УКРАЇНА

(19) UA **(11) 158553** **(13) U**

(51) МПК
H04B 1/54 (2006.01)
H04B 1/56 (2006.01)
H04B 1/58 (2006.01)
H04B 3/60 (2006.01)

НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ДЕРЖАВНА ОРГАНІЗАЦІЯ "УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ОФІС ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ІННОВАЦІЙ"

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2024 04319**

(22) Дата подання заявки: **03.09.2024**

(24) Дата, з якої є чинними права інтелектуальної власності: **20.02.2025**

(46) Публікація відомостей про державну реєстрацію: **19.02.2025, Бюл.№ 8**

(72) Винахідник(и):
Кашкевич Світлана Олександрівна (UA),
Шишацький Андрій Володимирович (UA),
Неронов Сергій Миколайович (UA),
Плєхова Ганна Анатоліївна (UA),
Єфименко Олександр Володимирович (UA),
Байдала Владислава Юріївна (UA),
Саєнко Владислав Олександрович (UA)

(73) Володілець (володільці):
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ АВТОМОБІЛЬНО-ДОРОЖНІЙ УНІВЕРСИТЕТ,
вул. Ярослава Мудрого, 25, м. Харків, 61002 (UA),
Плєхова Ганна Анатоліївна,
вул. Мотронінська, 9, м. Харків, 61003 (UA)

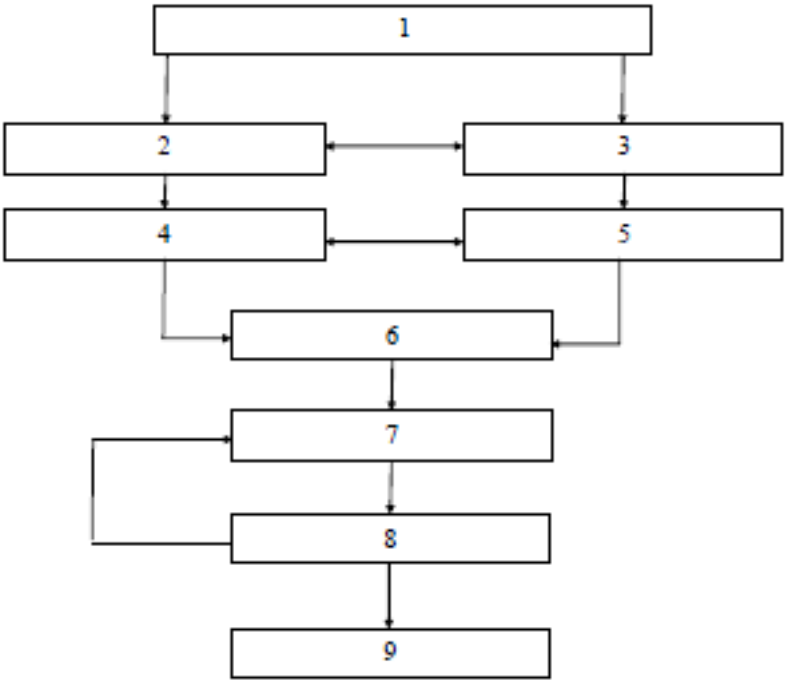
(74) Представник:
Азарова Алла Володимирівна

(54) ПРИСТРІЙ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

(57) Реферат:

Пристрій управління ризиками інформаційної безпеки в інформаційних системах містить модуль ідентифікації активів, модуль ідентифікації загроз, модуль ідентифікації вразливостей, модуль оброблення ризиків інформаційної безпеки, модуль оформлення звіту з аналізу ризиків інформаційної безпеки. 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.

UA 158553 U


1
2
3
4
5
6
7
8
9

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

Відомий пристрій управління ризиками інформаційної безпеки в інформаційних системах, 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 визначення значення ймовірності, 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 інформаційних системах, який вибрано за аналог, є низька швидкість аналізу ризиків інформаційної безпеки та низька ефективність алгоритму оцінки ризику інформаційної безпеки.

Найбільш близьким аналогом корисної моделі є пристрій управління ризиками інформаційної безпеки в інформаційних системах, 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 зворотнім зв'язком [2].

До недоліків найбільш близького аналога належить довготривалий процес аналізу рівня інформаційної безпеки, велика кількість звітного 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 поставлена задача 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 інформаційних системах 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 вирішується тим, що пристрій управління ризиками інформаційної безпеки в інформаційних системах, 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 зворотнім зв'язком, згідно з корисною моделлю, 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 зворотнім зв'язком.

Порівняння корисної моделі та найбільш близького аналога дозволяє зробити висновок, що корисна модель 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 інформаційних системах дійсно можливе тому, що:

- шляхом введення до складу пристрою управління ризиками інформаційної безпеки в інформаційних системах модуля визначення ймовірності реалізації загроз, дозволить визначити ймовірність реалізації загрози, тим самим дозволить підвищити швидкість аналізу рівня інформаційної безпеки;

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

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

Пристрій управління ризиками інформаційної безпеки в інформаційних системах 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, на якому представлена функціональна схема пристрою управління ризиками інформаційної безпеки в інформаційних системах.

Пристрій управління ризиками інформаційної безпеки в інформаційних системах 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 інформаційній мережі. Далі інформація про стан інформаційної системи надходить на модуль ідентифікації загроз (2), який визначає загрози, які можуть вплинути на роботу системи захисту інформації в інформаційній мережі. Деякі загрози виникають, коли впроваджені контролі або впроваджені неправильно, або втратили актуальність і вже стали причиною вразливості інформаційної системи та можуть бути використані для обходу контролів. Цей процес відомий як використання вразливості. Інформаційна послідовність про стан інформаційної 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 інформаційної 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 інформаційної системи надходить на вхід модуля оцінки можливих наслідків від реалізації загроз (5), де визначаються 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 інформаційній системі. З виходу модуля визначення рівня ризику інформаційної безпеки (6) інформація про стан інформаційної системи надходить на вхід модуля оброблення ризиків інформаційної безпеки (7), де відбувається оброблення інформації про рівень та характер ризику інформаційної безпеки інформаційної 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 інформаційної 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 інформаційної 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 інформаційної системи та його представлення за вимогою.

Підвищення ефективності застосування пристрою управління ризиками інформаційної безпеки в інформаційній системі, порівняно з найбільш близьким аналогом, полягає у тому, що шляхом додаткового введення до складу пристрою управління ризиками інформаційної безпеки в інформаційній 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 звітного 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:

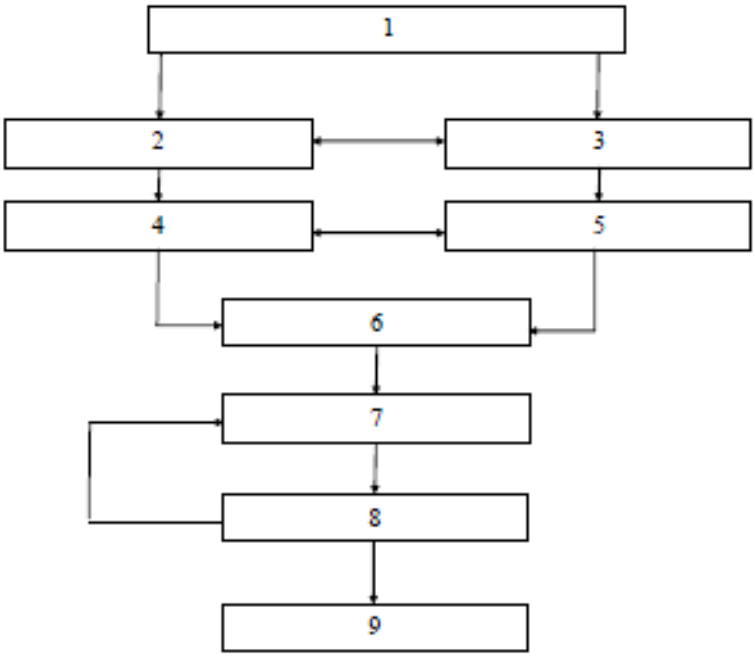
1. Swanson M. NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems / M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, D. Lynes. - 2010. - 149 p. - аналог.

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. - найбільш близький аналог.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Пристрій управління ризиками інформаційної безпеки в інформаційних системах, 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 зворотнім 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 зворотнім зв'язком.



Комп'ютерна верстка О. Гергіль

ДО "Український національний офіс інтелектуальної власності та інновацій", вул. Дмитра Годзенка, 1, м. Київ – 42, 01601