УДК 004.056.53
DOI https://doi.org/10.32838/2663-5941/2019.4-1/08

Гончар С.Ф.
Інститут проблем моделювання в енергетиці імені Г.Є. Пухова
Національної академії наук України

МЕТОДОЛОГІЯ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У роботі запропонована методологія оцінки суми ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури. Доведено актуальність даної методології оцінки ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури під час створення систем управління інформаційною безпекою та комплексної системи захисту інформації таких інформаційних систем. Показано, що економічна доцільність застосування і вибір тих чи інших заходів з обробки ризику, включно як організаційні, так і технічні, визначається оцінювальним порівнянням вартості таких заходів з максимальною величиною збитків в результаті дії декількох ризиків. Результат оцінки суми таких ризиків дають підстави для прийняття рішення щодо прийнятності їхнього рівня і необхідності чи економічної доцільності їхньої подальшої обробки. У даній статті під сумою ризиків розуміємо певну величину, що визначається збитками у результаті реалізації усіх складових частин ризиків, і ймовірністю реалізації цих ризиків. Запропонована у статті методологія базується на застосуванні методів розрахунку суми ризиків і обчислення комплексного ризику. Показано, що ризик можливо представити у вигляді комплексного числа. Приведені методи розрахунку суми ризиків і обчислення комплексного ризику. На підставі запропонованої в даній статті методології, можливо розробити комплекс структурних рішень обчислювальних систем оцінки ризику кібербезпеки інформаційних систем, що реалізують методи розрахунку суми ризиків та обчислення комплексного ризику, а також побудувати програмні та апаратно-програмні системи, які базуються на використанні методів розрахунку суми ризиків та обчислення комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Отримані результати можуть бути використані під час визначення ризику складного проекту (може бути складна інформаційна система), що характеризується наслідками під час реалізації даного проекту та ймовірністю цих наслідків.

Ключові слова: *кібербезпека, ризик, критична інфраструктура, інформаційна система, методологія.*

Постановка проблеми. Сьогодні в галузях, які життєво важливі для критичної інфраструктури широко використовуються автоматизовані системи управління технологічними процесами, які включають системи диспетчерського управління і збору даних, системи розподіленого управління та інші конфігурації систем управління.

Ще порівняно недавно питання безпеки об'єктів критичної інфраструктури держави вирішувалося за двома основними напрямами: захист від несанкціонованого доступу на об'єкт та забезпечення надійного функціонування автоматизованих систем управління технологічним процесом. Однак розвиток та поширення інформаційних технологій, глобалізація інформаційно-телекомунікаційних мереж зумовили появу нового типу загроз безпеки об'єктів – злому і порушення режимів функціонування ключових об'єктів інформатизації, які відповідають за управління та забезпечення безпеки об'єктів критичної інфраструктури. Забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури регламентується Законом України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини та громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності з забезпечення кібербезпеки. Відповідно до даного Закону України кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їхніх наслідків, відновлення сталості та надійності функціонування комунікаційних, технологічних систем. Забезпечення кібербезпеки досягається створенням системи управління інформаційною безпе-

кою (далі – СУІБ) відповідно до міжнародного стандарту ISO/IEC 27001:2013 та/або створенням комплексної системи захисту інформації (далі – КСЗІ) відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

Одним з основних етапів побудови СУІБ, КСЗІ являється створення системи ризик-менеджменту. В системі ризик-менеджменту процес оцінки ризику є основою та підґрунтям для наукових досліджень в області аналізу та удосконалення наявних, а також винаходу нових методів оцінки ризику, підвищення точності його оцінки, здійснення над ризиками математичних операцій.

Стейкхолдери інформаційних систем прагнуть звести до мінімуму ризики кібербезпеки, а також мінімізувати витрати на заходи з мінімізації цих ризиків. Економічна доцільність застосування і вибір тих чи інших заходів з обробки ризику, включно як організаційні, так і технічні, визначається оцінювальним порівнянням вартості таких заходів з максимальною величиною збитків в результаті дії декількох ризиків. Результат оцінки суми таких ризиків дають підстави для прийняття рішення щодо прийнятності їхнього рівня і необхідності чи економічної доцільності їхньої подальшої обробки. Під сумою ризиків будемо розуміти певну величину, що визначається збитками у результаті реалізації усіх складових частин ризиків, і ймовірністю реалізації цих ризиків. Таке завдання являється актуальною для визначення ризику складного проекту (може бути складна інформаційна система), що характеризується наслідками під час реалізації даного проекту та ймовірністю цих наслідків.

Аналіз останніх досліджень і публікацій. Наявні підходи до визначення поняття ризиків та методи їхньої оцінки недостатньо повно описують це поняття, не враховують суб'єктивний ризик, що ускладнює коректну його оцінку. Питання оцінки ризиків кібербезпеки інформаційних систем досліджувалося багатьма науковцями [1-8]. Водночас невирішеним залишається питання, пов'язане з можливістю розрахунку суми ризиків, що дало б можливість здійснення кількісної оцінки ризику проекту загалом або вибраного напряму розвитку процесу.

Постановка задачі. Таким чином, на сучасному етапі розвитку науки та техніки є об'єктивна суперечність між потребою в розрахунку суми ризиків та обчисленні комплексного ризику, з одного боку, та відсутністю відповідних методів розрахунку, з іншого.

З огляду на викладене вище, тема дослідження присвячена розв'язанню важливої науково-прикладної проблеми, пов'язаної з розробкою методології оцінки ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури, орієнтованої на створення відповідних методів розрахунку суми ризиків, є актуальною.

Виклад основного матеріалу. Є досить багато понять «ризик». Одне з них визначає ризик R як ймовірність або можливість p настання випадкової події, що призводить до певних збитків h, і може бути записано у вигляді:

$$R = p \cdot h\,, \qquad (1)$$

Відповідно до (1) залежність збитків h в результаті настання деякої події від ймовірності p її настання можна представити у вигляді:

$$h(p) = \frac{R}{p}, \text{ де } p \neq 0\,, \qquad (2)$$

Нехай, є n ризиків, де кожен ризик представлений графіком функції (2) і визначається ймовірністю настання випадкової події, що призводить до певних збитків (точки 4, 5, 6) (рис. 1).

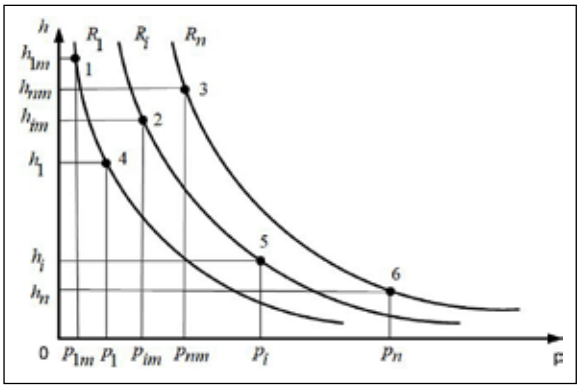

Рис. 1. Визначення суми ризиків

Метод визначення суми ризиків передбачає послідовного визначення: максимальних значень збитків для кожного ризику; ймовірності виникнення подій, що призводять до максимальних збитків (точки 1, 2, 3) (рис. 1); величини сумарних збитків, що не перевищує суму максимальних збитків для кожного з ризиків; ймовірність виникнення максимальних збитків, як суми ймовірностей сумісних подій.

Ризик суми визначається, як добуток величини сумарних збитків і ймовірності їхнього виникнення.

Використовуючи отримане значення суми ризиків на підставі вираження (2), будуємо графік функції (рис. 2).

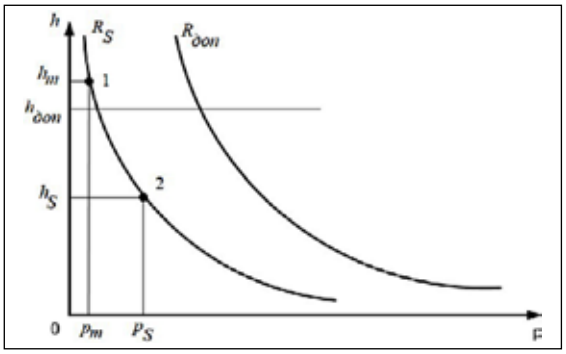

Рис. 2. Порівняльне оцінювання суми ризиків

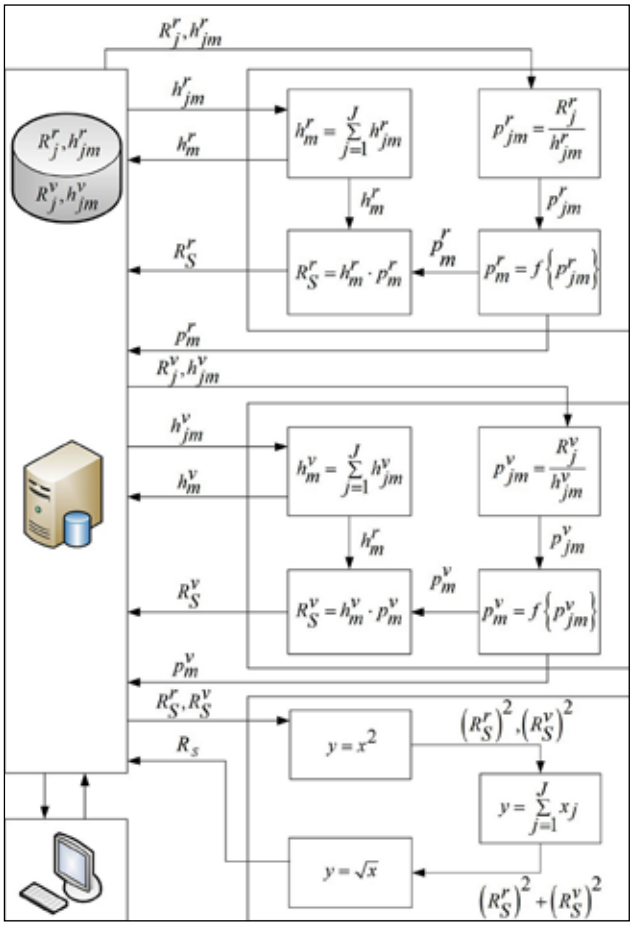

Рис. 3. Структурно-аналітичне відображення розробленої методології оцінки ризиків

Отримані результати дають можливість визначати величину сумарних збитків і ймовірність їхнього виникнення, а також здійснювати оцінювання суми ризиків з метою сприяння прийняттю рішень з його обробки. Оцінювання ризику містить порівняння отриманих результатів із заданими критеріями допустимого ризику або допустимих збитків.

Перевагами даного методу визначення суми ризиків є наочність і простота розрахунків.

Велику роль під час оцінки ризику відіграє те, які потреби індивіда можуть бути задоволені в результаті здійснення сприятливого результату і яку загрозу для нього може представляти несприятливий результат. Прийняття рішень у сфері управління ризиками значною мірою залежить від відчуття ризику. Доцільність врахування суб'єктивного ризику підтверджується дослідженнями, проведеними в [9].

Тому, коректна кількісна оцінка повного ризику повинна поєднувати в собі не тільки складову частину об'єктивного ризику, а й складову частину суб'єктивного ризику.

Однак, наявні методи оцінки ризиків не враховують суб'єктивну складову частину ризику, що ускладнює коректну оцінку ризиків.

Як показують дослідження [10], повний ризик можна представити у вигляді комплексного числа:

$$R = r + iv, \qquad (3)$$

де r – об'єктивний риск; v – суб'єктивний риск; $i = \sqrt{-1}$.

Водночас модуль комплексного ризику $|R|$ визначає дійсну характеристику повного ризику:

$$|R| = \sqrt{r^2 + v^2}, \qquad (4)$$

а, аргумент комплексного ризику:

$$\varphi = arctg\frac{v}{r}, \qquad (5)$$

є показником превалювання однієї складової частину ризику над іншою.

Узагальнена методологія, розроблена в даному розділі, базується на методі експертних оцінок і представлених вище методах та включає такі основні етапи:

1) визначення базових параметрів. Визначаються параметри, які являються базовими, для обчислення суми ризиків, використовуючи запропоновані у дисертаційній роботі методи. Визначення базових параметрів може бути здійснено, як приклад, методом експертних оцінок;

2) введення вхідних даних. Здійснюється в модуль пам'яті та далі в модуль обчислення. В модулі пам'яті формується база даних вхідних даних та результатів обчислень;

3) обчислення суми ризиків об'єктивної складової частину;

4) обчислення суми ризиків суб'єктивної складової частину;

5) визначення суми ризиків об'єктивної та суб'єктивної складових частин;

6) візуалізація результатів обчислень.

Надання ризику у вигляді комплексного числа, з урахуванням об'єктивної та суб'єктивної скла-

дових частин, відкриває перспективи побудови моделей поведінки з ризиками на основі застосування апарату теорії функцій комплексної змінної.

Структурно-аналітичне відображення розробленої методології оцінки ризиків представлена на рис. 3.

Використовуючи запропоновану в цій статті методологію, можливо побудувати програмні і апаратно-програмні системи, які базуються на використанні методів розрахунку суми ризиків та обчислення комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

Висновки. Отже, отримані результати можуть бути використані під час визначення ризику складного проекту (може бути складна інформаційна система), що характеризується наслідками під час реалізації даного проекту і ймовірністю цих наслідків, а також дають підстави для прийняття рішень про економічну доцільність застосування заходів зі зменшення ризику.

Список літератури:

1. Jinsoo Shin, Hanseong Son, Gyunyoung Heo. Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET. *Nuclear Engineering and Technology*. Vol. 49. Issue 3. 2017. P. 517–524.

2. Petar Radanlieva, David Charles De Rourea, Razvan Nicolescub, Michael Huthb, Rafael Mantilla Montalvoc, Stacy Cannadyc, Peter Burnap. Future developments in cyber risk assessment for the internet of things. *Computers in Industry*. Vol. 102. 2018. P.14–22.

3. Мохор В.В., Гончар С.Ф., Дибач О.М. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури. *Ядерна та радіаційна безпека*. 2019. № 2 (82). С. 57–61.

4. Mansour Alali, Ahmad Almogren, Mohammad Mehedi Hassan, Iehab A.L. Rassan, Md Zakirul Alam Bhuiyan Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*. Vol. 74. 2018. P. 323–339.

5. Derek Young, Juan Lopez Jr., Mason Rice, Benjamin Ramsey, Robert McTasney. A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*. Vol. 14. 2016. P.43-57.

6. Martin Eling, Jan Wirfs. What are the actual costs of cyber risk events? *European Journal of Operational Research*. 2019. Vol. 272, Issue 3. P. 1109–1119.

7. Jain P., Pasman H. J., Waldram S., Pistikopoulos E.N., Mannan M.S. Process Resilience Analysis Framework (PRAF) : A systems approach for improved risk and safety management. *Journal of Loss Prevention in the Process Industries*. 2018. Vol. 53. P. 61–73.

8. Terje Aven. Risk assessment and risk management : Review of recent advances on their foundation. *European Journal of Operational Research*. 2016. Vol. 253. Issue 1. P. 1–13.

9. Rowe W. D. An Anatomy of Risk. *Environmental Protection Agency*. Washington, 1975. 125 p.

10. Мохор В.В., Гончар С.Ф. Идея построения алгебры рисков на основе теории комплексных чисел. *Електронне моделювання*. 2018. Т.40. № 4. С. 107–111.

Honchar S.F. METHODOLOGY FOR RISK ASSESSMENT OF CYBER SECURITY OF INFORMATION SYSTEMS OF OBJECTS OF CRITICAL INFRASTRUCTURE

The paper proposes a methodology for estimating the amount of cybersecurity risks of the information system of critical infrastructure facilities. The relevance of this methodology of cybersecurity risk assessment of information systems of critical infrastructure objects in the creation of information security management systems and a comprehensive information security system of such information systems is proved. It is shown that the economic feasibility of the application and selection of various risk management measures, including both organizational and technical ones, is determined by the estimated comparison of the cost of such measures with the maximum amount of losses due to the effect of several risks. The result of assessing the amount of such risks provides a basis for deciding on the acceptability of their level and the need or economic feasibility of their further treatment. In this article, under the sum of risks we understand a certain amount, which is determined by the losses as a result of realization of all component risks, and the probability of realization of these risks. The methodology proposed in the article is based on the application of methods for calculating the amount of risk and calculating the complex risk. It is shown that the risk can be represented as a complex number. The methods of calculation of the sum of risks and calculation of complex risk are presented. Based on the methodology proposed in this article, it is possible to develop a set of structural solutions for computer systems risk assessment of cybersecurity information systems that implement methods of calculating the sum of risks and calculating complex risk, as well as build software and hardware-software systems based on the use of calculation methods and computing complex cyber security risk information for critical infrastructure facilities. The results obtained can be used to determine the risk of a complex project (may be a complex information system), characterized by the consequences of the implementation of the project and the likelihood of these consequences.

Key words: *cybersecurity, risk, critical infrastructure, information system, methodology.*