УДК 621.391

О.Г. Пузиренко[1], О.Ю. Іохов[2], О.М. Горбов[2], І.В. Кузьминич[2]

[1] *Генеральний штаб Збройних Сил України, Київ*
[2] *Академія внутрішніх військ МВС України, Харків*

МОДЕЛІ ЗМЕНШЕННЯ ВПЛИВУ ТА НЕЙТРАЛІЗАЦІЇ ІНФОРМАЦІЙНИХ РИЗИКІВ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В статті розглянуто нелінійна задача, спрощення за рахунок вибору ймовірності. Розроблено алгоритм, в якому передбачена можливість варіації закону розподілу вхідних даних, що дозволяє перейти від кусочно-лінійних до нелінійних функцій, а також можливість оцінки ризиків при різноманітних сценаріях реалізації множини загроз. Проведено кількісну оцінку інформаційних ризиків для конкретної інформаційно-телекомунікаційної системи.

Ключові слова: *інформаційно-телекомунікаційна система, оцінка ризику, нелінійна задача, інформаційна безпека, нечіткі вхідні данні.*

Вступ

Постановка проблеми. Останнім часом у світі спостерігається різке зростання масштабів і складності інформаційно-телекомунікаційних систем (ІТС) та збільшення кількості інформації, що в них циркулює. Відповідно, збільшується кількість вразливостей і загроз інформації (як випадкових, так і умисних), збитків (фінансових та інших) від реалізації цих загроз. Це призводить до зростання інформаційних ризиків. В загальному понятті ризик – це ймовірність загрози. Для мінімізації цих ризиків створюються комплексні системи захисту інформації (КСЗІ) для забезпечення режиму інформаційної безпеки (ІБ). При проектування КСЗІ необхідно мати адекватний апарат оцінки ризиків [1]. На основі результатів кількісної оцінки ризиків здійснюється оптимізація витрат на створення КСЗІ, що обумовлює важливість і актуальність задачі.

При розробці сучасних перспективних систем захисту інформації наразі широко використовується теоретичний апарат експертних систем, теорії нечіткої логіки, нейронних мереж [2]. Врахування ризиків різних типів представляється зручним використанням нечіткої логіки, яка є ефективним засобом моделювання в умовах невизначеності [3]. Перші роботи у сфері ІБ стосувались використання апарату нечіткої логіки для побудови систем захисту інформації [4], систем виявлення атак у обчислювальних мережах, систем оцінки якості функціонування систем захисту інформації в ІТС і т.д. Для оцінки ризиків використання теорії нечітких множин наведено у роботі [5], де показано ефективність методів нечіткої логіки для реалізації розповсюджених методик CRAMM та NIST і запропоновано застосовувати нечіткий логічний вивід для оцінки ризику для окремої загрози, що діє на ІТС. Але відкритим залишено питання оцінки сукупної дії загроз на систему, поза межами алгоритму залишилась проблема отримання вхідних даних та можливість оцінки ризиків при різноманітних сценаріях реалізації множини загроз.

В роботі, яка подавалася на розгляд стипендіальної комісії 2007 року було розроблено алгоритм кількісної оцінки інформаційних ризиків ІТС з використанням методів нечіткої логіки, який дозволив отримати оцінку ризиків для ІТС по всім загрозам моделі загроз. При побудові застосовувались елементи методики CRAMM [5,6]. Були враховані вимоги чинного законодавства [7-14].

Ймовірність реалізації нечіткої події A (P(A)) на множині U, коли P_i – звичайні ймовірності p_i, $0 \le p_i \le 1$, визначалась як [3]

$$P(A) = \mu_A(u_1)p_1 + ... + \mu_A(u_n)p_n , \qquad (1)$$

де $\mu_A(u_i)$ – значення функції належності нечіткої події A в точці універсальної множини u_i.

За умови рівномірного розподілу ймовірностей, функція належності нечіткого числа “Ризик” вважалася розподілом ймовірності реалізації ризику. Це дало можливість оцінити ймовірність втрат системи.

Для оцінки ризику окремої загрози було застосовано нечіткий логічний вивід, який здійснював перетворення значень двох вхідних величин “Ймовірність реалізації загрози” та “Збитки від реалізації” у вихідну величину “Ризик”, на базі робіт [5,15]. Оцінка сукупного ризику обчислювалась по формулі повної ймовірності.

Алгоритм було програмно реалізовано з використанням засобів Fuzzy Logic Toolbox математичного пакету MATLAB.

Отримані в ході роботи результати дозволили поставити наступні задачі, які необхідно розв’язати для підвищення ефективності кількісної оцінки ризиків:

реалізувати можливість обробки вхідних даних, представлених не числами, а масивами чисел, які описують розподіли ймовірностей;

мінімізувати середньоквадратичне відхилення сукупного ризику, отриманого в результаті оцінки, від заданого при постановці задачі;

створити програму, яка реалізує вказані зміни алгоритму.

Основний матеріал

Згідно поставленій задачі, її розв'язок можна розбити на три частини: забезпечення обробки нечітких вхідних даних, мінімізація середньоквадратичного відхилення сукупного отриманого ризику від заданого, програмна реалізація алгоритму засобами MATLAB.

Реалізація обробки системою нечітких вхідних даних

Обробка нечітких вхідних даних дозволяє розглядати реалізацію ієрархічних нечітких систем [15]. Використання таких систем відкриває можливість застосування системного підходу при оцінці інформаційних ризиків, запропонованого в [17]. Він полягає у переході від сукупної оцінки ризику для всієї системи до оцінки ризиків її складових частин. Так, у нормативних документах технічного захисту інформації (НД ТЗІ) [9-12], вводиться класифікація загроз по результатам дії загрози на кожну властивість інформації окремо: конфіденційність, цілісність, доступність і спостережність. В НД ТЗІ [11] вводиться поняття набору функціональних послуг захисту (ФПЗ), які забезпечують реалізацію кожної з властивостей інформації. Загрозами, в такій трактовці, є некоректне функціонування одної чи декількох ФПЗ. Введення понять засобів і механізмів захисту є наступним збільшенням деталізації поняття загрози. Приклад ієрархічної класифікації загроз у вигляді дерева логічного виводу наведено на рис. 1, де: R – корінь дерева, сукупний інформаційний ризик ІТС; x_i – термінальні вершини, які ілюструють ризики порушення функціонування окремих ФПЗ; f_i – нетермінальні вершини ілюструють нечіткий логічний вивід; дуги графа, які виходять з нетермінальних вершин, ілюструють ризики реалізації загроз по окремим властивостям інформації. Використання нечіткої ієрархічної системи дозволяє спростити процес оцінки ризиків, зробити його більш прозорим, а також чітко визначити критичні фактори, тощо.

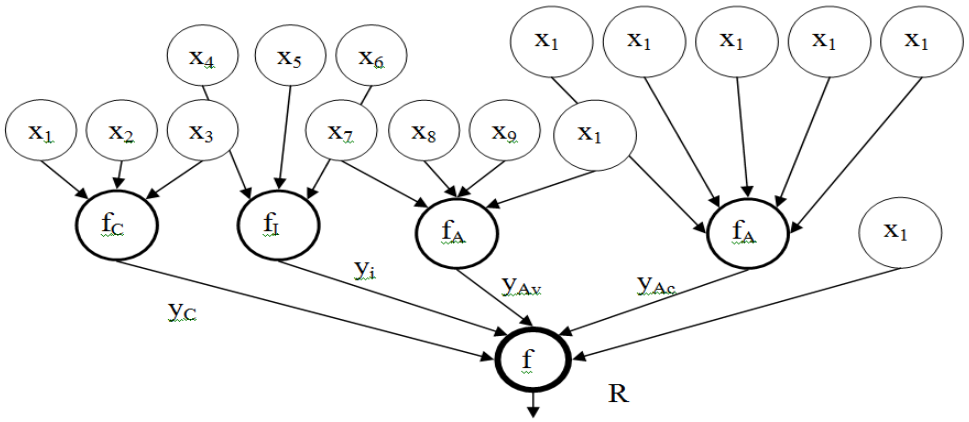

Рис. 1. Ієрархічна класифікація загроз, які формують значення сукупного ризику

На етапі фаззифікації нечіткого логічного виводу ступені належності входів до термів нечіткої бази знань розраховуються по-різному для чітких і нечітких вхідних значеннях. При нечітких вхідних даних необхідно визначити ступінь належності одної нечіткої множини $\tilde{X}$ (значення вхідної змінної) до іншої нечіткої множини $\tilde{Y}$ (терми з бази знань). Ступінь належності запропоновано розраховувати як висоту перетину цих нечітких множин (рис. 2) [15].

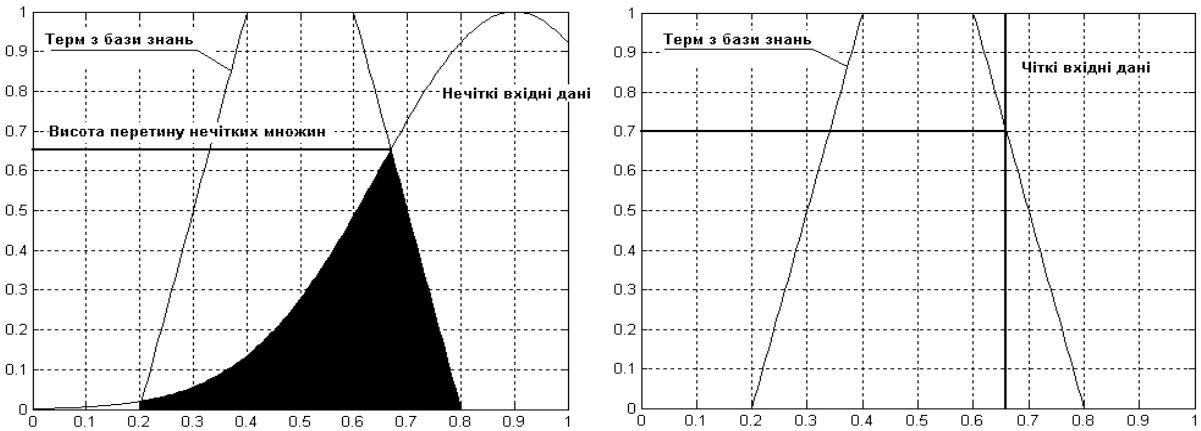

Рис. 2. Ступені належності входів до термів нечіткої бази знань при чітких і нечітких вхідних даних

Розроблено алгоритм нечіткого логічного виводу з забезпеченням перевірки і перетворення вхідних даних у відповідності до запропонованого підходу, що дозволяє розширити можливості алгоритму. Якщо раніше на вхід подавалася пара чисел, які відповідали значенням ймовірності реалізації загрози та збитків від її реалізації, то тепер алгоритм може працювати з нечіткими, а, отже у відповідності до формули (1), ймовірнісними вхідними даними.

Розроблений алгоритм дозволяє робити оцінку ризиків в умовах невизначеності, оперуючи лінгвістичними змінними, також алгоритм дозволяє обробляти різні комбінації нечітких і чітких вхідних даних.

Мінімізація середньоквадратичного відхилення сукупного ризику, отриманого в результаті оцінки, від заданого при постановці задачі

Від виду функцій належності термів вхідних і вихідних змінних залежить результат аналізу ризиків, але вибір цих характеристик не формалізовано і задача не є однозначною. Обраним варіантом її розв'язання на основі робіт [6] є адаптація системи нечіткого логічного виводу, шляхом формування функцій належностей на основі апріорної інформації (тестової вибірки), яка ставить у відповідність окремим значенням ймовірності реалізації загрози та збитків від її реалізації значення ризику для даної системи. Ці залежності можуть бути результатами збору статистики, попередніх експериментів, експертних оцінок, тощо.

Проведення адаптації системи кількісної оцінки ризиків реалізується поетапно. Попередньо формуються початкові шкали вхідних і вихідних змінних з рівномірним розташуванням функцій належності термів. Адаптація здійснюється для вхідної шкали збитків від реалізації загроз з наступних міркувань: формування цієї шкали найменш формалізовано і більше за інші залежить від ІТС; адаптація за однією шкалою зменшує складність процедури порівняно з використанням більшої кількості змінних. Оптимізація системи оцінки ризиків реалізується ітеративним алгоритмом за критерієм мінімального квадратичного відхилення [15]:

$$\mathrm{RMSE} = \sqrt{\frac{1}{M}\sum_{r=1}^{M}(y_r - F(P, X_r))^2} \to \min, \qquad (2)$$

де M – кількість пар значень (X_r, y_r) навчальної вибірки, $X_r = (x_{r1}, x_{r2})$ – вхідний вектор в r-й парі даних навчальної вибірки, y_r - відповідний X_r вихід, P – вектор параметрів функцій належності термів вхідних і вихідної змінної, шукомий в нашому випадку, $F(P, X_r)$ – результат нечіткого логічного виводу Мамдані з параметром P при значеннях входів X_r.

Програмну реалізацію даного алгоритму здійснено засобами Optimization Toolbox пакету MATLAB. Програму застосовано для адаптації системи оцінки ризиків для заданої множини загроз ІТС. Середньоквадратичне відхилення до і після адаптації наведене на рис. 3.

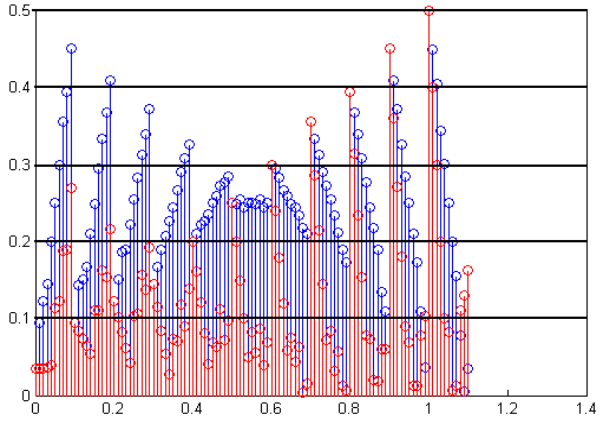

Рис. 3. Середньоквадратичне відхилення до і після адаптації

Аналіз отриманих результатів показав ефективність написаної програми для адаптації системи кількісної оцінки ризиків ІТС до заданої множини загроз. Програма дозволяє змінювати параметри системи нечіткого логічного виводу у відповідності до поставлених умов. Для заданої ІТС досягнуто зменшення середньоквадратичного відхилення в середньому в 2.5 – 3 рази (рис.3).

Програмна реалізація

У роботі здійснено програмну реалізацію алгоритму на основі засобів Fuzzy Logic Toolbox математичного пакету MATLAB. Для підвищення ефективності роботи з програмним продуктом було створено інтерфейсне вікно, яке дає можливість аналітику задавати значення вхідних змінних, параметри системи нечіткого логічного виводу, параметри адаптації системи, а також відображає результати оцінки ризиків і адаптації системи.

Для демонстрації можливостей програми проведено оцінку ризиків ІТС, що складається з комп'ютера, підключеного до глобальної інформаційно-комунікаційної мережі за допомогою Wi-Fi.

Оцінку вартості обладнання та інформації здійснено у нормованій шкалі. Модель порушника сформовано відповідно до рекомендацій [17]. Список основних загроз і ризиків для компонентів ІТС складено згідно стандарту [18]. На основі обраної моделі порушника було сформовано модель загроз, яка включала в себе числа – ймовірності реалізації кожної загрози та збитки від їхньої реалізації. При моделюванні загроз були враховані такі загрози:

1. Радіоперехоплення (eavesdropping).
2. Несанкціонований доступ (unauthorized access).
3. "Забиття" каналу завадами (interference and jamming).
4. Силовий деструктивний вплив (СДВ).
5. Неправильне конфігурування (mis-configuration).

Для оцінки ймовірностей реалізації загроз використовувалися статистичні дані CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 2006 та LODOGA, дані документації на прилади, дані постачальника послуг. Приклад нечіткого логічного виводу для загрози №1, якщо ймовірність її реалізації описується функцією Гауса з середнім значенням 0.15 і дисперсією 0.1, а збитки від її реалізації оцінено лінгвістичною змінною "більш-менш нехтовні" наведено на рис. 4. Чітке та нечітке значення ризику для ІТС по всім загрозам, отримане у результаті розрахунків, разом з інтерфейсним вікном програми наведено на рис. 5. Отримані результати знаходяться у відповідності з експертними оцінками для даної ІТС.

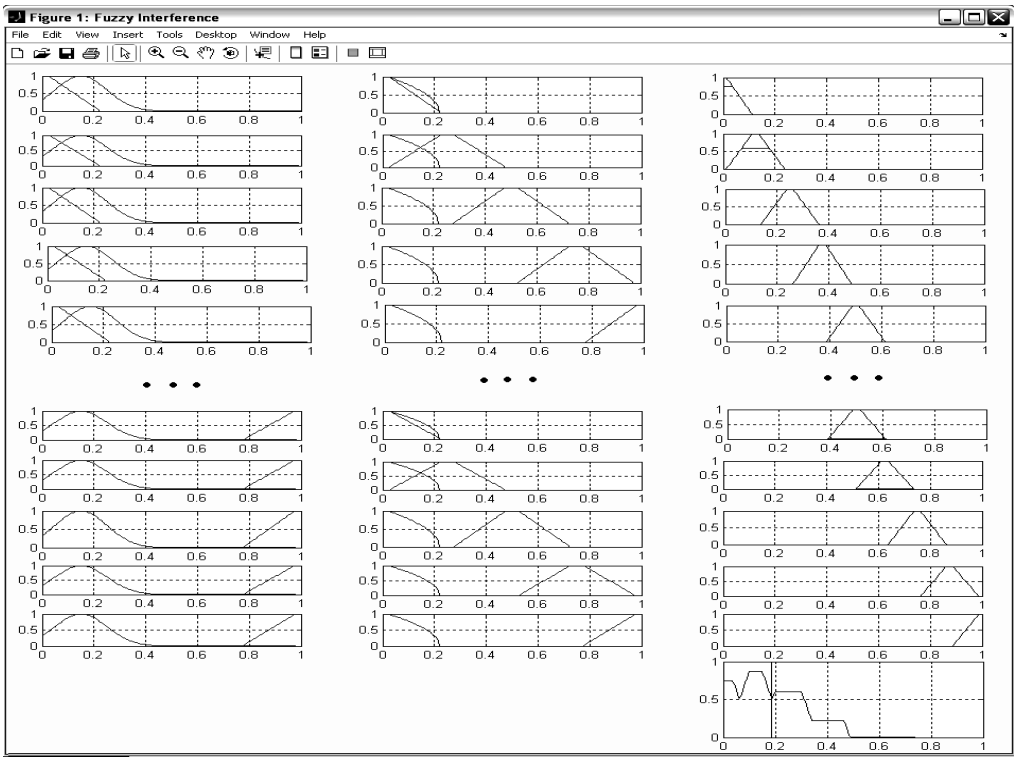

Рис. 4. Вікно нечіткого логічного виводу для загрози №1

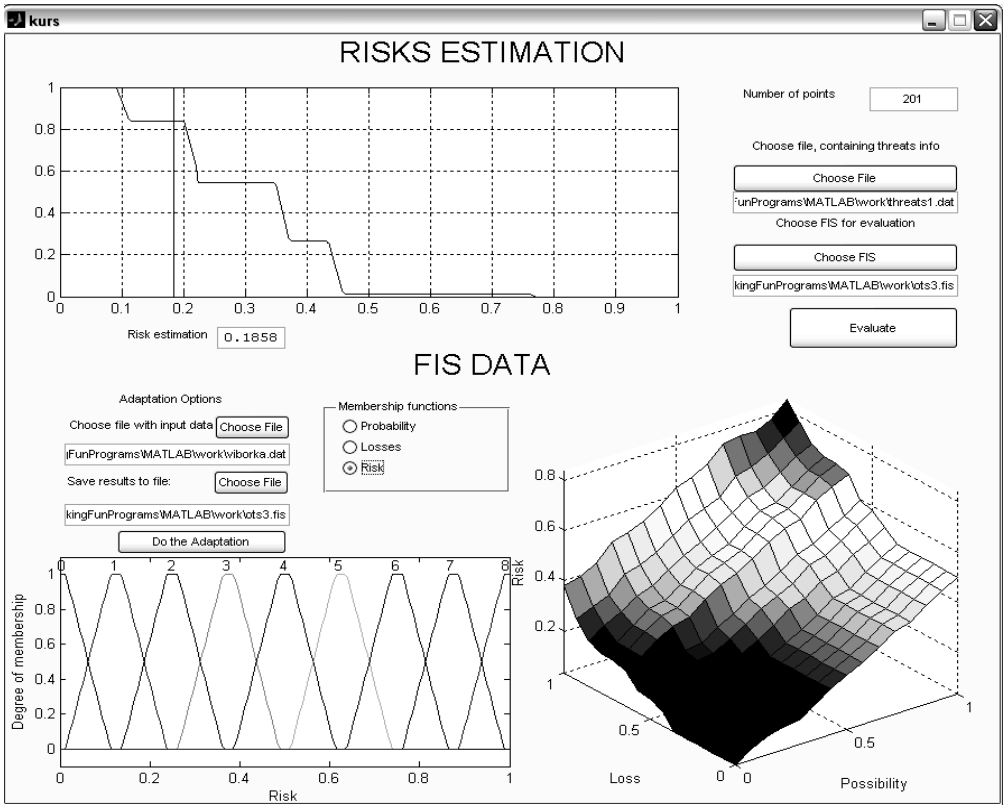

Рис. 5. Чітке та нечітке значення ризику для ІТС по всім загрозам у інтерфейсному вікні програми

Висновки

В даній статті розглянуто нелінійна задача, на першому етапі розв'язання якої вводяться спрощення за рахунок вибору ймовірності. В результаті роботи, розроблено алгоритм, в якому передбачена можливість варіації закону розподілу вхідних даних, що дозволяє перейти від кусочно-лінійних до нелінійних функцій, а також можливість оцінки ризиків при різноманітних сценаріях реалізації множини загроз. Здійснено програмну реалізацію алгоритму засобами MATLAB. Для широкого використання програми розроблено зручний інтерфейс, який дозволяє легко її використовувати для розв'язання практичних задач в області інформаційної безпеки інформаційно-телекомунікаційних систем.

Проведено кількісну оцінку інформаційних ризиків для конкретної ІТС. Отримані результати відповідають поставленій задачі і корелюють з експертними оцінками для даної ІТС.

На наступному етапі роботи планується реалізація нечіткої ієрархічної системи оцінки ризиків, розробка алгоритму оптимізації витрат на систему захисту для заданого режиму інформаційної безпеки ІТС.

Список літератури

1. К разработке модели адаптивной защиты информации / Г.Ф. Нестерук, А.А. Молдовян, Л.Г. Осовецкий, Ф.Г. Нестерук; Р.Ш. Фархутдинов // Вопросы защиты информации. – 2005. – № 3. – С. 11 – 16.

2. Суханов А.В. Представление знаний в адаптивных средствах мониторинга ИС / А.В. Суханов, А.А. Павлютенков // Защита информации. Инсайд. – 2008. – № 4. – С. 64 – 68.

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

4. Корченко А.Г. Построение систем защиты информации на нечетких множествах / А.Г. Корченко. – К.: МК-Пресс, 2006. – 316 с.

5. Балашов П.А. Оценка рисков информационной безопасности на основе нечеткой логики / П.А. Балашов, Р.И. Кислов, В.П. Безгузиков // Конфидент. – 2003. – 53, № 4. – С. 56 – 60; 54, № 6. – С. 60 – 66.

6. Архипов А.Е. Сравнение количественных оценок рисков при использовании теории нечетких множеств / А.Е.Архипов, С.М. Кущ, В.О. Шутовский // Технології безпеки інформації. – К.: 2007. – С. 30.

7. Закон України "Про інформацію". Введено в дію постановою Верховної Ради України від 02.10.92 р. № 2658-XII .

8. Закон України "Про захист інформації в автоматизованих системах". Введено в дію постановою Верховної Ради України від 05.07.94 р. № 80/94.

9. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

10. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

11. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

12. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

13. НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

14. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

15. Штовба С.Д. Проектирование нечетких систем средствами MATLAB / С.Д. Штовба. – М.: Горячая линия – Телеком, 2007. – 288 с.

16. Домарев В.В. Безопасность информационных технологий. Системный поход / В.В. Домарев. – К.:ООО ТИД «Диасофт», 2004. – 992 с.

17. ISO/IEC FDIS 18028-1.

Надійшло до редколегії 1.02.2013

Рецензент: д-р техн. наук проф. О.О. Морозов, Академія внутрішніх військ МВС України, Харків.

МОДЕЛИ УМЕНЬШЕНИЯ ВЛИЯНИЯ И НЕЙТРАЛИЗАЦИИ ИНФОРМАЦИОННЫХ РИСКОВ В ИНФОРМАЦИОННО ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А.Г. Пузыренко, А.Ю. Иохов, А.М. Горбов, И.В. Кузьминич

В статье рассмотрена нелинейная задача, упрощения за счет выбора вероятностей. Разработан алгоритм, в котором предусмотрена возможность вариации закона распределения входных данных, что позволяет перейти от кусочно-линейных до нелинейных функций, а также возможность оценки рисков при разнообразных сценариях реализации множества угроз. Проведена количественная оценка информационных рисков для конкретной информационно-телекоммуникационной системы

Ключевые слова: *информационно телекоммуникационная система, оценка риска, нелинейная задача, информационная безопасность, нечеткие входные данные*

IDENTIFICATION OF WAYS TO BUILD AN ADVANCED MOBILE RADIO SYSTEM OF INTERIOR TROOPS OF THE MINISTRY OF INTERIOR AFFAIRS OF UKRAINE

O.G. Puzyrenko, O.Y. Iohov, A.M. Gorbov, I.V. Kuzminich

In article the nonlinear task, simplifications at the expense of a choice of probabilities is considered. The algorithm in which possibility of a variation of the law of distribution of entrance data is provided that allows to pass from piecewise and linear before nonlinear functions, and also possibility of an assessment of risks at various scenarios of realization of a set of threats is developed. The quantitative assessment of information risks for concrete information and telecommunication system is carried out

Keywords: *informatively telecommunication system, risk estimation, nonlinear task, informative safety, unclear detains.*