УДК 004.891

к.т.н., доц. **Красильников С.Р.** (ХмНУ)
к.т.н. **Лєнков Є.С.** (ВІТІ)
Крижанський Р.О. (ХмНУ)
Міщенко А.О. (ВІТІ)

ОЦІНКА СТАНУ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА ОСНОВІ ЛІНГВІСТИЧНИХ ТА ВАРІАТИВНИХ БАЛЬНИХ ШКАЛ

У статті, як інструмент визначення рівня захищеності інформаційних ресурсів, представлені нечіткі моделі на основі лінгвістичної та варіативної бальної шкал. Враховуючи аспекти безпеки інформації та наявні можливості нечітких множин, було вирішено задачу побудови моделей визначення рівня захищеності інформаційних ресурсів. Моделі функціонують на основі даних експертів і результатів опитування користувачів, які проводять оцінку комплексу певних мір захисту. Вибір конкретної з моделей ґрунтується на одному із способів отримання даних від користувачів: відповідей у вигляді бальної або лінгвістичної форми.

Застосування логіко-лінгвістичого підходу в моделях дозволило формалізувати (за допомогою використання лінгвістичних змінних) стан безпеки в системі, який, зазвичай, визначається у лінгвістичній формі. Лінгвістичні змінні використовуються як механізм для опису складної системи з параметрами, які представлені не лише в кількісному, але і в якісному вигляді. Процес оцінювання стану захищеності комп'ютерної системи згідно побудованих моделей складається з наступних етапів: формування еталонних значень, оцінка і формування поточного значення, порівняння отриманого значення з еталонними і формування висновку про стан безпеки інформації. На основі розроблених нечітких моделей та на запропонованій Л.Хоффманом загальній послідовності дій по визначенню рівня безпеки, в результаті проведеного дослідження розроблено структуру системи оцінки стану безпеки інформаційних ресурсів на лінгвістичних та варіативних бальних шкалах.

Реалізація та використання системи оцінки рівня безпеки даних в комп'ютерній системі має вагоме практичне значення, так як з її допомогою можливо «використання» вчасно виявляти (і відповідно при необхідності ліквідовувати) загрози на інформацію за рахунок чого підвищується надійність та захищеність комп'ютерних систем.

Ключові слова: лінгвістичні та варіативні бальні шкали, логіко-лінгвістичний підхід, еталонні значення, захист інформації, комп'ютерні системи.

Вступ. В умовах глобального інформаційного суспільства, проблема захисту інформації відіграє провідну роль. Широка інформатизація всіх сфер життя ставить питання про комплексний підхід до інформаційної безпеки.

Володіння та подальше опрацювання інформації є, для цілого ряду підприємств, основним видом діяльності. Інформація стала об'єктом товарних відносин. Її, як і будь-який інший об'єкт економічних відносин, можна імпортувати, експортувати, купити, продати, вкрасти, сфальсифікувати, знищити, перетворити, спотворити, здійснити над нею інші дії, що матимуть несприятливі результати. Інформаційні системи являють собою основний засіб керування та організації виробництва. Розвиток будь-якого сучасного підприємства залежить від ефективної та надійної підтримки масових та специфічних його зв'язків через глобальні та локальні мережі. Втрата інформації або ж порушення її цілісності та конфіденційності може призвести до значних негативних фінансово-економічних наслідків, в зв'язку з чим, галузь інформаційного захисту привертає до себе все більшої уваги.

Комп'ютеризація інформаційної сфери дала змогу збільшити об'єми оброблюваної інформації, але разом з тим надала нові можливості до порушення безпеки інформаційних ресурсів. Питання захисту інформації в комп'ютерних системах, будучи абсолютно новою, поступово загострювалась з розвитком інформаційних технологій та тотального використання комп'ютерних систем та мереж у всіх галузях життя суспільства.

Повністю забезпечити конфіденційність ресурсу неможливо лише апаратним або ж лише програмним способом, тому для більш ефективного захисту існує потреба об'єднання різних засобів захисту. Крім того, для побудови ефективних систем захисту необхідно дослідити всі можливі шляхи та способи порушення цілісності інформаційних ресурсів, види

атак на ресурси комп'ютерних систем, що дозволить будувати системи захисту вже з урахуванням факторів ризику, за рахунок чого підвищиться ефективність роботи систем захисту.

Постановка задачі. Для надійного захисту, при створенні захисних систем, необхідно враховувати перевірені та випробувані технології. Серед яких: криптографічний захист, що забезпечує конфіденційність, цілісність та доступність інформації, технологія аутентифікації, технології захисту локальних мереж від зовнішніх загроз з боку глобальних мереж та локальних мереж інших організацій, технології захисту від вторгнень, вірусів (в тому числі антивірусна профілактика), інші засоби інформаційного захисту, а також використовувати комплексний підхід до цього питання, що забезпечить раціональне об'єднання зазначених технологій та методів.

Проте, навіть врахування всіх зазначених вище факторів та засобів не забезпечує максимального захисту даних. Серед відомих на сьогодні методів організації систем захисту інформаційних ресурсів і досі немає таких, використання яких забезпечує повну конфіденційність інформації. Отже, на разі постає необхідність пошуку, розробки та реалізації нових методів захисту, а також удосконалення існуючих.

Для забезпечення ефективного вирішення проблеми оцінки захисту інформації в комп'ютерній системі (КС) необхідні спеціальні інтелектуальні засоби. Традиційними математичними методами не завжди можливо ефективно і коректно вирішити дане питання, тому тут доцільніше використовувати методи, основані на нечітких множинах (НМ) та лінгвістичних змінних (ЛЗ), неформальному оцінюванні та пошуку оптимальних рішень.

Стан безпеки в системі характеризується, зазвичай, лінгвістичними даними і для їх формалізації найкраще використовувати поняття ЛЗ. Лінгвістична змінна характеризується набором $(X, T(X), U, G, M)$, 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 $M(X)$. Терми ЛЗ повинні бути впорядковані, а функція належності НМ, що визначає базовий терм повинна задовольняти ряду умов:

- 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: $\forall i = \overline{1,n} \ 0 < \int\limits_x \mu_T(x)dx < \infty$

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.

Нечітка модель з бальною шкалою. Процес оцінювання стану На основі розглянутого підходу та нечітких арифметичних операцій розроблено нечітку модель з бальною шкалою для оцінки рівня захищеності КС на основі даних експертів (еталонних значень) та

результатів опитування користувачів, які проводять оцінку комплексу певних мір захисту. захищеності КС складається з кількох етапів: формування еталонних значень; оцінка і формування поточного значення та порівняння отриманого значення з еталонними й на основі чого формування висновку про рівень захищеності оцінюваної КС. Суть оцінки згідно моделі з бальною шкалою полягає в тому, що користувач відповідає на попередньо ранжовані питання (компоненти експертного запиту) за складеною експертом N-бальною шкалою. Діапазон $[\underline{X}_j, \overline{X}_j](\underline{X}_j = 0, \overline{X}_j = N_j)$ зміни параметру $X_j^*, j = \overline{1,n}$ (N_j – максимально можлива кількість балів по кожному питанню) відображається на множинні еталонних нечітких чисел (НЧ) $U = [0, L-1]$ (L – кількість еталонів), для чого фіксоване значення X_j^* перераховується у відповідний елемент $U_j^* \in [0, L-1]$ за формулою:

$$U_j^* = (L-1)\frac{X_j^* - \underline{X}_j}{\overline{X}_j - \underline{X}_j}. \quad (1)$$

А ФН $\mu_i^j(U_j^*), i = \overline{1,L}$ нечіткого терму з номером i обраховується за допомогою виразу:

$$\mu_i^j(U_j^*) = \left[\frac{1}{1+(U_j^* - i + 1)^2}\right]^{PN_j n}, \quad (2)$$

де $PN_j, j = \overline{1,n}$ – коефіцієнти важливості, обчисленні за оцінками експертів для кожного з компонентів експертного запиту.

На заключній стадії визначається показник рівня захищеності за наступним виразом:

$$\mu_S = (X_j^*) \bigvee_{i=1}^{L} \bigwedge_{j=1}^{n} \mu_i^j, \quad (3)$$

де $i = \overline{1,L}$ – номер терму з базової терм-множини T, а $j = \overline{1,n}$ – номер компоненту експертного запиту. На основі запропонованої нечіткої моделі з бальною шкалою розроблено метод визначення рівня безпеки в КС з варіативною бальною шкалою (рис. 1).

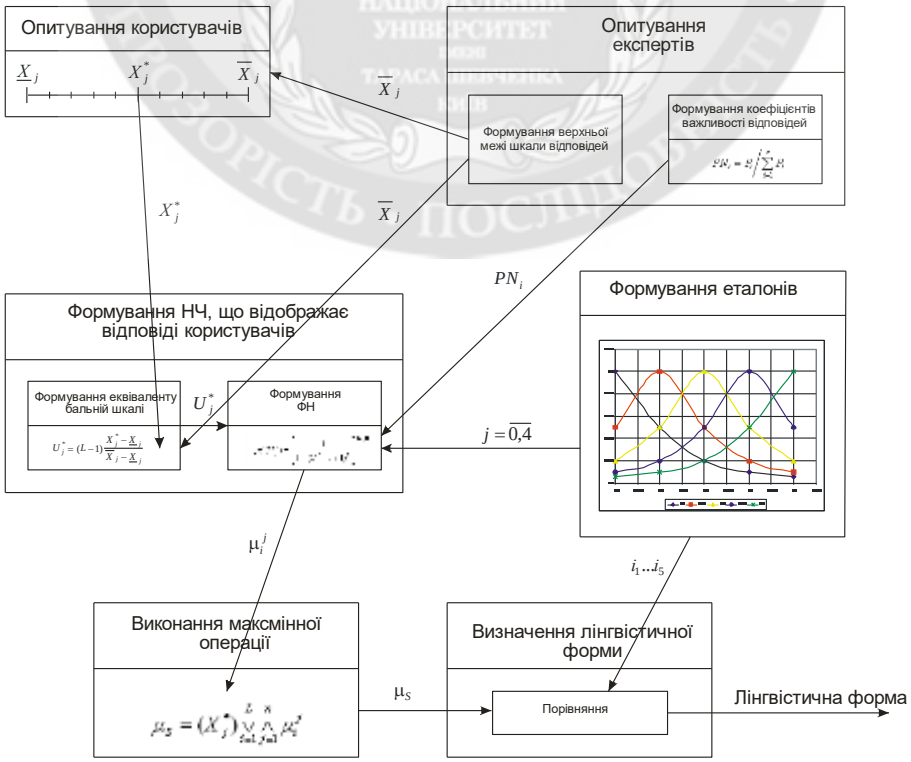

Рис. 1. Метод визначення рівня безпеки КС на моделі з варіативною бальною шкалою

Таким чином першим кроком буде формування нечітких еталонів для відображення ЛЗ “Рівень захисту”. Дану ЛЗ визначаємо у вигляді базової терм множини з п’ятьма нечіткими термами $T=\{T_1,\ T_2,\ T_3,\ T_4,\ T_5\}=$ {“низький”(Н), “нижче середнього” (НС), “середній” (С), “вижче середнього” (ВС), “високий” (В)}, які і будуть прикладом для порівняння НЧ.

Побудову НЧ здійснюємо за методом коректування параметрів, де діапазон зміни носіїв $X_i, i=\overline{1,L}$ буде відображатись на універсальній множині $U=[0,4]$. Отримані в такому випадку еталонні НЧ представлені на рис. 2.

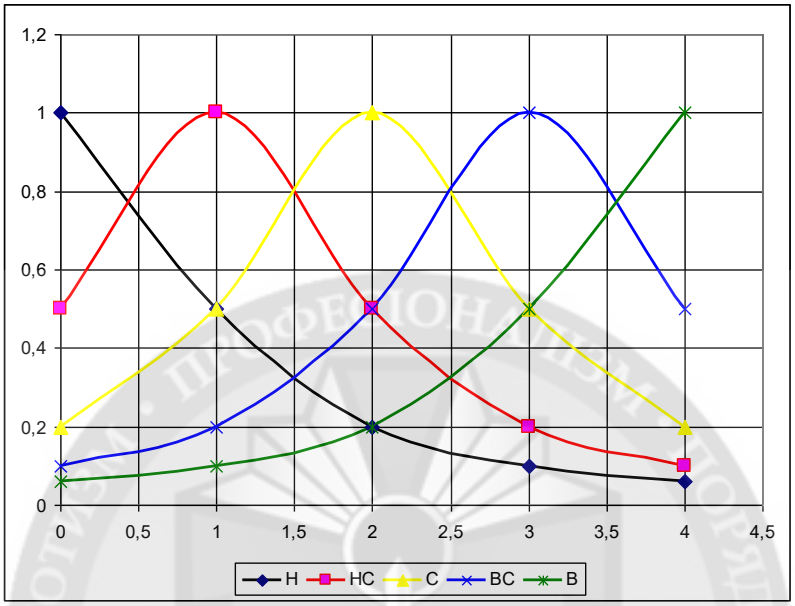

Рис. 2. Еталонні нечіткі числа

Визначення стану безпеки КС реалізовується за результатами опитування користувачів системи відповідно до експертного запиту, компоненти якого попередньо ранжуються через визначення коефіцієнту важливості кожного з компонентів експертного запиту. Для ранжування компонентів складається матриця попарного порівняння $A=\|a_{ij}\|$, яка потім перетворюється за (4)

$$a_{vw}=\begin{cases}100/(a_{ij}+1)*a_{ij}, & \forall i<j:\ \ v=i, w=j;\\ 1, & \forall i<j:\ \ v=w=i=j;\\ 100/(a_{ij}+1), & \forall i<j:\ \ v=j, w=i,\end{cases} \tag{4}$$

де $i=j=\overline{1,n}$ (n – кількість компонентів запиту).

Значення коефіцієнту важливості (КВ) для кожного з компонентів експертного запиту визначається за формулою:

$$P_i=\sum_{j=1}^{n}a_{ij}^{'}\quad \forall i\neq j\,. \tag{5}$$

Після визначення КВ здійснюється їх нормалізація за виразом (6) щоб виконувалась умова (7).

$$PN_i=P_i\Big/\sum_{i=1}^{n}P_i\,, \tag{6}$$

$$\sum_{i=1}^{n}PN_i=1. \tag{7}$$

На основі запропонованої моделі можна визначити оцінку рівня безпеки досліджуваної КС за допомогою даних, отриманих від користувачів у вигляді бальних оцінок на кожен компонент попередньо ранжованого експертного запиту.

Нечітка модель з лінгвістичною шкалою. Суть моделі з лінгвістичною шкалою полягає у тому, що група з N користувачів відповідає на n запитань, відповідно до складеної експертом нечіткої шкали. За відповідями користувачів формується НЧ $Z_t, t=\overline{1,N}$, якому ставиться у відповідність одне з еталонних значень. Значення НЧ, що відповідає оцінці відповідей всієї групи користувачів на певне питання визначається за формулою:

$$L_j = \sum_{t=1}^{N} Z_t \Big/ N, \tag{8}$$

де $\sum_{t=1}^{N} Z_t$ – нечітка сумма, визначенна за методом ЛАЛМ.

Сумарну оцінку безпеки КС визначають з урахуванням раніше обчислених коефіцієнтів важливості:

$$LS = \sum_{j=1}^{n} (PN_j \times L_j). \tag{9}$$

Визначене значення LS порівнюється з еталонними НЧ, для чого використовується метод АУР:

$$d(X,Y) = \Big(\sum_{j=1}^{k}\sum_{i=1}^{m}|x_i - y_i|\Big) \Big/ k, \quad \forall \mu_y \geq \alpha \tag{10}$$

де α – задане значення α-рівня $(0 \leq \alpha \leq 1)$, x_i, y_i – відповідно носії отриманого та еталонного НЧ X та Y, m – кількість компонентів НЧ X, k – кількість компонентів НЧ Y з ФН $\mu_y \geq \alpha$.

Критерієм відповідності LS одному з еталонних НЧ є мінімальне АУР $d\min_i$, яке і визначить рівень захищенності оцінюваної КС:

$$d\min_i = \bigwedge_{j=1}^{n} d(L_i, L_j). \tag{11}$$

Ґрунтуючись на моделі з лінгвістичною шкалою на рис. 3 представлений метод оцінювання стану безпеки інформаційних ресурсів в КС.

Модель з лінгвістичною шкалою дає змогу опрацьовувати вхідні дані, отримані від користувачів у лінгвістичному вигляді, вона є більш точною, проте потребує потужнішого математичного механізму для опрацювання даних.

Висновки. Застосування логіко-лінгвістичого підходу в моделях дозволило формалізувати (за допомогою використання лінгвістичних змінних) стан безпеки в комп'ютерній системі, який, зазвичай, визначається у лінгвістичній формі. Лінгвістичні змінні використовуються як механізм для опису складної системи з параметрами, які представлені не лише в кількісному, але і в якісному вигляді. Процес оцінювання стану захищеності комп'ютерної системи згідно побудованих моделей складається з наступних етапів: формування еталонних значень, оцінка і формування поточного значення, порівняння отриманого значення з еталонними і формування висновку про стан безпеки інформації. На базі побудованих нечітких моделей розроблено методи для визначення стану безпеки досліджуваної комп'ютерної системи. На основі розроблених нечітких моделей та на запропонованій Л.Хоффманом загальній послідовності дій по визначенню рівня безпеки, в результаті проведеного дослідження розроблено структуру системи оцінки стану безпеки інформаційних ресурсів на лінгвістичних та варіативних бальних шкалах.

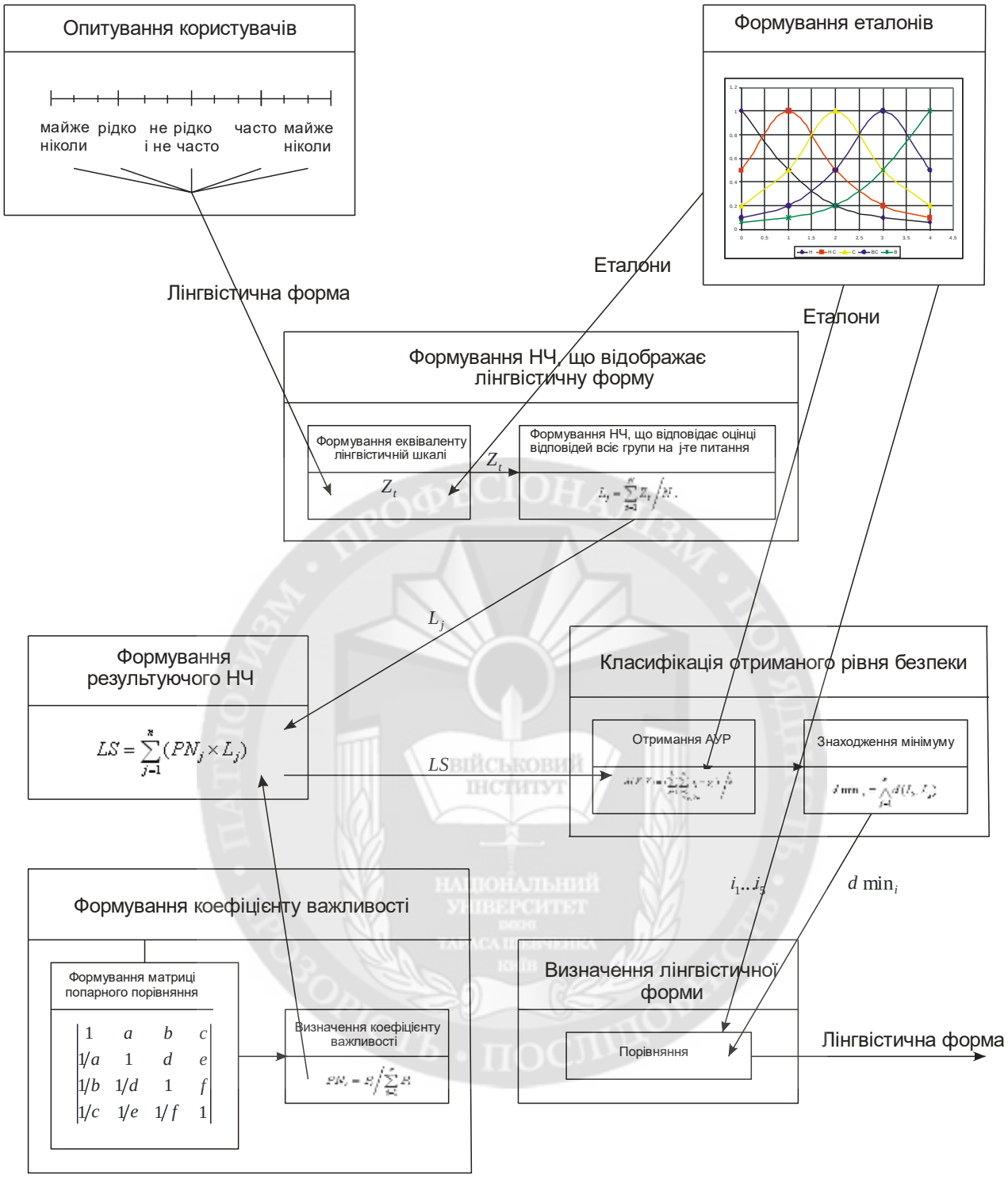

Рис. 3. Схема обробки даних, на основі нечіткої моделі з лінгвістичною шкалою

Реалізація та використання системи оцінки рівня безпеки даних в комп'ютерній системі має вагоме практичне значення, так як з її допомогою можливо «використання» вчасно виявляти (і відповідно при необхідності ліквідовувати) загрози на інформацію за рахунок чого підвищується надійність та захищеність комп'ютерних систем.

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. – 400 с.

5. С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. Методы и средства защиты информации. Несанкционированное получение информации. Монография / – Харьков: ТОВ «Фактор-Друк», 2008. – Том 1. – 464 с.

6. С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. Методы и средства защиты информации. Информационная безопасность. Монография / – Харьков: ТОВ «Фактор-Друк», 2008. – Том 2. – 342 с.

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

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

REFERENCES:

1. O.G. 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, 2001 - 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. S.V. Lenkov, D.A. Peregudov, V.A Khoroshko. Methods of protection means and information.. Unauthorized receipt of information. Monograph / it is Kharkov: TOV «Faktor-Druk», 2008. is Tom 1. – 464 p.

6. S.V. Lenkov, D.A. Peregudov, V.A Khoroshko. Methods of protection means and information.. Unauthorized receipt of information. Monograph / it is Kharkov: TOV «Faktor-Druk», 2008. is Tom 2. – 342 p.

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

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

Рецензент: д.т.н., проф. Замаруєва І.В., Київський національний університет імені Тараса Шевченка

к.т.н.доц. Красильников С.Р., к.т.н. Ленков Е.С., Крижанський Р.А., Мищенко А.А.

ОЦЕНКА СОСТОЯНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ НА ОСНОВЕ ЛИНГВИСТИЧЕСКИХ И ВАРИАТИВНЫХ БАЛЬНЫХ ШКАЛ

В статье, как инструмент определения уровня защищенности информационных ресурсов, представленные нечеткие модели на основе лингвистической и вариативной балльной шкал. Учитывая аспекты безопасности информации и имеющиеся возможности нечетких множеств, была решена задача построения моделей определения уровня защищенности информационных ресурсов. Модели работают на основе данных экспертов и результатов опроса пользователей, которые проводят оценку комплекса определенных мер защиты. Выбор конкретной из моделей основывается на одном из способов получения данных от пользователей: ответов в виде балльной или лингвистической формы.

Применение логико-лингвистичого подхода в моделях позволило формализовать (посредством использования лингвистическох переменных) состояние безопасности в системе,

которое, как правило, определяется в лингвистической форме. Логические переменные используются как механизм для описания сложной системы с параметрами, которые представлены не только в количественном, но и в качественном виде. Процесс оценки состояния защищенности компьютерной системы согласно построенных моделей состоит из следующих этапов: формирование эталонных значений, оценка и формирование текущего значения, сравнение полученного значения с эталонными и формирование заключения о состоянии безопасности информации. На основе разработанных нечетких моделей и на предложенной Л.Хоффманом общей последовательности действий по определению уровня безопасности, в результате проведенного исследования разработана структура системы оценки состояния безопасности информационных ресурсов на лингвистических и вариативных балльной шкале.

Реализация и использование системы оценки уровня безопасности данных в компьютерной системе имеет большое практическое значение, так как с ее помощью возможно «использование» своевременно выявлять (и соответственно при необходимости ликвидировать) угрозы на информацию за счет чего повышается надежность и защищенность компьютерных систем..

Ключевые слова: лингвистические и вариативные балльные шкалы, логико-лингвистический подход, эталонные значения, защита информации, компьютерные системы.

Ph.D. Krasilnikov S.R, Ph.D. Lenkov E.S., Krizhansky R.A., Michenko A.A.

THE ASSESSMENT OF INFORMATION RESOURCES SAFETY BASED ON LINGUISTIC AND VARIABLE POINT SCALES

The fuzzy model which are based on the linguistic and variable grade scale are described in the article as the tool to determine the level of the information resources protection. The problem of constructing models to determine the level of the information resources protection has been sold taking into account the aspects of information security and opportunities of fuzzy sets. The model works on the basis of data experts and survey results from users who are evaluating a set of specific protection measures. The choice of specific models is based on one of the ways of getting data from users: responses in the form of a point or linguistic forms. The use of linguistic-logical approach in models helped to formalize (by the use of logical variables) the security status of the system, which is usually defined in the linguistic form. Logical variables are used as a mechanism for describing a complex system with parameters that are not only quantitative but also in qualitative form. The process of assessing the security state of a computer system consists, according to the constructed models, of the following stages: the formation of the reference values, the evaluation and formation of the current value, comparing the obtained values with the reference and forming conclusions on the state of information security.

The assessment structure system of information resources safety based on a linguistic variable scale has been developed as a result of the study and base on developed fuzzy models and proposed L. Hoffman General procedure for determining the safety level.

The implementation and use of the data security level assessment system in a computer system is of great practical importance, since with it the ability to "use" promptly identify (and thus, if necessary, eliminate) the threat to information thereby increasing the reliability and security of computer systems .

Keywords: linguistic and divergent point scale, logical-linguistic approach, reference values, information security, computer systems.