ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ МОДЕЛЮВАННЯ

doi: <https://doi.org/10.15407/emodel.41.06.065>

УДК 004.056.5

В.В. Мохор, чл.-кор. НАН України, **С.Ф. Гончар**, канд. техн. наук
Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України
(Україна, 03164, Київ, вул. Генерала Наумова, 15,
тел. (044) 4241466; e-mail: Serhii Honchar [sfgonchar@gmail.com])

Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури

Обґрунтовано поняття комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури (ІСОКІ). Запропоновано векторну модель ризику та модель комплексного ризику. Запропоновано методи обчислення сумарного ризику і комплексного ризику. Розроблено структурні рішення обчислювальних систем для розрахунку сумарного ризику кібербезпеки ІСОКІ з використанням запропонованих методів.

К л ю ч о в і с л о в а: ризик, комплексний ризик, векторна модель ризику, модель комплексного ризику, об'єктивний ризик, суб'єктивний ризик.

Події останніх років в Україні і у світі свідчать про нагальну необхідність забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури (ІСОКІ), особливо енергетичного сектору. Власники ІСОКІ прагнуть звести до мінімуму ризику кібербезпеки, а також зменшити витрати на заходи по мінімізації цих ризиків. Економічна доцільність застосування і вибір заходів по обробці ризику, включаючи організаційні і технічні, визначається оціночним порівнянням вартості таких заходів з максимальною величиною збитків в результаті дії декількох ризиків.

Результати оцінювання сумарного ризику дозволяють приймати рішення щодо їх рівня і необхідності чи економічної доцільності їх подальшої обробки. Сумарним ризиком будемо вважати певну величину, яка визначається збитками в результаті реалізації усіх складових ризиків і ймовірністю реалізації цих ризиків. Така задача є актуальною для визначення ризику кібербезпеки ІСОКІ в цілому з урахуванням критичних особливостей таких інформаційних систем у порівнянні з традиційними

© Мохор В.В., Гончар С.Ф., 2019

системами інформаційних технологій, а також з урахуванням ризику людського чинника при прийнятті управлінського рішення.

Дослідженню проблем, пов'язаних із процесом оцінювання ризику кібербезпеки ІСОКІ присвячена значна частина публікацій вітчизняних і зарубіжних вчених [1—10]. Але існуючі підходи до визначення поняття ризиків та методи їх оцінювання недостатньо повно описують це поняття, не враховують суб'єктивний ризик, що ускладнює коректне його оцінювання. Невирішеним залишається питання, пов'язане із можливістю розрахунку суми ризиків. Вирішення цього питання уможливило б здійснення кількісного оцінювання ризику в цілому та врахування при оцінюванні ризику впливу людського чинника, що є надзвичайно актуальним для об'єктів критичної інфраструктури, особливо в енергетичному секторі. Незважаючи на значну кількість підходів до вирішення даної проблеми, вона залишається актуальною не тільки для України, але і для всієї світової спільноти.

Мета проведених досліджень — обґрунтувати поняття комплексного ризику кібербезпеки ІСОКІ, створити векторну модель ризику та модель комплексного ризику, запропонувати методи обчислення сумарного ризику, комплексного ризику та розробити структурні рішення обчислювальних систем для розрахунку сумарного ризику кібербезпеки ІСОКІ з використанням запропонованих методів.

Найбільш небезпечними для об'єктів критичної інфраструктури, особливо в енергетичному секторі, є аварійні режими внаслідок помилок управлінських рішень експлуатаційного персоналу — інсайдера. Водночас, основна особливість функціонування об'єкту критичної інфраструктури, у тому числі енергетичної системи, вимагає наявності інсайдера як єдиного управління процесом роботи усієї системи.

Головна відмінність інсайдера від зовнішнього порушника полягає у тому, що інсайдер має легітимний доступ до системи. Натомість, зовнішній порушник прикладає зусилля, щоб подолати систему захисту, прагнучи отримати доступ до інформації. Зазвичай інсайдер отримує цю інформацію абсолютно безперешкодно в межах своєї компетенції або незаконно розширюючи свої права і можливості. Тому будь-який захист системи від зовнішнього порушника виявляється неефективним відносно інсайдера. При цьому зовнішній порушник може здійснювати кібератаки на програмно-апаратну складову інформаційної системи, використовуючи вразливість системи захисту інформації об'єкту критичної інфраструктури, або чинити інформаційно-психологічний вплив на інсайдера (зовнішні дестабілізуючі чинники).

Рис. 1. Структурна модель взаємодії елементів ІСОКІ

Окрім зовнішніх дестабілізуючих чинників до можливих деструктивних дій інсайдера можуть спонукати внутрішні дестабілізуючі чинники, а саме людські потреби, через захищеність яких може здійснюватися забезпечення кібербезпеки ІСОКІ, а також власні ненавмисні помилки. У залежності від того, які чинники спонукають інсайдера на деструктивні дії, його дії поділяють на типи в залежності від мети, мотивації і послідовності дій.

Необхідно зазначити наступне: якщо інсайдер отримує доступ до активів ІСОКІ, незаконно розширюючи свої права та можливості, для цього йому необхідна наявність сприятливих умов. У випадку отримання інсайдером доступу до активів ІСОКІ у межах своєї компетенції необхідності у сприятливих умовах немає. Крім того, у цьому випадку інсайдером здійснюється обхід системи захисту інформації.

Розглянемо структурну модель взаємодії елементів ІСОКІ і вплив кожної з її складових (організаційна, технічна, персонал) на забезпечення кібербезпеки такої системи (рис. 1). Загроза кібербезпеці інформаційної системи, яка циркулює в ІСОКІ, буде вважатися актуальною, якщо для вказаної ІСОКІ з заданими структурно-функціональними характеристиками і особливостями функціонування існує ймовірність реалізації розглянутої загрози порушником з відповідним потенціалом і її реалізація призведе до неприйнятних збитків від порушення конфіденційності, цілісності або доступності інформації. Небезпека загрози в ІСОКІ визначається оцінюванням можливих наслідків від її реалізації щодо впливу

на функціонування цих систем, а рівень тяжкості таких наслідків — коефіцієнтом небезпеки даної загрози.

Актуальність n -ї загрози кібербезпеці інформаційної системи у загальному вигляді можна описати так:

$$A_n = f \{P(R_{nu} | K_n); H_n\},$$

де $P(R_{nu} | K_n)$ — ймовірність реалізації n -ї загрози з використанням u -ї уразливості за умови наявності сприятливих для цього умов K_n ; H_n — наслідки від реалізації n -ї загрози кібербезпеці ІСОКІ.

Визначимо оцінку ймовірності (можливості) реалізації загрози кібербезпеці інформаційної системи. Ймовірність реалізації загрози кібербезпеці інформаційної системи визначаємо експертним методом (з урахуванням структурно-функціональних характеристик і особливостей функціонування інформаційної системи) за допомогою градації даного показника щодо n -ї загрози, який залежить від наступних факторів:

наявності чи відсутності сприятливих умов для реалізації n -ї загрози K_n ;

наявності чи відсутності необхідної статистики щодо фактів реалізації n -ї загрози (виникнення інцидентів порушення кібербезпеки інформаційної системи) S_n ;

наявності чи відсутності у потенційних порушників мотивації для реалізації n -ї загрози внутрішніх та (або) зовнішніх дестабілізуючих чинників, тобто модель порушника та модель загроз інформаційної системи об'єкта критичної інфраструктури q_n ;

можливої частоти реалізації n -ї загрози ω_n .

Можливість реалізації n -ї загрози кібербезпеці інформаційної системи можна оцінити, враховуючи рівень захищеності інформаційної системи і потенціал порушника, необхідні для реалізації цієї загрози безпеці інформації в ІСОКІ із заданими структурно функціональними характеристиками і особливостями функціонування. Можливість реалізації n -ї загрози подамо у вигляді, $W(R_n) = f(X_n; Y_n)$ де X_n — рівень захищеності ІСОКІ щодо реалізації n -ї загрози; Y_n — потенціал порушника, необхідний для реалізації n -ї загрози, тобто модель загроз.

Для оцінювання ступеня можливого збитку H_n від реалізації n -ї загрози безпеці інформації необхідно визначити можливий результат реалізації загрози кібербезпеці в ІСОКІ, вид збитку, до якого може призвести реалізація загрози кібербезпеці інформаційної системи, ступінь наслідків від реалізації загрози безпеці інформації для кожного виду збитку.

Ступінь можливих наслідків H_n від реалізації n -ї загрози кібербезпеці інформаційної системи визначається ступенем негативних наслідків від порушення конфіденційності, цілісності або доступності кожного виду інформації, яка циркулює в ІСОКІ.

Отже, ступінь негативних наслідків від порушення конфіденційності, цілісності або доступності інформації визначається для кожного виду збитку, залежить від цілей і завдань, які виконуються інформаційною системою об'єкта критичної інфраструктури, і може мати різні значення для різних власників інформації і операторів та визначається експертним методом.

Загальний вигляд схематичного зображення методу визначення актуальності загрози кібербезпеці ІСОКІ показано на рис. 2. За результатами проведеного оцінювання приймаються рішення щодо впровадження відповідних заходів, спрямованих на ефективне та своєчасне блокування (нейтралізацію) загроз безпеці інформації, реалізація яких може мати негативні наслідки.

Прийняття рішень у сфері управління ризиками в значній мірі залежить від людського чинника, який має суб'єктивний характер. Тому коректне кількісне оцінювання повного ризику можливе через визначення комплексного ризику. Комплексним ризиком будемо вважати ризик, який включає в себе складові об'єктивного та суб'єктивного ризиків.

Ризики мають конкретні значення. Водночас, ризик може зменшуватися або збільшуватися, змінюючи напрям, зберігаючи при цьому знак. Тому ризики, як об'єктивні, так і суб'єктивні, мають напрямки та значення і їх можна подати у вигляді векторів.

Для визначення комплексного ризику необхідно додати об'єктивний і суб'єктивний ризики. Але алгебраїчно додавати ці два ризики неможливо через те, що вони різні за характером. При вирішенні такої задачі виникає необхідність отримувати числові характеристики векторів (довжини) та їх взаємного розміщення (кут між векторами).

Результати досліджень [11—13] показують, що для двовимірного векторного простору, у якому подано вектори ризиків $R_1 = p_1 \cdot h_1$ та $R_2 = p_2 \cdot h_2$, задано скалярний добуток цих векторів і справедливі аксіоми, характерні для евклідового простору. Це означає, що зазначений векторний простір є двовимірним евклідовим простором. Наявність скалярного добутку дозволяє ввести довжину вектора, кут між векторами, поняття проєкції вектора на вісь, поняття ортогональності векторів.

Рис. 2. Схематичне відображення методу визначення актуальності загрози

З урахуванням викладеного створено векторну модель ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури (рис. 3). Використовуючи векторну модель ризиків і подаючи вектор комплексним числом, пропонуємо модель комплексного ризику, зображену на рис. 4.

На основі векторної моделі ризиків та моделі комплексного ризику розроблено метод розрахунку комплексного ризику кібербезпеки ІСОКІ. Метод передбачає введення вхідних параметрів об'єктивного та суб'єктивного ризиків, які враховують вплив людського чинника, обчислення згідно до розроблених моделей та виведення результатів обчислень. Схематичне відображення методу наведено на рис. 5.

За допомогою розроблених методів можна побудувати системи (як програмні, так і апаратно-програмні), спрямовані на оцінювання суми ризиків кібербезпеки ІСОКІ. Комплекс структурних моделей (рішень) обчислювальних систем оцінювання ризику кібербезпеки інформаційних

Рис. 3. Векторна модель ризику

Рис. 4. Модель комплексного ризику

систем, що реалізують запропоновані методи, показано на рис. 6, а структурне рішення апаратно-програмного комплексу оцінки та аналізу ризику, базованого на запропонованому методі, — на рис. 7.

Структурна модель обчислювальної системи «калькулятор ризиків», схема якої зображена на рис. 6, а, за допомогою модулів введення, обчислення і аналізу даних, блоків розрахунку, визначення та формування даних дозволяє здійснювати автоматизований розрахунок наслідків дії сумісних подій з урахуванням їх ймовірності. Результати обчислень ви-

Рис. 5. Схематичне відображення методу обчислення комплексного ризику

водяться на пристрій відображення інформації, що міститься у модулі виведення та візуалізації інформації 11, і в блок пам'яті 2.

Структурна модель обчислювальної системи «калькулятор комплексного ризику», схема якої зображена на рис. 6, б, за допомогою модулів введення, обчислення і аналізу даних, блоків розрахунку, визначення та формування даних, що реалізують метод розрахунку суми ризиків, дозволяє здійснювати автоматизований розрахунок повного ризику з урахуванням об'єктивної та суб'єктивної його складових з використанням теорії векторної алгебри та комплексних чисел. Результати обчислень виводяться на пристрій відображення інформації, що міститься у модулі 7, і в блок пам'яті 2.

Рис. 6. Блок-схеми структурних моделей обчислювальних систем: *а* — 1 — модуль введення початкових даних; 2 — блок пам'яті; 3 — модуль обчислення і аналізу даних; 4 — блок формування масиву ризиків подій; 5 — блок розрахунку значення максимальних збитків у результаті суми ризиків; 6 — блок формування масиву ймовірностей подій, що призводять до максимальних наслідків в умовах дії кожного ризику; 7 — блок визначення ймовірності суми ризиків сумісних випадкових подій; 8 — блок визначення ймовірності події, що призводить до суми ризиків з максимальними наслідками для кожної події; 9 — блок розрахунку суми ризиків в умовах дії ризиків; 10 — блок розрахунку збитків при дії суми ризиків; 11 — модуль виведення та візуалізації інформації; *б* — 1 — модуль введення початкових даних; 2 — блок пам'яті; 3 — модуль обчислення і аналізу даних; 4 — блок розрахунку квадрату вхідних даних; 5 — блок суматора вхідних даних; 6 — блок розрахунку квадратного кореня; 7 — модуль виведення та візуалізації інформації.

Запропоновані обчислювальні системи можуть бути використані як частина системи підтримки прийняття рішень.

Висновки

Запропоновані методи дозволяють розраховувати суму визначеної множини ризиків, загальні наслідки та ймовірність їх реалізації, а також здійснювати оцінювання зазначених ризиків з урахуванням впливу людського чиннику.

Розроблені векторна модель та модель комплексного ризику кібербезпеки ІСОКІ дозволяють ввести метрику векторів ризиків та здійснювати векторні операції над ними.

За допомогою структурних моделей обчислювальних систем для розрахунку суми ризиків кібербезпеки ІСОКІ можна автоматизувати процес розрахунку сумарного ризику та виконувати обчислення комплексного ризику з урахуванням об'єктивної та суб'єктивної складових.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Eling M., Wirfs J. What are the actual costs of cyber risk events? // *European Journal of Operational Research*, 2019, № 272, с. 1109—1119.
2. Radanliev P., De Roure D. C., Nicolescu R. et al. Future developments in cyber risk assessment for the internet of things // *Computers in Industry*, 2018, № 102, p. 14—22.
3. Sheehan B., Murphy F., Mullins M., Ryan C. Connected and autonomous vehicles: A cyber-risk classification framework // *Transportation Research Part A: Policy and Practice*, 2019, № 124, p. 523—536.
4. Renaud K., Flowerday S., Warkentin M. et al. Is the responsabilization of the cyber security risk reasonable and judicious? // *Computers & Security*, 2018, № 78, p. 198—211.
5. Ruan K. Chapter 4 - Cyber Risk Measurement in the Hyperconnected World // *Digital Asset Valuation and Cyber Risk Management*, 2019, p. 75—86.
6. Stine I., Rice M., Dunlap S., Pecarina J. A cyber risk scoring system for medical devices // *International Journal of Critical Infrastructure Protection*, 2017, № 19, p. 32—46.
7. Wang S.S. Integrated framework for information security investment and cyber insurance // *Pacific-Basin Finance Journal*, 2019, № 57, p. 101—173.
8. Tianlei Z., Shibin G., Baoxu L. et al. Integrated fault propagation model based vulnerability assessment of the electrical cyber-physical system under cyber attacks // *Reliability Engineering & System Safety*, 2019, № 189, p. 232—241.
9. Akinrolabu O., Nurse J.R.C., Martin A., New S. Cyber risk assessment in cloud provider environments: Current models and future needs // *Computers & Security*, 2019, № 87, p. 101—106.
10. Boiko A., Shendryk V., Boiko O. Information systems for supply chain management: uncertainties, risks and cyber security // *Procedia Computer Science*, 2019, № 149, p. 65—70.
11. 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.
12. Мохор В.В., Гончар С.Ф. Дослідження правомірності подання ризиків векторами у евклідовому просторі // *Електрон. моделювання*, 2019, **41**, № 4, с. 73—84.
13. Мохор В.В., Гончар С.Ф. Идея построения алгебры рисков на основе теории комплексных чисел // *Там же*, 2018, **40**, № 4, с. 107—111.

Отримано 25.10.19

REFERENCES

1. Eling, M. and Wirfs, J. (2019), "What are the actual costs of cyber risk events?", *European Journal of Operational Research*, no. 272, pp. 1109-1119.
2. Radanliev, P., Charles De Roure, D. and Nicolescu, R. (2018), "Future developments in cyber risk assessment for the internet of things", *Computers in Industry*, no. 102, pp. 14-22.
3. Sheehan, B., Murphy, F., Mullins, M. and Ryan, C. (2019), "Connected and autonomous vehicles: A cyber-risk classification framework", *Transportation Research Part A: Policy and Practice*, no. 124, pp. 523-536.
4. Renaud, K., Flowerday, S. and Warkentin, M. (2018), "Is the responsabilization of the cyber security risk reasonable and judicious?", *Computers & Security*, no. 78. pp. 198-211.
5. Ruan, K. (2019), "Cyber Risk Measurement in the Hyperconnected World", *Digital Asset Valuation and Cyber Risk Management*, Chapter 4, pp. 75-86.

6. Stine, I., Rice M., Dunlap, S. and Pecarina, J. (2017), "A cyber risk scoring system for medical devices", *International Journal of Critical Infrastructure Protection*, no. 19, pp. 32-46.
7. Shaun, S.W. (2019), "Integrated framework for information security investment and cyber insurance", *Pacific-Basin Finance Journal*, no. 57, pp. 101-173.
8. Tianlei, Z., Shibin, G. and Baoxu, L. (2019), "Integrated fault propagation model based vulnerability assessment of the electrical cyber-physical system under cyberattacks", *Reliability Engineering & System Safety*, no. 189, pp. 232-241.
9. Akinrolabu, O., R.C. Nurse, J., Martin, A. and New, S. (2019), "Cyber risk assessment in cloud provider environments: Current models and future needs", *Computers & Security*, no. 87, pp. 101-106.
10. Boiko, A., Shendryk, V. and Boiko, O. (2019), "Information systems for supply chain management: uncertainties, risks and cyber security", *Procedia Computer Science*, no. 149, pp. 65-70.
11. Mokhor, V., Gonchar, S. and Dybach, O. (2019), "Methods for the Total Risk Assessment of Cybersecurity of Critical Infrastructure Facilities", *Yaderna ta radiatsiyna bezpeka*, no. 2, pp. 57-61.
12. Mokhor, V. and Gonchar, S. (2019), "Research of Validity of Presentation of Risks by Vectors in the Euclidean Space", *Elektronne modelyuvannya*, Vol.41, no. 4, pp. 73-84.
13. Mokhor, V. and Gonchar, S. (2018), "The Idea of the Construction of the Algebra of Risks on the Basis of the Theory of Complex Numbers", *Elektronne modelyuvannya*, Vol. 40, no. 4, pp. 107-111.

Received 25.10.19

B.B. Мохор, С.Ф. Гончар

ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Обосновано понятие комплексного риска кибербезопасности информационных систем объектов критической инфраструктуры (ИСОКИ). Предложены векторная модель риска и модель комплексного риска. Предложены методы вычисления суммарного риска и комплексного риска. Разработаны структурные решения вычислительных систем для расчета суммарного риска кибербезопасности ИСОКИ с использованием предложенных методов.

К л ю ч е в ы е с л о в а: риск, комплексный риск, векторная модель риска, модель комплексного риска, объективный риск, субъективный риск.

V.V. Mokhor, S.F. Honchar

EVALUATION OF RISKS OF CYBER SECURITY OF INFORMATION SYSTEMS OF OBJECTS OF CRITICAL INFRASTRUCTURE

The concept of complex cyber security risk of information systems of critical infrastructure objects is substantiated. The vector risk model and the integrated risk model are proposed. The methods of calculation of the total risk, complex risk are offered, the structural solutions of the computer systems are developed for the calculation of the total risk of cybersecurity of information systems of critical infrastructure objects using the proposed method.

К e y w o r d s: risk, complex risk, vector risk model, complex risk model, objective risk, subjective risk.

МОХОР Володимир Володимирович, чл.-кор. НАН України, д-р техн. наук, професор, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 1977 р. закінчив Київський ін-т цивільної авіації. Область наукових досліджень — математичне і комп'ютерне моделювання, спеціалізовані обчислювальні системи, інформаційна безпека.

ГОНЧАР Сергій Феодосійович, канд. техн. наук, пров. наук. співроб. Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 1997 р. закінчив Вінницький національний технічний університет. Область наукових досліджень — теорія ризиків безпеки, кібербезпека об'єктів критичної інфраструктури, у тому числі в енергетичній галузі.