



МІНІСТЕРСТВО
ЕКОНОМІЧНОГО
РОЗВИТКУ І ТОРГІВЛІ
УКРАЇНИ

УКРАЇНА

(19) **UA** (11) **119265** (13) **U**
(51) МПК (2017.01)
G05B 13/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

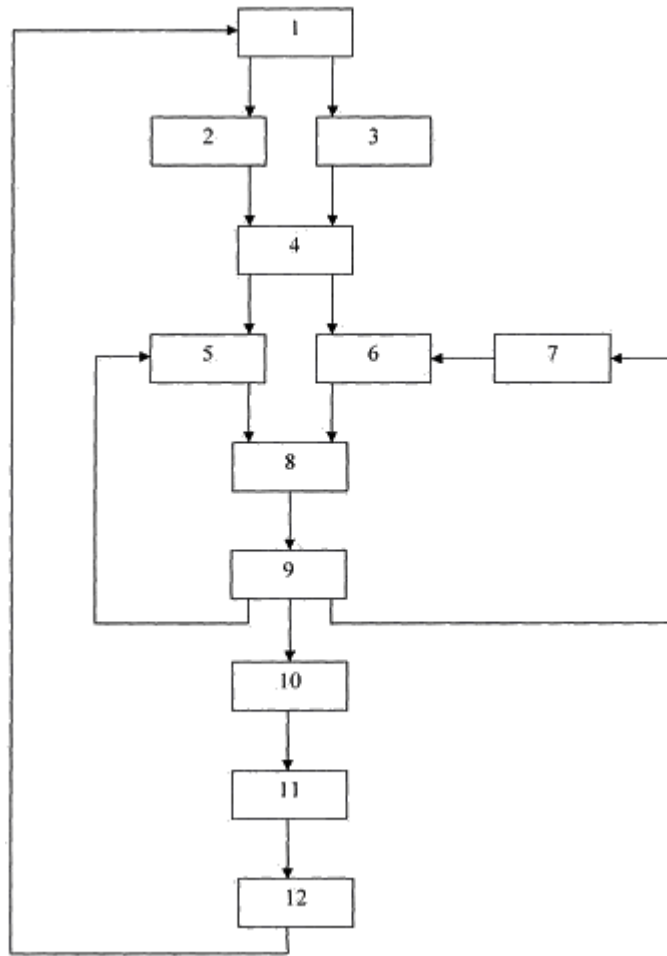
(21) Номер заявки: u 2016 13344	(72) Винахідник(и): Баришев Юрій Володимирович (UA)
(22) Дата подання заявки: 26.12.2016	(73) Власник(и): ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ, Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)
(24) Дата, з якої є чинними права на корисну модель: 25.09.2017	
(46) Публікація відомостей про видачу патенту: 25.09.2017, Бюл.№ 18	

(54) СИСТЕМА АДАПТИВНОГО КЕРУВАННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

(57) Реферат:

Система адаптивного керування інформаційною безпекою містить об'єкт керування, з'єднаний з блоком визначення експертних знань, редактор системи правил висновування, блок отримання чітких вхідних даних, вхід якого є виходом об'єкта керування, а його виходи, як і виходи блока визначення експертних знань, з'єднані з блоком перетворення вхідної інформації, а також блок виконання. Додатково в систему введено нейронну мережу, вхід якої з'єднано з виходом блока перетворення вхідної інформації; базу знань, входи якої з'єднано з виходом блока перетворення вхідної інформації та виходом редактора системи правил висновування; блок перевірки адекватності, входами якого є виходи нейронної мережі та бази знань; блок адаптації, входом якого є вихід блока перевірки адекватності, а виходи з'єднано з редактором системи правил висновування, нейронною мережею та блоком керування; блок індикації, входом якого є вихід блока керування, вихід якого з'єднано з блоком виконання, а його вихід є входом об'єкта керування.

UA 119265 U



Корисна модель належить до систем керування об'єктами, а саме до систем керування системами захисту інформації.

Відома система керування параметрами організації [Патент України №9181, м. кл. G05B 13/00, від 15.09.2005, бюл. №9 2005 р.], що містить об'єкт керування, з'єднаний з вимірником параметрів об'єкта керування, виходи якого з'єднані з редактором функцій належності, вихід якого є входом блоку прийняття рішення, редактор правил системи нечіткого виводу, виходи якого з'єднані з блоком прийняття рішення, блок керування, з'єднаний з блоком прийняття рішення, причому блок прийняття рішення реалізовано на основі апарата нечіткої логіки.

Недоліком такої системи є зниження якості прийнятих рішень з плином часу внаслідок відсутності адаптивності до зміни умов оточуючого середовища.

Найбільш близьким до системи, що заявляється, є система оптимізації комплексної безпеки об'єкту [Патент України № 29269, м.кл. G05B 13/00, від 10.01.2008, бюл. №1 2008р.], що містить об'єкт оптимізації комплексної безпеки, в подальшому об'єкт керування, з'єднаний з блоком визначення експертних знань, блок прийняття рішення, в подальшому база знань, реалізований на основі апарата нечіткої логіки, редактор правил системи нечіткого виводу, в подальшому редактор системи правил висновування, з'єднаний з базою знань, причому введено блок отримування чітких вхідних даних, вхід якого є виходом об'єкта оптимізації комплексної безпеки, виходи якого, як і виходи блока визначення експертних знань, з'єднані з блоком перетворення, в подальшому блоком перетворення вхідної інформації, виходи якого з'єднані з блоком оцінювання захищеності об'єкта, вихід блока оцінювання захищеності об'єкта з'єднано з блоком визначення рангів, виходи якого є входами блока прийняття рішення та блока оцінювання захищеності об'єкта, виходи блока прийняття рішення з'єднані з блоком виконання.

Недоліком найближчого аналога є зниження якості прийнятих рішень за умов зміни сили впливу вхідних параметрів та появи нових параметрів таких як нові загрози інформації або нові засоби й заходи для забезпечення її безпеки, що притаманно для предметної області, де застосовується така система.

В основу корисної моделі поставлено задачу створення системи адаптивного керування інформаційною безпекою, в якій за рахунок введення нових елементів та зв'язків, підвищується якість керування.

Поставлена задача вирішується тим, що система адаптивного керування інформаційною безпекою, що містить об'єкт керування, з'єднаний з блоком визначення експертних знань, редактор системи правил висновування, блок отримування чітких вхідних даних, вхід якого є виходом об'єкта керування, а його виходи, як і виходи блока визначення експертних знань, з'єднані з блоком перетворення вхідної інформації, а також блок виконання, нейронну мережу, вхід якої з'єднано з виходом блока перетворення вхідної інформації; базу знань, входи якої з'єднано з виходом блока перетворення вхідної інформації та виходом редактора системи правил висновування; блок перевірки адекватності, входами якого є виходи нейронної мережі та бази знань; блок адаптації, входом якого є вихід блока перевірки адекватності, а виходи з'єднано з редактором системи правил висновування, нейронною мережею та блоком керування; блок індикації, входом якого є вихід блока керування, вихід якого з'єднано з блоком виконання, а його вихід є входом об'єкта керування.

На кресленні представлено схему системи адаптивного керування інформаційною безпекою.

Система містить об'єкт керування 1, виходи якого з'єднані з блоком отримування чітких вхідних даних 2 та блоком визначення експертних знань 3, виходи яких з'єднані блоком перетворення вхідної інформації 4. Виходи блока перетворення вхідної інформації 4 є входами нейронної мережі 5 та бази знань 6. Також до складу системи входить редактор системи правил висновування 7, виходи якого з'єднані з нечіткою базою знань 6. Виходи нейронної мережі 5 та бази знань 6 є входами для блока перевірки адекватності моделей 8, блоком адаптації 9, вихід якого з'єднано з нейронною мережею 5, редактором системи правил висновування 7 та блоком керування 10. Вихід блока керування 10 з'єднано з блоком індикації 11. Вихід блока індикації 11, з'єднано з блоком виконання 12, вихід якого з'єднано з об'єктом керування 1.

Система адаптивного керування інформаційною безпекою виконується таким чином. З блока отримування чітких вхідних даних 2 отримують інформацію про поточний стан параметрів об'єкта керування 1, виражених чисельно. Параметри об'єкта керування 1, які неможливо виразити чисельно, визначають за допомогою блока визначення експертних знань 3, шляхом залучення експертів, які виражають свої знання за допомогою лінгвістичних термів. Всі дані, отримані як в чіткому, так і в нечіткому вигляді, надсилають до блока перетворення вхідної інформації 4, де вхідну інформацію з блока отримування чітких вхідних даних 2 та з блока визначення експертних знань 3 перетворюють в уніфікований нечіткий вигляд і надсилають до

входів нейронної мережі 5 та бази знань 6, яку попередньо формують за допомогою редактора системи правил висновування 7, де визначають загальний стан інформаційної безпеки об'єкта керування 1 та вплив значень його параметрів на його загальний стан. Результати, отримані з нейронної мережі 5 та бази знань 6, порівнюють, за допомогою блока перевірки адекватності 8, де перевіряють відповідність отриманих результатів одне одному. У випадку, коли рівень невідповідності між отриманими результатами більше максимально допустимого за допомогою блока адаптації 9 генерують керуючий сигнал для редагування бази знань 6 за допомогою редактора системи правил висновування 7 із залученням експертів, після чого знову визначають загальний стан об'єкта керування 1 та вплив значень його параметрів на його загальний стан за допомогою бази знань 6 та знову порівнюють, отримані результати за допомогою блока перевірки адекватності 8. У випадку, коли рівень невідповідності між отриманими результатами залишається більше максимально допустимого за допомогою блока адаптації 9 генерують керуючий сигнал для навчання нейронної мережі 5, а до блока керування 10 надсилають сигнал, отриманий за допомогою бази знань 6. У випадках, коли рівень невідповідності між отриманими результатами з нейронної мережі 5 та бази знань 6 нижче максимального допустимого до блока керування 10 надсилають обидва результати. За допомогою блока керування 10 визначають можливі керуючі дії, а також порівнюють стан об'єкта керування 1 з мінімальним допустимим значенням. У випадку, коли стан об'єкта керування 1 є задовільним за допомогою блока індикації 11 виводять можливі керуючі дії із зазначенням того, що поточний стан об'єкта є задовільним, при цьому за допомогою блока виконання 12 не виконують керуючі дії, спрямовані на зміну параметрів об'єкта керування 1. Коли загальний стан об'єкта керування 1 гірший за мінімальне допустиме значення, то керуючі дії, виведені за допомогою з блока індикації 11, надсилають до блока виконання 12, за допомогою якого ці керуючі дії впроваджують на об'єкті керування 1.

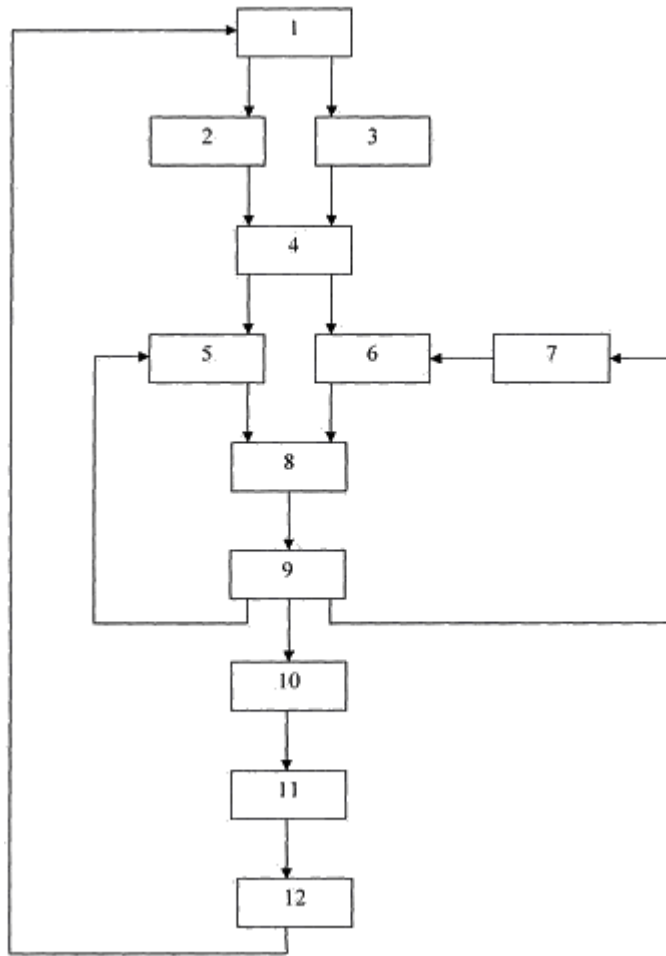
25

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Система адаптивного керування інформаційною безпекою, що містить об'єкт керування, з'єднаний з блоком визначення експертних знань, редактор системи правил висновування, блок отримання чітких вхідних даних, вхід якого є виходом об'єкта керування, а його виходи, як і виходи блока визначення експертних знань, з'єднані з блоком перетворення вхідної інформації, а також блок виконання, яка **відрізняється** тим, що в неї введено нейронну мережу, вхід якої з'єднано з виходом блока перетворення вхідної інформації; базу знань, входи якої з'єднано з виходом блока перетворення вхідної інформації та виходом редактора системи правил висновування; блок перевірки адекватності, входами якого є виходи нейронної мережі та бази знань; блок адаптації, входом якого є вихід блока перевірки адекватності, а виходи з'єднано з редактором системи правил висновування, нейронною мережею та блоком керування; блок індикації, входом якого є вихід блока керування, вихід якого з'єднано з блоком виконання, а його вихід є входом об'єкта керування.

30

35



Комп'ютерна верстка Л. Ціхановська

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601