APPLICATION OF GENERATORS OF PSEUDO-RANDOM NUMBERS AND SEQUENCES IN CYBER SECURITY, METHODS OF THEIR CONSTRUCTION AND QUALITY ASSESSMENT

Due to the rapid development of computing and measurement technology, as well as the implementation of advanced technologies, the scope of application for pseudo-random number generators and pseudo-random sequences has significantly expanded, placing new demands on their design and quality evaluation methods. Quality pseudo-random sequences, although essentially deterministic, possess nearly all the properties of true random processes and successfully replace them, as the generation of random sequences is extremely complex. Due to the diversity and wide range of tasks that require the use of pseudo-random numerical sequences, new algorithms, methods, and tools for obtaining such sequences are constantly being developed and improved. Using pseudo-random sequence generators, one can obtain sequences of numbers where each element is practically independent of others and follows a specific prescribed distribution law, with the uniform distribution being the most common. Thanks to their statistical properties and generation speed, pseudo-random number and sequence generators are essential tools in various fields, including simulation modeling (economic, mathematical, physical, medical research, military applications), computer game development (generation of 3D models, textures, and worlds, as well as creating diversity and randomness in the behavior of characters and events), and measurement technology. Overall, it's important to note that developers of pseudo-random sequence generators face a set of stringent requirements regarding specific characteristics of the results they create using these generators. These requirements can vary depending on the generator's intended purpose and can be particularly high and demanding when pseudo-random sequences are used in cyber-security and information protection. For example, for cryptographic applications, the requirements are extremely rigorous and may sometimes even contradict each other. To verify whether the generated sequence meets the specified criteria and requirements, it is necessary to evaluate its quality, which involves assessing various features and parameters. Since the development of pseudo-random sequence generators aims to make them resemble sequences of truly random numbers, the basis for any evaluation of generators lies in comparing the statistical characteristics of the generated sequence with the characteristics of truly random sequences. For this purpose, various tests are used, which allow the detection of existing statistical regularities and, thus, the identification of low-quality pseudo-random sequences.

Keywords: pseudorandom number generators, pseudorandom sequence generators, cyber security, generation, testing, quality assessment.

Хомік Марія Анатоліївна, студентка 3-го курсу, спеціальності «Кібербезпека» Національного університету «Львівська політехніка».

Mariia Khomik, A third-year student the Department of Information Security, National University "Lviv Polytechnic".
E-mail: mariia.khomik.kb.2021@lpnu.ua.
Orcid ID: 0009-0004-6031-5618.

Гарасимчук Олег Ігорович, к.т.н., доцент, доцент кафедри захисту інформації Національного університету «Львівська політехніка».

Oleh Harasymchuk, Ph.D., Associate Professorat the Department of Information Security, National University "Lviv Polytechnic".
E-mail: oleh.i.harasymchuk@lpnu.ua.
Orcid ID: 0000-0002-8742-8872.

DOI: 10.18372/2410-7840.25.17941
УДК 004.056.5

МЕТОДОЛОГІЯ ОЦІНКИ СУМИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сергій Гончар, Олександр Потенко

Для визначення економічної доцільності застосування і вибору тих чи інших заходів по обробці ризику проекту у цілому, включаючи як організаційні, так і технічні, необхідно здійснити оціночне порівняння вартості таких заходів з максимальною величиною збитків в результаті дії декількох ризиків. В роботі запропонована методологія оцінки суми ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури. Запропонована у статті методологія базується на застосуванні методів розрахунку суми ризиків і обчислення комплексного ризику. На підставі запропонованої в даній статті методології представлено структурні рішення обчислювальних систем оцінки ризику кібербезпеки інформаційних систем, що реалізують методи

розрахунку суми ризиків та обчислення комплексного ризику, а також побудовані програмні системи. Отримані результати можуть бути використані при визначенні ризику складного проекту (може бути складна інформаційна система), що характеризується наслідками при реалізації даного проекту і ймовірністю цих наслідків.

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

ВСТУП

На сьогоднішній день 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 відносно недавно питання безпеки об'єктів критичної інфраструктури держави вирішувалося по двох основних напрямках: 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 і 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 із забезпечення кібербезпеки. У відповідності 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 їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем. Забезпечення кібербезпеки досягається створенням системи управління інформаційною безпекою (СУІБ) у відповідності до міжнародного стандарту ISO/IEC 27001:2013 та/або створенням комплексної системи захисту інформації (КСЗІ) у відповідності 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 вдосконалення існуючих, 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 по мінімізації цих ризиків. Економічна доцільність застосування і вибір тих чи інших заходів по обробці ризику, включаючи як організаційні, так і технічні, визначається оціночним 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 їх рівня і необхідності чи економічної доцільності їх подальшої обробки. Під сумою ризиків будемо розуміти певну величину, що визначається збитками у результаті реалізації усіх складових ризиків, і ймовірністю реалізації цих ризиків. Така задача являється актуальною для визначення ризику складного проекту (може бути складна інформаційна система), що характеризується наслідками при реалізації даного проекту і ймовірністю цих наслідків.

Існуючі підходи до визначення поняття ризиків та методи їх 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 [1-6]. Разом з тим, невирішеним залишається питання,

пов'язане із можливістю розрахунку суми ризиків, що дало би можливість здійснення кількісної оцінки ризику проекту у цілому або вибраного напряму розвитку процесу.

Таким чином, на сучасному етапі розвитку науки і техніки існує об'єктивне протиріччя 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 вирішенню 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.

ОСНОВНА ЧАСТИНА

Існує досить багато понять «ризик». Одне з них визначає ризик R, як ймовірність або можливість p настання випадкової події, що приводить 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, існує n ризиків, де кожен ризик представлений графіком функції (2) і визначається ймовірністю настання випадкової події (рис.1), що приводить до певних збитків (точки 4, 5, 6).

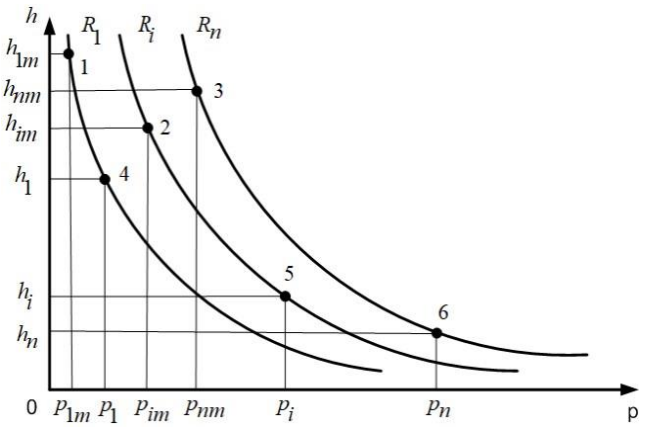

Рис. 1. Визначення суми ризиків

Метод визначення суми ризиків передбачає послідовного визначення: максимальних значень збитків для кожного ризику; ймовірності виникнення подій (рис.1), що призводять до максимальних збитків (точки 1, 2, 3),; 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 їх виникнення.

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

Велику роль при оцінці 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 в сфері управління ризиками в значній мірі залежить від відчуття ризику. Доцільність урахування суб'єктивного ризику підтверджується дослідженнями, проведеними в [7].

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

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

Як показують дослідження [8], повний ризик можна представити у вигляді комплексного числа:

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

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

При цьому, 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 ризику над іншою.

Маємо схематичне відображення методу обчислення комплексного ризику (рис. 2).

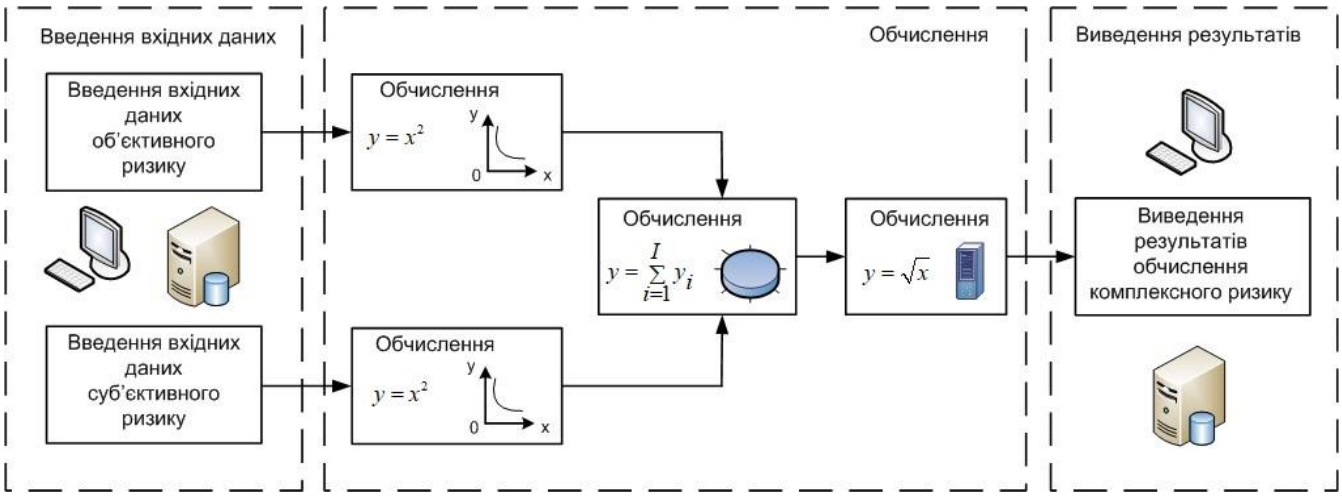

Рис. 2. Схематичне відображення методу обчислення комплексного ризику

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

- 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;

- введення вхідних даних: введення вхідних даних здійснюється в модуль пам'яті і далі в модуль обчислення. В модулі пам'яті формується база даних вхідних даних та результатів обчислень;

- обчислення суми ризиків об'єктивної складової;

- обчислення суми ризиків суб'єктивної складової;

- визначення суми ризиків об'єктивної і суб'єктивної складових;

- візуалізація результатів обчислень.

Надання ризику у вигляді комплексного числа, з урахуванням об'єктивної та суб'єктивної складових, відкриває перспективи побудови моделей поведінки з ризиками на основі застосування апарату теорії функцій комплексної змінної.

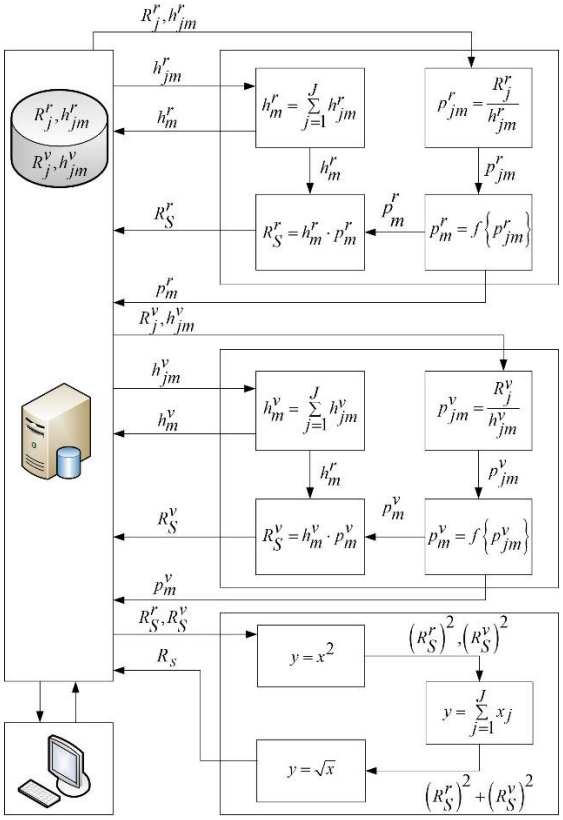

Рис. 3. Структурно-аналітичне відображення розробленої методології оцінки ризиків.

Маємо структурно-аналітичне відображення розробленої методології оцінки ризиків (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.

На підставі даної методології вперше розроблено структурні рішення обчислювальних систем розрахунку суми ризиків (рис. 4), та обчислення комплексного ризику кібербезпеки інформаційних систем (рис.5).

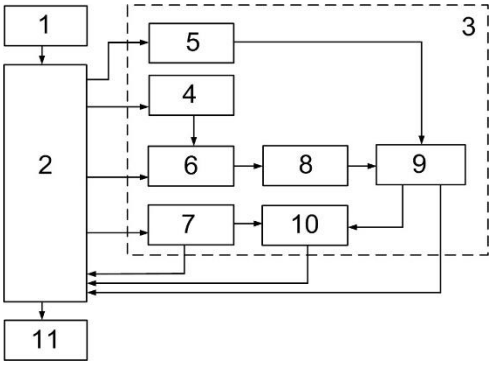

Рис. 4. Структурне рішення обчислювальної системи суми ризиків

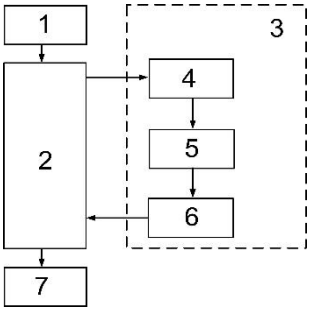

Рис. 5. Структурне рішення обчислювальної системи розрахунку комплексного ризику

Структурне рішення обчислювальної системи розрахунку суми ризиків (рис. 4), яке, за рахунок використання модулів введення, обчислення і аналізу даних, блоків розрахунку, визначення та формування даних, дозволяє здійснювати автоматизований розрахунок наслідків від дії сумісних подій, з урахуванням показників, таких як ймовірність виникнення подій, що призводять до наслідків, та величина цих наслідків.

До складу обчислювальної системи (рис. 4) входять: модуль введення початкових даних 1, блок пам'яті 2, модуль обчислення і аналізу даних 3, модуль виведення та візуалізації інформації 11, модуль обчислення і аналізу даних 3 містить блоки формування масиву ризиків подій 4, блок розрахунку значення максимальних збитків у результаті суми ризиків 5, блок формування масиву ймовірностей виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику 6, блок визначення ймовірності суми ризиків сумісних випадкових подій 7, блок визначення ймовірності події, що призводить до суми ризиків з максимальними наслідками для кожної події 8, блок розрахунку суми ризиків в умовах дії ризиків 9, блок розрахунку збитків при дії суми ризиків 10.

Структурне рішення обчислювальної системи комплексного ризику (рис. 5), яке, за рахунок використання модулів введення, обчислення і аналізу даних, блоків розрахунку, визначення та формування даних, дозволяє здійснювати автоматизований розрахунок повного ризику, з урахуванням об'єктивної та суб'єктивної його складових, з використанням теорії векторної алгебри та комплексних чисел.

До складу обчислювальної системи (рис. 5) входять: модуль введення початкових даних 1, блок пам'яті 2, модуль обчислення і аналізу даних 3, модуль виведення та візуалізації інформації 7, модуль обчислення і аналізу даних 3 містить блок розрахунку квадрату вхідних даних 4, блок сумматора вхідних даних 5, блок розрахунку квадратного кореня 6.

На базі запропонованої методології та структурних рішень обчислювальних систем розроблено алгоритмічне забезпечення для реалізації відповідного програмного забезпечення і на їх основі розроблено прикладні програмні системи.

Маємо інтерфейс програмної системи розрахунку суми ризиків, наслідків від цих ризиків, ймовірності настання цих наслідків (рис. 6).

Використовуючи запропоноване програмне забезпечення виконано обчислення суми ризиків: від загроз, що можуть виникнути під час мережевої взаємодії, від загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням, від загроз, що можуть виникнути в мережевих операційних системах інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу.

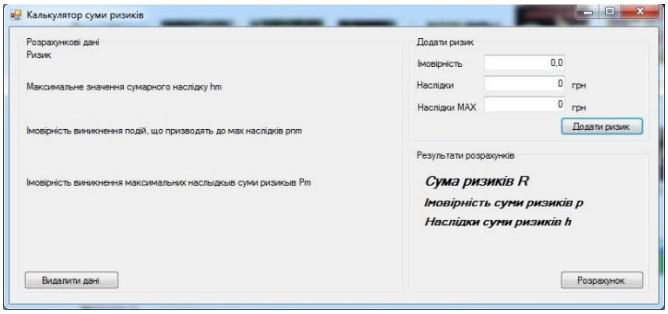

Рис. 6. Інтерфейс програми

В результаті роботи програмного засобу (рис. 7) здійснено розрахунок значення сум ризиків від загроз, що можуть виникнути під час мережевої взаємодії, від загроз, що можуть виникнути під час роботи з прикладним програмним забезпеченням, від загроз, що можуть виникнути в мережевих операційних системах інформаційно-телекомунікаційної системи захищеного вузлу Інтернет доступу. Також здійснено розрахунок значення наслідків при реалізації кожної з груп загроз і ймовірність виникнення цих наслідків.

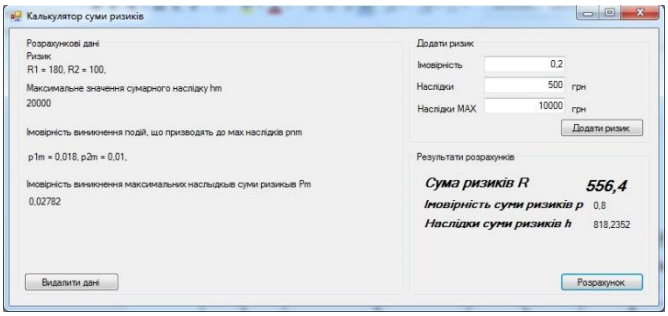

Рис. 7. Приклад розрахунку

ВИСНОВКИ

Отримані результати можуть бути використані при визначенні ризику складного проекту (може бути складна інформаційна система), що характеризується наслідками при реалізації даного проекту і ймовірністю цих наслідків, а також дають підстави для прийняття рішень про економічну доцільність застосування заходів по зменшенню ризику.

ЛІТЕРАТУРА

[1] 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. pp.14-22.

[2] 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.

[3] MansourAlali, AhmadAlmogren, Mohammad MehediHassan, 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. pp. 323-339.

[4] 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. pp. 43-57.

[5] Martin Eling, Jan Wirfs. What are the actual costs of cyber risk events? European Journal of Operational Research. 2019. Vol. 272, Issue 3. pp. 1109-1119.

[6] 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. pp. 61-73.

[7] Rowe W. D. An Anatomy of Risk. Environmental Protection Agency. Washington, 1975. 125 p.

[8] Мохор В.В., Гончар С.Ф. Идея построения алгебры рисков на основе теории комплексных чисел // Електронне моделювання. 2018. Т.40. №4. С. 107-111.

METHODOLOGY FOR ASSESSMENT THE SUM OF CYBERSECURITY RISKS OF THE INFORMATION SYSTEM OF OBJECTS OF CRITICAL INFRASTRUCTURE

To determine the economic feasibility of the application and selection of certain measures to handle the risk of the project as a whole, including both organizational and technical, it is necessary to make an estimated comparison of the cost of such measures with the maximum amount of losses resulting from several risks. The paper proposes a methodology for assessing the amount of cybersecurity risks of the information system of critical infrastructure facilities. The methodology proposed in the article is based on the application of methods for calculating the sum of risks and calculating complex risk. Based on the methodology proposed in this article, structural solutions of computing systems for assessing the risk of cybersecurity of information systems that implement methods for calculating the sum of risks and calculating complex risk are presented, as well as software systems are built. The results can be used to determine the risk of a complex project (there may be a complex information system), characterized by the con-

sequences of the project and the likelihood of these consequences.
Keywords: cybersecurity, risk, critical infrastructure, information system, methodology.

Гончар Сергій Феодосійович, кандидат технічних наук, учений секретар Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

Serhii Honchar, PhD in Eng., Scientific Secretary of Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine (Kyiv, Ukraine).
E-mail: sfgonchar@gmail.com.
Orcid ID: 0000-0002-9978-8998.

Потенко Олександр Сергійович, провідний інженер Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

Alexander Potenko, Senior Engineer of Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine (Kyiv, Ukraine).
E-mail: alexpo84@gmail.com.
Orcid ID: 0009-0009-4067-1267.