока, $БВН$ – більш висока ніж низька, $В$ – висока, $ДВ$ – дуже висока.

Таким чином на основі проведених розрахунків, поточне значення КВК(М) за значенням функції впорядкування найближче знаходиться до еталонного B^{eA}, що, згідно евристичних правил, дає змогу зробити висновок, що можливість сканування портів є високою.

Висновки. Проблема захисту інформації в комп'ютерних системах є відносно новою, проте із розвитком інформаційних технологій і тотального використання комп'ютерних систем та мереж у всіх галузях життя людей ця проблема потребує все більшої уваги. На сьогодні в сфері захисту інформації сформувалась досить потужна індустрія, що орієнтована на вирішення основних питань безпеки. Безпека інформації залежить від стану базових характеристик безпеки інформації та від успішності реалізації тієї чи іншої загрози. Процес оцінювання стану захищеності комп'ютерних систем складається з декількох етапів. Це формування еталонних значень, оцінка і формування поточного значення та порівняння отриманого значення з еталонними і на основі чого формування висновку про рівень захищеності оцінюваної комп'ютерної системи.

ЛІТЕРАТУРА:

1. Корченко О.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения./ О.Г. Корченко – К.: "МК-Пресс", 2006. – 320 с., ил.

2. Пескова О.Ю. Методическое пособие «Теория и практика организации защиты информационных систем» по курсу «защита информационных систем». / О.Ю. Пескова -Часть 1. Таганрог: изд.-во ТРТУ, 2001. - с.

3. Анин Б. Ю. Защита компьютерной информации. /Б. Ю. Анин –СПб.: БХВ-Петербург, 2000. –384 с.: ил.

4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. /В.А. Герасименко - М: Энергоатомиздат, 1994. – 400с.

5. Хорошко В.А. Методы и средства защиты информации. / В.А. Хорошко, А.А.Чекатов – К.: Юниор, 2003. –. 478 с. 3.

6. Заде Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений. / Л.А. Заде -М.:Мир, 1976.-165 с.

7. Хоффман Л. Современные методы защиты информации. / Л. Хоффман - М.: Сов. радио, 1980. - 264 с.

REFERENCES:

1. OG Korchenko Building a system of information protection in nechetkyh multitude. Theory and praktycheskye decision. / OG Korchenko - K .: "MK-Press", 2006. - 320 p., Ill.

2. O. Peskov Metodycheskoe posobye "Theory and Practice of organization of protection of information systems" on course "protection of information systems." / O. Peskov -Chast 1. Taganrog: yzd.-in TRTU, 2000 p.

3. Anyn B. Yu Zashchita of computer information. / B. Yu Anyn SPb .: BHV-Peterburg, 2000. --- 384 pp .: ill.

4. Gerasimenko VA Zashchita of information systems in avtomatyzyrovannыh obrabotku data. /V.A. Gerasimenko - M: Energoatomizdat, 1994. - 400p.

5. Khoroshko VA Methods of protection means and information. / VA Khoroshko, A.A.Chekatov - K .: Yunyor, 2003. -. 478 p. 3.

6. 6. LA Zadeh The concept lynhvystycheskoy variable and ego Application for Adoption pryblyzhennыh decisions. / LA Zadeh -M. Peace, 1976.-165 with.

7. 7. L. Hoffman Modern methods of information protection. / L. Hoffman - M .: Sov. radio, 1980. - 264 p.

Без рецензії.

д.т.н., проф. Ленков С.В. **к.т.н. Красильников С.Р., Крижанский Р.А.**

ОЦЕНКА СОСТОЯНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ НА ОСНОВЕ ЛОГИКО-ЛИНГВИСТИЧЕСКОЕ ПОДХОДА

В статье рассмотрен метод оценки состояния безопасности информации в компьютерных системах, основанный на логико-лингвистическом подходе. Процесс оценки состояния защищенности компьютерных систем состоит из нескольких этапов. Это формирование эталонных значений, оценка и формирование текущего значения и сравнения полученного значения с эталонными и на основе чего формирования заключения об уровне защищенности оцениваемой компьютерной системы. Приведены соответствующие расчеты по оценке состояния защищенности компьютерных систем. Логико-лингвистический подход можно применить для построения модели формирования нечетких параметров, которые можно использовать для повышения эффективности технологий в системе обнаружения атак. Проблема защиты информации в компьютерных системах является относительно новой, однако с развитием информационных технологий и тотального использования компьютерных систем и сетей во всех сферах жизни людей эта проблема требует все большего внимания. На сегодня в сфере защиты информации сформировалась достаточно мощная индустрия, ориентированная на решение основных вопросов безопасности. Безопасность зависит от состояния базовых характеристик безопасности информации и от успешности реализации той или иной угрозы.

Ключевые слова: логико-лингвистический подход, эталонные значения, защита информации, компьютерные системы.

Prof. Lenkov S.V., Ph.D. Krasil'nikov SR, Krizhansky R.A.

ASSESSMENT OF SAFETY IN COMPUTER INFORMATION SYSTEMS BASED LOGICAL APPROACH LINGUISTIC

The article describes the method of assessing the security state of the information in computer systems based on the logical-linguistic approach. The process of assessing the state of computer security systems consists of several stages. It is the formation of the reference values, the evaluation and formation of the current value and compare the value obtained with the reference and the basis on which to conclude the formation of the level of security of the computer system being evaluated. The corresponding calculations to assess the state of security of computer systems. Logico-linguistic approach can be used to build the model of formation of the fuzzy parameters, which can be used to improve efficiency technologies in intrusion detection system. The problem of protection of the information in computer systems is a relatively new, but with the development of information technology and the total use of computer systems and networks in all aspects of people's lives, this problem requires more attention. At present, formed a sufficiently powerful industry, focused on addressing the major security issues in the field of information security. Security depends on the basic characteristics of information security and the success of the implementation of a threat.

Keywords: logical-linguistic approach, reference values, information security, computer systems.