



УКРАЇНА

(19) **UA**

(11) **99150**

(13) **U**

(51) МПК

**H04B 1/54** (2006.01)

**H04B 1/56** (2006.01)

**H04B 1/58** (2006.01)

**H04B 3/60** (2006.01)

ДЕРЖАВНА СЛУЖБА  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ  
УКРАЇНИ

## (12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2014 11609**

(22) Дата подання заявки: **27.10.2014**

(24) Дата, з якої є чинними  
права на корисну  
модель: **25.05.2015**

(46) Публікація відомостей  
про видачу патенту: **25.05.2015, Бюл.№ 10**

(72) Винахідник(и):

**Пузиренко Олександр Григорович (UA),  
Шишацький Андрій Володимирович  
(UA),  
Куровська Тетяна Юріївна (UA),  
Лук'янов Павло Олександрович (UA),  
Комаров Володимир Олександрович  
(UA),  
Сайко Володимир Григорович (UA)**

(73) Власник(и):

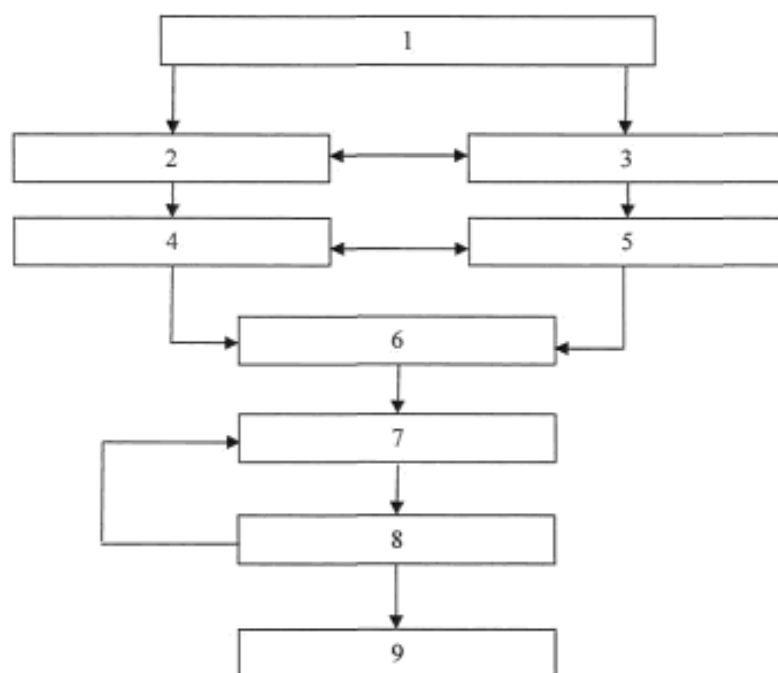
**Пузиренко Олександр Григорович,  
вул. Шолуденка, 12, кв. 23, м. Київ, 04116  
(UA),  
Шишацький Андрій Володимирович,  
б-р Перова, 44, кв. 16, м. Київ, 02139 (UA),  
Куровська Тетяна Юріївна,  
вул. Княжий Затон, 2/30, кв. 138, м. Київ-95,  
02095 (UA),  
Лук'янов Павло Олександрович,  
проспект Повітрофлотський, 28, м. Київ,  
03168 (UA)**

## (54) ПРИСТРІЙ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ

(57) Реферат:

Пристрій управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі містить модуль ідентифікації активів, модуль ідентифікації загроз, модуль ідентифікації вразливостей, модуль оброблення ризиків інформаційної безпеки, модуль оформлення звіту з аналізу ризиків інформаційної безпеки. Додатково пристрій містить модуль визначення ймовірності реалізації загроз, модуль оцінки можливих наслідків від реалізації загроз, модуль визначення рівня ризику інформаційної безпеки, модуль визначення допустимого рівня ризику інформаційної безпеки.

**UA 99150 U**



Корисна модель належить до систем безпеки в галузі захисту інформації, а саме систем управління ризиками інформаційної безпеки в інформаційно-телекомунікаційних системах.

Відомий пристрій управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі, що містить модуль визначення характеристик системи, модуль ідентифікації загроз, модуль ідентифікації вразливостей, модуль аналізу наявних засобів/заходів захисту, модуль визначення значення ймовірності, модуль аналізу впливу, модуль визначення значення ризику, модуль вибору засобів/заходів захисту, модуль документування отриманих результатів, при цьому вихід модуля визначення характеристик системи послідовно з'єднаний з входом модуля ідентифікації загроз, вихід модуля ідентифікації загроз послідовно з'єднано з входом модуля ідентифікації вразливостей, вихід якого послідовно з'єднано з входом модуля аналізу наявних засобів/заходів захисту, вихід якого послідовно з'єднано з входом модуля визначення значення ризику, вихід якого послідовно з'єднано з входом модуля аналізу впливу, вихід якого послідовно з'єднано з входом модуля визначення значення ризику, вихід якого послідовно з'єднано з входом модуля вибору засобів/заходів захисту, вихід якого послідовно з'єднано з входом модуля документування отриманих результатів [1].

До недоліків пристрою управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі, який вибрано за аналог, є низька швидкість аналізу ризиків інформаційної безпеки та низька ефективність алгоритму оцінки ризику інформаційної безпеки.

Найбільш близьким технічним рішенням, вибраним як найближчий аналог, є пристрій управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі, що містить модуль ідентифікації активів, модуль ідентифікації загроз, модуль ідентифікації вразливостей, модуль оброблення ризиків інформаційної безпеки, модуль оформлення звіту з аналізу ризиків інформаційної безпеки, причому перший вихід модуля ідентифікації активів з'єднано з входом модуля ідентифікації загроз, а другий вихід з'єднано з входом модуля ідентифікації вразливостей, які з'єднані між собою зворотним зв'язком [2].

До недоліків відомого пристрою управління інформаційною безпекою в інформаційно-телекомунікаційній системі є довготривалий процес аналізу рівня інформаційної безпеки, велика кількість звітної матеріалу, що генерується пристроєм в процесі роботи, відсутність можливості створювати шаблони звіту про рівень інформаційної безпеки та модифікувати наявні, відсутність можливості уникнення ризику або прийняття ризику інформаційної безпеки.

В основу корисної моделі поставлено задачу шляхом додаткового введення модуля визначення ймовірності реалізації загроз, модуля оцінки можливих наслідків від реалізації загроз, модуля визначення рівня ризику інформаційної безпеки, модуля визначення допустимого рівня ризику інформаційної безпеки до складу пристрою управління інформаційною безпекою в інформаційно-телекомунікаційній системі забезпечити підвищення швидкості аналізу рівня інформаційної безпеки, підвищити ефективність алгоритму оцінки ризику інформаційної безпеки, створити додаткову можливість уникнення ризику або прийняття ризику інформаційної безпеки.

Поставлена задача в пристрої управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі, що складається з модуля ідентифікації активів, модуля ідентифікації загроз, модуля ідентифікації вразливостей, модуля оброблення ризиків інформаційної безпеки, модуля оформлення звіту з аналізу ризиків інформаційної безпеки, вирішується тим, що, згідно з корисною моделлю, до складу пристрою управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі додатково введено модуль визначення ймовірності реалізації загроз, модуль оцінки можливих наслідків від реалізації загроз, модуль визначення рівня ризику інформаційної безпеки та модуль визначення допустимого рівня ризику інформаційної безпеки, причому перший вихід модуля ідентифікації активів з'єднано з входом модуля ідентифікації загроз, а другий вихід з'єднано з входом модуля ідентифікації вразливостей, які з'єднані між собою зворотним зв'язком, при цьому вихід модуля ідентифікації загроз з'єднано з входом модуля визначення ймовірності реалізації загроз, вихід якого з'єднано з першим входом модуля визначення рівня ризику інформаційної безпеки, вихід модуля ідентифікації вразливостей з'єднано з входом модуля оцінки можливих наслідків від реалізації загроз, вихід якого з'єднано з другим входом модуля визначення допустимого рівня ризику інформаційної безпеки, вихід модуля визначення рівня ризику інформаційної безпеки з'єднано з входом модуля оброблення ризиків інформаційної безпеки, вихід якого з'єднано з входом модуля визначення допустимого рівня ризику інформаційної безпеки, перший вихід якого з'єднано з другим входом модуля оброблення ризиків інформаційної безпеки, а другий вихід модуля визначення допустимого рівня ризику інформаційної безпеки з'єднано з входом модуля оформлення звіту з аналізу ризиків інформаційної безпеки, при цьому модуль визначення

ймовірності реалізації загроз і модуль оцінки можливих наслідків від реалізації загроз з'єднані зворотним зв'язком.

Порівняння корисної моделі, що заявляється, із найближчим аналогом, дозволяє зробити висновок, що пристрій управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі, що заявляється, відрізняється тим, що додатково містить модуль визначення ймовірності реалізації загроз, модуль оцінки можливих наслідків від реалізації загроз, модуль визначення рівня ризику інформаційної безпеки, модуль визначення допустимого рівня ризику інформаційної безпеки.

Вирішення технічної задачі в пристрої управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі (що заявляється), дійсно можливе тому, що:

- шляхом введення до складу пристрою управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі модуля визначення ймовірності реалізації загроз, дозволить визначається ймовірність реалізації загрози, тим самим дозволить підвищити швидкість аналізу рівня інформаційної безпеки;

- шляхом введення до складу пристрою управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі модуля оцінки можливих наслідків від реалізації загроз дозволить підвищити ефективність алгоритму оцінки ризику інформаційної безпеки та створити додаткову можливість створення шаблону звіту рівня інформаційної безпеки та модифікувати наявні;

- шляхом введення до складу пристрою управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі модуля визначення рівня ризику інформаційної безпеки дозволить підвищити швидкість аналізу рівня інформаційної безпеки та зменшити кількість звітної матеріалу, що генерується в процесі роботи;

- шляхом введення до складу пристрою управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі модуля визначення допустимого рівня ризику інформаційної безпеки дозволить створити додаткову можливість уникнення ризику інформаційної безпеки або його прийняття.

Пристрій управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі конструктивно містить модуль ідентифікації активів (1), модуль ідентифікації загроз (2), модуль ідентифікації вразливостей (3), модуль визначення ймовірності реалізації загроз (4), модуль оцінки можливих наслідків від реалізації загроз (5), модуль визначення рівня ризику інформаційної безпеки (6), модуль оброблення ризиків інформаційної безпеки (7), модуль визначення допустимого рівня ризику інформаційної безпеки (8), модуль оформлення звіту з аналізу ризиків інформаційної безпеки (9).

Суть корисної моделі пояснюється за допомогою креслення, де подана функціональна схема запропонованого пристрою управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі.

Пристрій управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі працює наступним чином:

Модуль ідентифікації активів (1) визначає процеси, додатки, системи або активи, які розглядаються. Ключовим моментом розгляду є те, що розгляду підлягають лише ті системи/активи, які є критичними для забезпечення неперервності функціонування системи захисту інформації в інформаційно-телекомунікаційній мережі. Далі інформація про стан інформаційно-телекомунікаційної системи надходить на модуль ідентифікації загроз (2), який визначає загрози, які можуть вплинути на роботу системи захисту інформації в інформаційно-телекомунікаційній мережі. Деякі загрози виникають, коли впроваджені контролі або впроваджені неправильно, або втратили актуальність і вже стали причиною вразливості інформаційно-телекомунікаційної системи та можуть бути використані для обходу контролів. Цей процес відомий як використання вразливості. Інформаційна послідовність по стан інформаційно-телекомунікаційної системи надходить також на вхід модуля ідентифікації вразливостей (3), де ідентифікуються ті вразливості, які виникають, а саме їх тип, походження та рівень загрози. У ході роботи проходить обмін між модулем ідентифікації загроз (2) та модулем ідентифікації вразливостей (3) для найбільш повного аналізу. З виходу модуля ідентифікації загроз (2) інформація про стан інформаційно-телекомунікаційної системи надходить на вхід модуля визначення ймовірності реалізації загроз (4), де визначається ймовірність реалізації загрози. Після того, як список загроз ідентифіковано, з'ясовується, наскільки ймовірне виникнення конкретних загроз. З виходу модуля ідентифікації вразливостей (3) інформація про стан інформаційно-телекомунікаційної системи надходить на вхід модуля оцінки можливих наслідків від реалізації загроз (5), де визначається можливі наслідки від реалізації загроз. У ході роботи проходить двосторонній обмін інформацією між модулем

визначення ймовірності реалізації загроз (4) та модулем оцінки можливих наслідків від реалізації загроз (5) для найбільш повного аналізу. З виходу модуля визначення ймовірності реалізації загроз (4) та модуля оцінки можливих наслідків від реалізації загроз (5) інформація про стан системи надходить на вхід модуля визначення рівня ризику інформаційної безпеки (6), де на підставі інформації від модуля визначення ймовірності реалізації загроз (4) та модуля оцінки можливих наслідків від реалізації загроз (5) визначається рівень ризику для забезпечення інформаційної безпеки в інформаційно-телекомунікаційній системі. З виходу модуля визначення рівня ризику інформаційної безпеки (6) інформація про стан інформаційно-телекомунікаційної системи надходить на вхід модуля оброблення ризиків інформаційної безпеки (7), де відбувається оброблення інформації про рівень та характер ризику інформаційної безпеки інформаційно-телекомунікаційної системи. Після того, як рівень ризику визначено, модуль визначає способи, які могли б усунути ризик або принаймні знизити його до прийнятного рівня, та вибирає відповідні заходи захисту. З виходу модуля оброблення ризиків інформаційної безпеки (7) інформація про стан інформаційної безпеки інформаційно-телекомунікаційної системи надходить на вхід модуля визначення допустимого рівня ризику інформаційної безпеки (8), на підставі вищенаведених даних модуль визначення допустимого рівня ризику інформаційної безпеки (8), визначає який рівень ризику найбільш прийнятний для системи та визначає, яким з них можна знехтувати в даний час, якщо його не можливо локалізувати. Один вихід модуля визначення допустимого рівня ризику інформаційної безпеки (8) з'єднаний з входом модуля оброблення ризиків інформаційної безпеки (7), і якщо рівень інформаційної безпеки низький то дає команду на його ігнорування, а якщо вищий допустимого, то на його локалізацію. Інформація про стан інформаційної безпеки інформаційно-телекомунікаційної системи по другому виходу модуля визначення допустимого рівня ризику інформаційної безпеки (8) надходить на вхід модуля оформлення звіту з аналізу ризиків інформаційної безпеки (9), що виконує функцію оформлення звіту про стан інформаційної безпеки інформаційно-телекомунікаційної системи та його представлення за вимогою.

Підвищення ефективності застосування пристрою управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі, у порівнянні з найближчим аналогом, полягає у тому, що шляхом додаткового введення до складу пристрою управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі модуля визначення ймовірності реалізації загроз, модуля оцінки можливих наслідків від реалізації загроз, модуля визначення рівня ризику інформаційної безпеки, модуля визначення допустимого рівня ризику інформаційної безпеки, забезпечується підвищення швидкості аналізу рівня інформаційної безпеки, підвищується ефективність алгоритму оцінки ризику інформаційної безпеки, зменшується кількість звітної матеріалу, що генерується пристроєм в процесі роботи, а також створюється додаткова можливість створювати шаблони звіту рівня інформаційної безпеки та модифікувати наявні, створюється додаткова можливість уникнення ризику або прийняття ризику інформаційної безпеки.

Джерела інформації:

1. Swanson M. NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems / M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, D. Lynes. - 2010. - 149 p - аналог.

2. Балашов П. А. Оценка рисков информационной безопасности на основе нечеткой логики: П.А. Балашов, В.П. Безгузиков, Р.И. Кислов - М.: Научная литература, 2009. - 165 с. - найближчий аналог.

#### ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Пристрій управління ризиками інформаційної безпеки в інформаційно-телекомунікаційній системі, що містить модуль ідентифікації активів, модуль ідентифікації загроз, модуль ідентифікації вразливостей, модуль оброблення ризиків інформаційної безпеки, модуль оформлення звіту з аналізу ризиків інформаційної безпеки, причому перший вихід модуля ідентифікації активів з'єднано з входом модуля ідентифікації загроз, а другий вихід з'єднано з входом модуля ідентифікації вразливостей, які з'єднані між собою зворотним зв'язком, який **відрізняється** тим, що додатково містить модуль визначення ймовірності реалізації загроз, модуль оцінки можливих наслідків від реалізації загроз, модуль визначення рівня ризику інформаційної безпеки, модуль визначення допустимого рівня ризику інформаційної безпеки, при цьому вихід модуля ідентифікації загроз з'єднано з входом модуля визначення ймовірності реалізації загроз, вихід якого з'єднано з першим входом модуля визначення рівня ризику інформаційної безпеки, вихід модуля ідентифікації вразливостей з'єднано з входом модуля

- оцінки можливих наслідків від реалізації загроз, вихід якого з'єднано з другим входом модуля визначення допустимого рівня ризику інформаційної безпеки, вихід модуля визначення рівня ризику інформаційної безпеки з'єднано з входом модуля оброблення ризиків інформаційної безпеки, вихід якого з'єднано з входом модуля визначення допустимого рівня ризику інформаційної безпеки, перший вихід якого з'єднано з другим входом модуля оброблення ризиків інформаційної безпеки, а другий вихід модуля визначення допустимого рівня ризику інформаційної безпеки з'єднано з входом модуля оформлення звіту з аналізу ризиків інформаційної безпеки, при цьому модуль визначення ймовірності реалізації загроз і модуль оцінки можливих наслідків від реалізації загроз з'єднані зворотним зв'язком.

