УКРАЇНА

(19) UA (11) 60550 (13) U

(51) МПК (2011.01)
G05B 13/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ
НА КОРИСНУ МОДЕЛЬ

видається під
відповідальність
власника
патенту

(54) СИСТЕМА КЕРУВАННЯ СТАНОМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

(21) u201013608
(22) 16.11.2010
(24) 25.06.2011
(46) 25.06.2011, Бюл.№ 12, 2011 р.
(72) ДУДАТЬЄВ АНДРІЙ ВЕНІАМІНОВИЧ, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(57) Система керування станом інформаційної безпеки, що містить об'єкт захисту, виходи якого з'єднані з блоком отримування чітких вхідних даних та блоком визначення експертних знань, виходи яких з'єднані з блоком перетворення, вихід якого з'єднано з блоком оцінювання стану інформаційної безпеки об'єкта, блок виконання, блок індикації, вихід якого з'єднано з блоком виконання, вихід якого з'єднано з об'єктом захисту, яка **відрізняється** тим, що введено блок визначення комплексу засобів захисту інформації, блок визначення ефективності засобів захисту інформації, блок визначення вартості засобів захисту інформації, блок визначення найкращого набору засобів захисту інформації, блок визначення критеріїв оптимізації, вихід блока оцінювання стану інформаційної безпеки об'єкта є входом блока визначення комплексу засобів захисту інформації, вихід якого з'єднано з входами блока визначення ефективності засобів захисту інформації та блока визначення вартості засобів захисту інформації, перший вихід блока визначення ефективності засобів захисту інформації є входом блока перетворення, другий вихід блока визначення ефективності засобів захисту інформації є першим входом блока визначення найкращого набору засобів захисту інформації, другим входом якого є вихід блока визначення вартості засобів захисту інформації, третім входом блока визначення найкращого набору засобів захисту інформації є вихід блока визначення критеріїв оптимізації, вихід блока визначення найкращого набору засобів захисту інформації є входом блока індикації.

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

Відома система оптимізації комплексної безпеки об'єкта [Патент України №29269 від 10.01.2008 р., М. кл. G05B 13/00, бюл. №1, 2008 р.], що містить об'єкт оптимізації комплексної безпеки, з'єднаний з блоком визначення експертних знань, блок прийняття рішення, реалізований на основі апарата нечіткої логіки, редактор правил системи нечіткого виводу, з'єднаний з блоком прийняття рішення, згідно з корисною моделлю, введено блок отримування чітких вхідних даних, вхід якого є виходом об'єкта оптимізації комплексної безпеки, а виходи якого, як і виходи блока визначення експертних знань, з'єднані з блоком перетворення, 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 аналога є низька якість прийнятих рішень, що пов'язана з відсутністю врахування наявних ресурсів підприємства, наслідком чого може бути запропоновано рішення, виконання якого неможливо для конкретної організації через недостатню кількість ресурсів, необхідних для впровадження даного рішення.

Найбільш близьким до системи, що заявляється, є система керування параметрами організації [Патент України №35528 від 25.09.2008 р., М. кл. G05B 13/00, бюл. №18, 2008 р.], що містить об'єкт керування, в подальшому об'єкт захисту, виходи якого з'єднані з блоком отримування чітких вхідних даних та блоком визначення експертних знань, виходи яких з'єднані з блоком перетворення, виходи якого з'єднані з блоком оцінювання стану об'єкта, в подальшому блоком оцінювання стану інформаційної безпеки об'єкта, блок прийняття рішення, блок виконання, блок керування, входом якого є вихід блока прийняття рішення, блок індикації, входом якого є вихід блока керування, вихід блока індикації з'єднано з блоком виконання, вихід якого з'єднано з об'єктом захисту,

(19) UA (11) 60550 (13) U

вихід блока керування з'єднано з блоком оцінювання стану інформаційної безпеки об'єкта.

Недоліком прототипу є низька якість прийнятих рішень, що пов'язана з відсутністю оптимізації рішення за критерієм його вартості, а також відсутністю двокритеріальної оптимізації.

В основу корисної моделі поставлено задачу створення системи керування станом інформаційної безпеки, яка за рахунок введення нових елементів та зв'язків приводить до підвищення якості керування за рахунок вибору найкращого рішення відповідно до критеріїв максимального стану інформаційної безпеки та мінімальної вартості рішення.

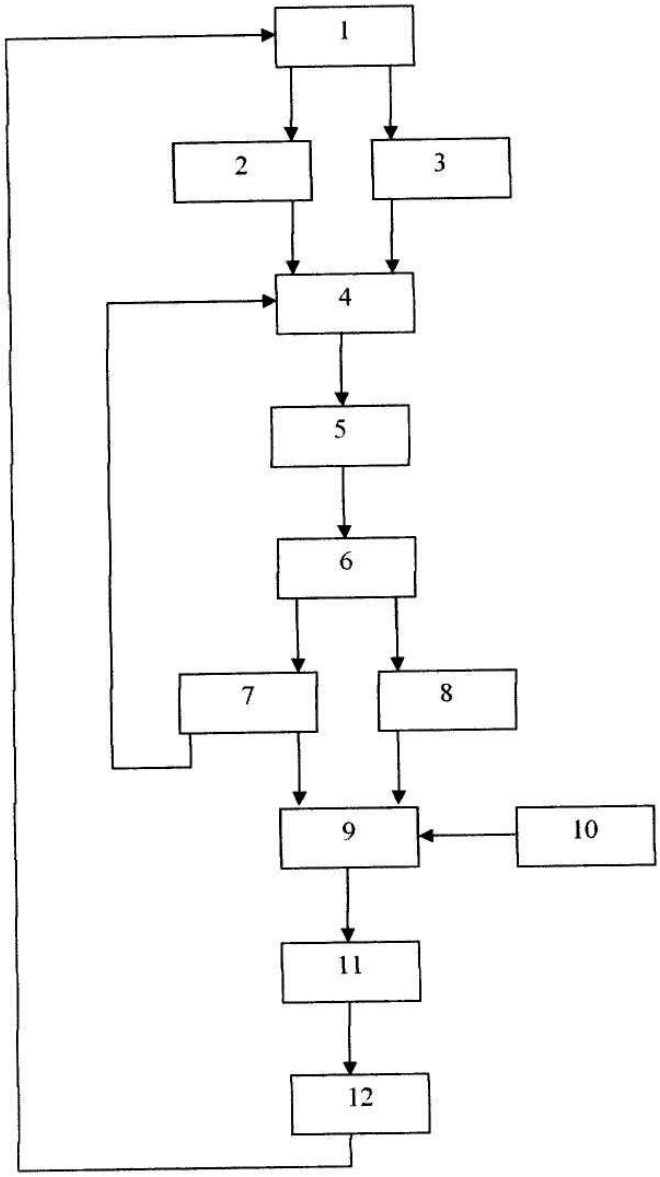
Поставлена задача вирішується за рахунок того, що система керування станом інформаційної безпеки містить об'єкт захисту, виходи якого з'єднані з блоком отримування чітких вхідних даних та блоком визначення експертних знань, виходи яких з'єднані з блоком перетворення, вихід якого з'єднано з блоком оцінювання стану інформаційної безпеки об'єкта, блок виконання, блок індикації, вихід якого з'єднано з блоком виконання, вихід якого з'єднано з об'єктом захисту, блок визначення комплексу засобів захисту інформації, блок визначення ефективності засобів захисту інформації, блок визначення вартості засобів захисту інформації, блок визначення найкращого набору засобів захисту інформації, блок визначення критеріїв оптимізації, вихід блока оцінювання стану інформаційної безпеки об'єкта є входом блока визначення комплексу засобів захисту інформації, вихід якого з'єднано з входами блока визначення ефективності засобів захисту інформації та блока визначення вартості засобів захисту інформації, перший вихід блока визначення ефективності засобів захисту інформації є входом блока перетворення, другий вихід блока визначення ефективності засобів захисту інформації є першим входом блока визначення найкращого набору засобів захисту інформації, другим входом якого є вихід блока визначення вартості засобів захисту інформації, третім входом блока визначення найкращого набору засобів захисту інформації є вихід блока визначення критеріїв оптимізації, вихід блока визначення найкращого набору засобів захисту інформації є входом блока індикації.

На кресленні наведено схему системи керування станом інформаційної безпеки.

Система керування станом інформаційної безпеки містить об'єкт захисту 1, виходи якого з'єднані з блоком отримування чітких вхідних даних 2 та блоком визначення експертних знань 3, виходи яких з'єднані з блоком перетворення 4. Виходи блока перетворення 4 є входами блоками оцінювання стану інформаційної безпеки 5, вихід якого з'єднано з входом блока визначення комплексу засобів захисту інформації 6. Вихід блока визначення комплексу засобів захисту інформації 6 з'єднано з входами блока визначення ефективності засобів захисту інформації 7 та блока визначення вартості засобів захисту інформації 8. Перший вихід блока визначення ефективності засобів захисту інформації 7 з'єднано з входом блока перетворення 4. Другий вихід блока визначення ефективності засобів захисту інформації 7 з'єднано з першим входом блока визначення найкращого набору засобів захисту інформації 9. Другим входом блока визначення найкращого набору засобів захисту інформації 9 є вихід блока визначення вартості засобів захисту інформації 8, а третім входом - вихід блока визначення критеріїв оптимізації 10. Вихід блока визначення найкращого набору засобів захисту інформації 9 є входом блока індикації 11, вихід якого є входом блока виконання 12. Вихід блока виконання 12 з'єднано з об'єктом захисту 1.

Система керування станом інформаційної безпеки працює так. З блока отримування чітких вхідних даних 2 отримують інформацію про поточний стан параметрів об'єкта захисту 1, виражених чисельно. Параметри об'єкта захисту 1, які неможливо виразити чисельно, визначають за допомогою блока визначення експертних знань 3, шляхом залучення експертів, які висловлюють свої знання за допомогою лінгвістичних термів. Всі дані, отримані як в чіткому, так і в нечіткому вигляді, надсилають до блока перетворення 4, де вхідну інформацію з блока отримування чітких вхідних даних 2 та з блока визначення експертних знань 3 перетворюють в уніфікований вигляд і надсилають до входу блока оцінювання стану інформаційної безпеки 5, де оцінюють загальний стан інформаційної безпеки об'єкта захисту 1 та рівень впливу кожного фактора, що оцінюється за допомогою блоків отримування чітких вхідних даних 2 та блока визначення експертних знань 3, на його загальний стан інформаційної безпеки. Отримані оцінки надсилають до блока визначення комплексу засобів захисту інформації 6, за допомогою якого визначають всі комплекси засобів для захисту від найбільш значущих для загального стану інформаційної безпеки факторів. Оцінку загального стану та цей набір комплексів засобів захисту надсилають з виходу блока визначення комплексу засобів захисту інформації 6 до входу блока визначення ефективності засобів захисту інформації 7 та до блока визначення вартості засобів захисту інформації 8. За допомогою блока визначення ефективності засобів захисту інформації 7, що може бути реалізований за допомогою залучення експертів, прогнозують ефект від впровадження кожного комплексу засобів захисту, виражений в очікувальній зміні оцінок стану об'єкта захисту, та вносять відповідні зміни до оцінок у блоці перетворення 4, з виходу якого прогнозовані оцінки надсилають до блока оцінювання стану інформаційної безпеки 5, де визначають прогнозовані оцінки загального стану інформаційної безпеки, які через блок визначення комплексу засобів захисту інформації 6 надсилають до блока визначення ефективності засобів захисту інформації 7, з виходу якого надсилають всі набори комплексів засобів захисту та значення зміни оцінок загального стану інформаційної безпеки, якої можна досягти за допомогою цих комплексів засобів захисту, до блока визначення найкращого набору засобів захисту інформації 9. Одночасно за допомогою блока визначення вартості засобів захисту інформації 8, який може бути реалізований у вигляді бази знань, ви-

значають вартість кожного комплексу засобів захисту, значення яких надсилають до блока визначення найкращого набору засобів захисту інформації 9. За допомогою блока визначення критеріїв оптимізації 10 визначають тип та критерії оптимізації та надсилають їх до блока визначення найкращого набору засобів захисту інформації 9, де визначають найкраще рішення відповідно до цих критеріїв серед тих, що надійшли з блока визначення ефективності засобів захисту інформації 7. У випадку, коли серед визначених наборів комплексів засобів захисту відсутні рішення, що задовольняють заданим критеріям, з блока визначення найкращого набору засобів захисту інформації 9 формується запит щодо зміни критеріїв оптимізації, який відображається за допомогою блока індикації 11. Якщо найкраще рішення знайдене, то його надсилають за допомогою блока індикації 11 до блока виконання 12, за допомогою якого його впроваджують на об'єкті захисту 1.



Комп'ютерна верстка Г. Паяльніков Підписне Тираж 24 прим.

Міністерство освіти і науки України

Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

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