МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

УКРАЇНА

(19) UA **(11) 116649** **(13) U**

(51) МПК (2017.01)
G05B 13/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2016 13379**

(22) Дата подання заявки: **26.12.2016**

(24) Дата, з якої є чинними права на корисну модель: **25.05.2017**

(46) Публікація відомостей про видачу патенту: **25.05.2017, Бюл.№ 10**

(72) Винахідник(и):
Баришев Юрій Володимирович (UA)

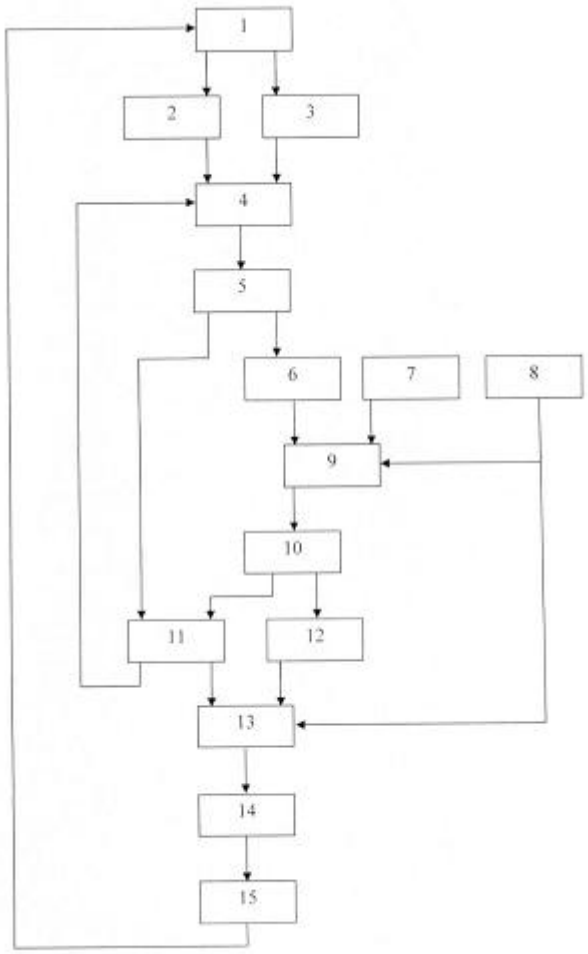
(73) Власник(и):
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ,
Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

(54) СИСТЕМА КЕРУВАННЯ СТАНОМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

(57) Реферат:

Система керування станом інформаційної безпеки містить об'єкт захисту, блок отримування чітких вхідних даних, блок визначення експертних знань, блок перетворення, блок оцінювання стану інформаційної безпеки об'єкта, блок виконання, блок індикації, блок визначення комплексів 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, блок індикації та блок первинної оптимізації.

UA 116649 U



Фіг.

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

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

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

Найбільш близькою до системи, що заявляється, є система керування станом інформаційної безпеки [Патент України № 60550 від 25.06.2011 р., М. кл. G05B 13/00, бюл. № 12, 2011 р.], 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, блок визначення комплексу засобів захисту інформації, в подальшому блок визначення комплексів 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 комплексів 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.

Недоліком прототипу є низька швидкість керування, що пов'язана з необхідністю оцінювання вартості та очікуваного ефекту від всіх можливих варіантів реалізації комплексів засобів захисту інформації.

В основу корисної моделі поставлено задачу створення системи керування станом інформаційної безпеки, яка за рахунок введення нових елементів та зв'язків призводить до підвищення швидкості керування за рахунок зменшення кількості можливих засобів, що реалізують комплекс засобів захисту інформації перед проведенням оцінювання очікуваного ефекту від їх впровадження.

Поставлена задача вирішується тим, 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 комплексів 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 комплексів 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, згідно з корисною моделлю, введено блок первинної оптимізації, першим входом якого є вихід блока визначення комплексів засобів захисту інформації, другим входом є вихід бази засобів захисту інформації, третім входом є вихід блока визначення критеріїв оптимізації, вихід блока первинної оптимізації є входом бази наборів комплексів засобів захисту інформації, перший вихід якої є входом блока визначення

ефективності засобів захисту інформації, а другий вихід є входом блока визначення вартості засобів захисту інформації.

На кресленні наведено схему системи керування станом інформаційної безпеки.

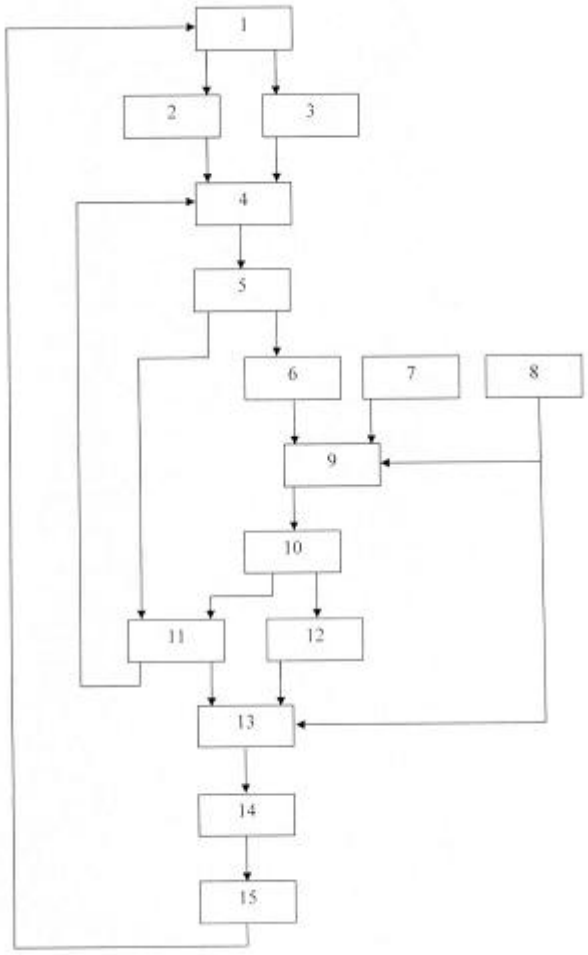
Система керування станом інформаційної безпеки містить об'єкт захисту 1, виходи якого з'єднані з блоком отримування чітких вхідних даних 2 та блоком визначення експертних знань 3, виходи яких з'єднані з блоком перетворення 4. Виходи блока перетворення 4 є входами блоками оцінювання стану інформаційної безпеки об'єкта 5, вихід якого з'єднано з входом блока визначення комплексів засобів захисту інформації 6 та блока визначення ефективності засобів захисту інформації 11. Вихід блока визначення комплексів засобів захисту інформації 6 є першим входом блока первинної оптимізації 9, другим входом якого є вихід бази засобів захисту інформації 7, а третім входом - вихід блока визначення критеріїв оптимізації 8. Вихід блока первинної оптимізації 9 є входом бази наборів комплексів засобів захисту інформації 10. Виходи бази наборів комплексів засобів захисту інформації 10 з'єднані з входами блока визначення ефективності засобів захисту інформації 11 та блока визначення вартості засобів захисту інформації 12. Перший вихід блока визначення ефективності засобів захисту інформації 11 з'єднано з входом блока перетворення 4. Другий вихід блока визначення ефективності засобів захисту інформації 11 з'єднано з першим входом блока визначення найкращого набору засобів захисту інформації 13. Другим входом блока визначення найкращого набору засобів захисту інформації 13 є вихід блока визначення вартості засобів захисту інформації 12, а третім входом - вихід блока визначення критеріїв оптимізації 8. Вихід блока визначення найкращого набору засобів захисту інформації 13 є входом блока індикації 14, вихід якого є входом блока виконання 15. Вихід блока виконання 15 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 об'єкта 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 ефективності засобів захисту інформації 11 та блока визначення комплексів засобів захисту інформації 6, за допомогою якого визначають структурні складові комплексів засобів для захисту від найбільш значущих для загального стану інформаційної безпеки факторів. Оцінку загального стану та перелік структурних складових комплексів засобів захисту інформації надсилають з виходу блока визначення комплексів засобів захисту інформації 6 до входу блока первинної оптимізації 9, в якому на основі отриманих відомостей про ефективність та вартість окремих засоби захисту інформації, які отримують з бази засобів захисту інформації 7, визначають потенційно оптимальні набори комплексів засобів захисту інформації, відкидаючи ті набори, реалізація яких напевно поступається реалізації інших комплексів засобів захисту інформації, відповідно до критеріїв оптимізації, які отримують за допомогою блока визначення критеріїв оптимізації 8. Зменшений набір комплексів засобів та захисту інформації для можливості подальшого аналізу надсилають до бази наборів комплексів засобів захисту інформації 10, з якої їх по одному надсилають до входу блока визначення ефективності засобів захисту інформації 11 та до блока визначення вартості засобів захисту інформації 12. За допомогою блока визначення ефективності засобів захисту інформації 11, що може бути реалізований за допомогою залучення експертів, прогнозують ефект від впровадження кожного комплексу засобів захисту, виражений в очікуваній зміні оцінок стану об'єкта захисту 1, та вносять відповідні зміни до оцінок у блоці перетворення 4, з виходу якого прогнозовані оцінки надсилають до блока оцінювання стану інформаційної безпеки об'єкта 5, де визначають прогнозовані оцінки загального стану інформаційної безпеки, які надсилають до блока визначення ефективності засобів захисту інформації 11, з виходу якого по завершенню обробки всіх наборів комплексів засобів захисту, які знаходяться в базі наборів комплексів засобів захисту інформації 10, надсилають ці 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 13. Одночасно за допомогою блока визначення вартості засобів захисту інформації 12, який може бути реалізований у вигляді бази знань,

визначають вартість кожного комплексу засобів захисту, значення яких надсилають до блока визначення найкращого набору засобів захисту інформації 13. З блока визначення критеріїв оптимізації 8 надсилають тип та критерії оптимізації до блока визначення найкращого набору засобів захисту інформації 13, де визначають найкраще рішення відповідно до цих критеріїв серед тих, що надійшли з блока визначення ефективності засобів захисту інформації 11. У випадку, коли серед визначених наборів комплексів засобів захисту відсутні рішення, що задовольняють заданим критеріям, з блока визначення найкращого набору засобів захисту інформації 13 формується запит щодо зміни критеріїв оптимізації, який відображається за допомогою блока індикації 14. Якщо найкраще рішення знайдене, то його надсилають за допомогою блока індикації 14 до блока виконання 15, за допомогою якого його впроваджують на об'єкті захисту 1.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

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, блок визначення комплексів 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 комплексів 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, яка **відрізняється** тим, що введено блок первинної оптимізації, першим входом якого є вихід блока визначення комплексів засобів захисту інформації, другим входом є вихід бази засобів захисту інформації, третім входом є вихід блока визначення критеріїв оптимізації, вихід блока первинної оптимізації є входом бази наборів комплексів засобів захисту інформації, перший вихід якої є входом блока визначення ефективності засобів захисту інформації, а другий вихід є входом блока визначення вартості засобів захисту інформації.



Комп'ютерна верстка А. Крижанівський

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