УДК 004.056 DOi 10.30837/ bi.2024.2(101).07

Н. В. Шаронова[1], Г. А. Плєхова[2], М. В. Костікова[3], С. М. Неронов[4], С. О. Кашкевич[5]
[1]НТУ «ХПІ», м. Харків, Україна, nvsharonova@ukr.net, ORCID iD: 0009-0004-9878-1761
[2]ХНАДУ, м. Харків, Україна, plehovaanna11@gmail.com, ORCID iD: 0000-0002-6912-6520
[3]ХНАДУ, м. Харків, Україна, kmv_topaz@ukr.net, ORCID iD: 0000-0001-5197-7389
[4]ХНАДУ, м. Харків, Україна, sernikner@gmail.com, ORCID iD: 0000-0003-2381-1271
[5]НАУ, м. Київ, Україна, svitlana.kashkevych@npp.nau.edu.ua, ORCID iD: 0000-0002-4448-3839

ПРИСТРІЙ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

У роботі запропоновано пристрій управління ризиками інформаційної безпеки в інформаційних системах. Запропонований пристрій містить модуль ідентифікації активів, модуль ідентифікації загроз, модуль ідентифікації вразливостей, модуль оброблення ризиків інформаційної безпеки, модуль оформлення звіту з аналізу ризиків інформаційної безпеки. 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. Технічним результатом є забезпечення підвищення швидкості аналізу рівня інформаційної безпеки, підвищення ефективності алгоритму оцінки ризику інформаційної безпеки, зменшення кількості звітного матеріалу, що генерується пристроєм в процесі роботи, створювати додаткову можливість створювати шаблони звіту рівня інформаційної безпеки та модифікувати наявні, створити додаткову можливість уникнення ризику або прийняття ризику інформаційної безпеки шляхом додаткового введення до складу пристрою управління ризиками інформаційної безпеки в інформаційних системах 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.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНА СИСТЕМА, РИЗИК, АНАЛІЗ, ПРИСТРІЙ

N. V. Sharonova, G. A. Pliekhova, M. V. Kostikova, S. M. Neronov, S. O. Kashkevych. Information security risk management device in information systems. The paper proposes a device for managing information security risks in information systems. The proposed device contains an asset identification module, a threat identification module, a vulnerability identification module, an information security risk processing module, and an information security risk analysis report design module. The first output of the asset identification module is connected to the input of the threat identification module, and the second output is connected to the input of the vulnerability identification module, which are interconnected by feedback. The technical result is to increase the speed of information security level analysis, increase the efficiency of the information security risk assessment algorithm, reduce the amount of reporting material generated by the device during operation, create an additional opportunity to create information security level report templates and modify existing ones, create an additional opportunity to avoid risk, or acceptance of information security risk by additional introduction to the information security risk management device in information systems of the module for determining the probability of the realization of threats, the module for assessing the possible consequences of the implementation of threats, the module for determining the level of information security risk, the module for determining the permissible level of information security risk.

INFORMATION SECURITY, INFORMATION SYSTEM, RISK, ANALYSIS, DEVICE

Вступ

Забезпечення національної безпеки держави пов'язане, поряд з іншим, з використанням значного інформаційного ресурсу, що спричиняє підвищену потребу інформаційної безпеки держави. В сучасних умовах до інформації, яка циркулює в інформаційному просторі між об'єктами та суб'єктами управління, висуваються особливі вимоги стосовно її основних властивостей: достовірності, доступності, повноти (достатності), цілісності, конфіденційності, порушення яких може становити загрозу інформаційній безпеці держави, реально призвести до нанесення значної шкоди в різних сферах життєдіяльності. Проблема безпеки інформації як складової забезпечення інформаційної безпеки в загальній системі її забезпечення постає вкрай актуальною [1].

У зв'язку із зростаючою роллю інформаційних технологій у житті сучасного суспільства, а також через реальності численних загроз з точки зору їх захищеності проблема інформаційної безпеки вимагає до себе все більшої уваги. Системний характер впливу на інформаційну безпеку великої сукупності різних обставин призводять до необхідності комплексного підходу щодо вирішення даної проблеми [2].

Тому розробка пристроїв управління ризиками інформаційної безпеки в інформаційних системах, дуже необхідна. Такі моделі належать до систем безпеки в галузі захисту інформації, а саме систем управління ризиками інформаційної безпеки в інформаційних системах.

1. Виклад основного матеріалу

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. 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 модуля аналізу наявних засобів/заходів захисту послідовно з'єднано з входом модуля визначення значення ризику, вихід якого послідовно з'єднано з входом модуля визначення значення ймовірності. Вихід модуля визначення значення ймовірності послідовно з'єднано з входом модуля аналізу впливу, вихід якого послідовно з'єднано з входом модуля визначення значення ризику. Вихід модуля визначення значення ризику послідовно з'єднано з входом модуля вибору засобів/заходів захисту, вихід якого послідовно з'єднано з входом модуля документування отриманих результатів [3].

До недоліків пристрою управління ризиками інформаційної безпеки в інформаційних системах, який обрано за аналог, є низька швидкість аналізу ризиків інформаційної безпеки та низька ефективність алгоритму оцінки ризику інформаційної безпеки.

Найбільш близьким технічним рішенням, обраним за прототип 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 [4].

До недоліків відомого пристрою управління інформаційною безпекою в інформаційних системах є 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 моделі покладено 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 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.

Суть моделі в пристрої управління ризиками інформаційної безпеки в інформаційних системах, 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 в тому, що до складу пристрою управління ризиками інформаційної безпеки в інформаційних системах 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. 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. 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. Модуль визначення ймовірності реалізації загроз і модуль оцінки можливих наслідків від реалізації загроз з'єднані зворотнім зв'язком.

Порівняння технічного рішення, що пропонується, із прототипом, дозволяє зробити висновок, що пристрій управління ризиками інформаційної безпеки в інформаційних системах, що пропонується, 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.

Рішення технічної задачі в пристрою управління ризиками інформаційної безпеки в інформаційних системах (що пропонується), дійсно можливе тому, що:

– шляхом введення до складу пристрою управління ризиками інформаційної безпеки в інформаційних системах 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 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 моделі пояснюється за допомогою креслень, де на рис. 1 подана функціональна схема запропонованого пристрою управління ризиками інформаційної безпеки в інформаційних системах.

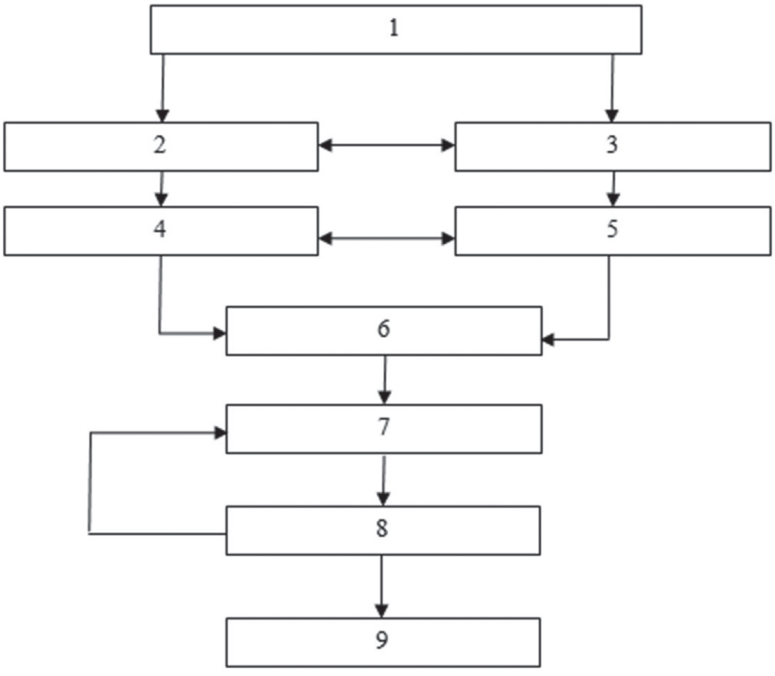

Рис. 1. Функціональна схема пристрою управління ризиками інформаційної безпеки в інформаційних системах

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 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) з метою 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 вищій 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.

Висновки

Підвищення ефективності застосування пристрою управління ризиками інформаційної безпеки в інформаційній системі, у порівнянні з прототипом, 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.

Список літератури

[1] Сніцаренко, П. М., Саричев, Ю. А., Зубков, В. П., Піщанський, Ю. А. (2022). Методичний підхід до управління ризиками безпеки інформації як складової забезпечення інформаційної безпеки держави. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, 2(75), 47-55. URL: http://znp-cvsd.nuou.org.ua/article/view/266779/262799.

[2] Аналіз оцінки загроз інформаційній безпеці на об'єктах інформаційної діяльності / С. П. Євсеєв [та ін.] // International independent scientific journal. – 2021. – № 34. – С. 33-39. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/48505dd3-1a87-40fe-b9b1-e45f8f2bd72a/content.

[3] 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.

[4] Балашов П. А. Оценка рисков информационной безопасности на основе нечеткой логики: учебное пособие / П. А. Балашов, В. П. Безгузиков, Р. И. Кислов – М.: Научная литература, 2009. – 165 с.

Надійшла до редколегії 11.11.2024