УДК 004.056.5
Doi: https://doi.org/10.32918/nrs.2019.2(82).01

Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури

Мохор В. В.
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, м. Київ, Україна
ORCID:https://orcid.org/0000-0001-5419-9332

Гончар С. Ф.
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, м. Київ, Україна
ORCID:https://orcid.org/0000-0002-9978-8998

Дибач О. М.
Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Київ, Україна
ORCID: https://orcid.org/0000-0002-1807-8514

У роботі наведені результати аналізу вітчизняної та зарубіжної літератури за темою методів оцінки ризиків кібербезпеки, у тому числі об'єктів критичної інфраструктури, зазначається, що забезпечення кібербезпеки і оцінка ризиків кібербезпеки являється важливою проблемою об'єктів критичної інфраструктури. У роботі запропоновано графічний та аналітичний методи оцінки сумарного ризику кібербезпеки інформаційних систем, у тому числі об'єктів критичної інфраструктури. Зазначені методи оцінки сумарного ризику базуються на визначенні максимальних значень наслідків для кожного ризику. Показано, що максимальні значення наслідків кіберзагроз можуть бути визначені експертним шляхом, як максимальні збитки, що можуть бути завдані активам компанії. Запропоновані методи дають можливість визначати сумарний ризик кібербезпеки об'єктів критичної інфраструктури, сумарні збитки в результаті дії множини кіберзагроз, сумарну величину збитків в результаті дії однієї кіберзагрози за певний період часу, ймовірність виникнення максимальних втрат в результаті дії множини кіберзагроз. Приведено переваги даних методів оцінки сумарного ризику. На основі запропонованих методів можливо розробити методологію оцінки ризиків кібербезпеки інформаційних систем, у тому числі об'єктів критичної інфраструктури, будувати системи підтримки прийняття рішень щодо застосування заходів по зменшенню ризику. Визначається економічна доцільність застосування тих чи інших заходів по обробці ризику, включаючи як організаційні, так і технічні, здійснюється оціночне порівняння вартості таких заходів з максимальною величиною збитків в результаті дії сумарного ризику.

Ключові слова: сумарний ризик, кібербезпека, об'єкти критичної інфраструктури, кіберзагроза, метод оцінки ризику

На об'єктах критичної інфраструктури, включаючи об'єкти атомної енергетики, використовуються автоматизовані системи управління технологічними процесами, які включають в себе системи диспетчерського управління та збору даних, системи розподіленого управління та інші конфігурації систем управління. Кількість таких систем стає дедалі більшою.

На відміну від традиційних систем інформаційних технологій, в автоматизованих системах управління технологічними процесами об'єктів критичної інфраструктури існує досить тісний взаємозв'язок автоматизованих систем з фізичними процесами і виконавчими пристроями. Тому, порушення кібербезпеки таких систем може привести до наслідків в промисловому секторі. Можливі збитки від реалізації кіберзагроз крім фінансових втрат будуть включати ризики репутації і ризики, пов'язані з втратою здоров'я і життя людей, а також ризики виникнення екологічних катастроф. У цих умовах надзвичайно важливу роль відіграє підтримання безпеки, у тому числі і кібербезпеки, об'єктів критичної інфраструктури. Одним із ключових процесів при управлінні та забезпеченні кібербезпеки, у тому числі об'єктів критичної інфраструктури, є процес оцінки ризиків.

Власники об'єктів критичної інфраструктури прагнуть звести до мінімуму ризики кібербезпеки, а також мінімізувати витрати на заходи по мінімізації цих ризиків. Для досягнення цієї мети необхідно розробити адекватні методи оцінки ризиків кібербезпеки. Результати оцінки ризику дають підстави для прийняття рішення щодо прийнятності його рівня і необхідності чи економічної доцільності його подальшої обробки.

Аналіз літературних даних

Дослідженню проблем, пов'язаних із оцінкою ризику кіберзагроз присвячені публікації вітчизняних і зарубіжних вчених [1–6].

Так у [7] розглядаються і детально аналізуються двадцять чотири методи оцінки ризику для систем SCADA. Описується суть методів, розглядаються етапи управління ризиками, запропонована схема класифікації методів оцінки ризиків кібербезпеки для SCADA систем.

У роботі [8] досліджено широкий спектр загроз, які призводять до ризику кібербезпеки, створено базу даних фактичних втрат у випадку реалізації цих загроз, здійснено аналіз втрат з використанням методів статистики та актуарної математики.

Структура, яка включає в себе принципи роботи страхової галузі для надання кількісних оцінок ризиків кібербезпеки представлена в [9]. Запропонована структура використовує методи оптимізації, щоб запропонувати рівні інвестицій в заходи з кібербезпеки і страхування для власників об'єктів критичної інфраструктури і може бути використана для розробки стратегій по мінімізації ризиків кібербезпеки.

Удосконалення моделі оцінки ризиків кібербезпеки з використанням апарату нечіткої логіки запропоновано в [10]. Модель враховує чотири фактори ризику: уразливість, загроза, ймовірність та вплив.

Нові метрики ризику, шляхом адаптації існуючих методів для розрахунку ризиків і невизначеностей представлені в [11]. Також у роботі пропонується таксономічна класифікація вимог до оцінки кібернетичних ризиків. Розглянуті метрики ризику дозволяють вимірювати ризик «*Internet*

of Things», а модель ризику дозволяє встановити прийнятний рівень ризику «*Internet of Things»*.

В роботі [12] пропонується модель оцінки ризику кібербезпеки для пристроїв і систем управління ядерними установками з використанням Байєсовської мережі і дерева подій. Зазначається, що забезпечення кібербезпеки являється важливою проблемою в області ядерної техніки, так як ядерні установки використовують цифрове обладнання і цифрові системи, що можуть призвести до серйозних небезпек у випадку аварії. Показано, що органи, які здійснюють регулювання по усьому світу оголосили про керівні документи кібербезпеки, пов'язані з ядерними установками, включаючи «NRC Regulatory Guide 5.71» (США) і важливо оцінити ризик кібербезпеки у відповідності з цими нормативними документами. В роботі пропонується ймовірнісний метод оцінки ризику кібербезпеки.

Проте, незважаючи на велику кількість досліджень, спрямованих на розробку методів оцінки ризику кібербезпеки, невирішеним залишаються задачі, пов'язані із можливістю визначення сумарного ризику кібербезпеки, максимальних збитків в результаті дії сумарного ризику, ймовірність виникнення максимальних збитків в результаті дії сумарного ризику.

Постановка завдань дослідження

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 сумарного ризику.

Таким чином, оцінка ризику являється важливою, актуальною науково-практичною задачею і основою для прийняття рішень по обробці ризику.

Метою дослідження є розробка методів оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури.

Графічний метод оцінки сумарного ризику

Існує досить багато понять «ризик». Одне з них визначає ризик R, як ймовірність або можливість p настання випадкової події, що призводить до певних наслідків h, і може визначатися за формулою:

$$R = p \cdot h. \tag{1}$$

Наслідки можуть бути як додатними так і від'ємними. Під додатними наслідками будемо розуміти збитки, під від'ємними — прибуток.

На підставі виразу (1) залежність наслідків h в результаті настання деякої події від ймовірності p її настання можна представити у вигляді:

$$h(p) = \frac{R}{p}, \tag{2}$$

де $p \neq 0$.

Графік функції (2) для кожного значення $R = \text{const}$ буде представляти собою криву, рисунок 1. На рисунку 1, *а* представлено додатній ризик R, тобто ймовірність p настання випадкової події, що призводить до певних втрат.

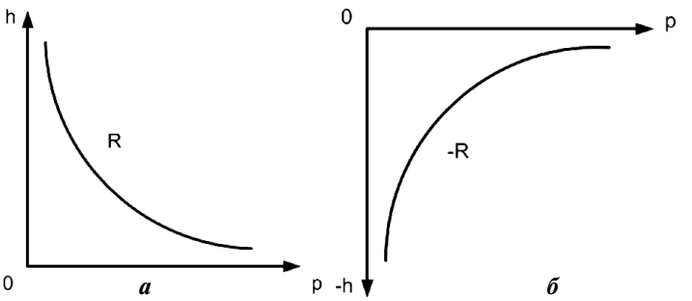

Рисунок 1 — Графічне представлення ризику

На рисунку 1(б) представлено від'ємний ризик − R, тобто ймовірність p настання випадкової події, що призводить до прибутку.

Нехай існує множина із n ризиків:

$$\begin{aligned} R_1 &= p_1 \cdot h_1, \\ &\dots \\ R_i &= p_i \cdot h_i, \\ &\dots \\ R_n &= p_n \cdot h_n, \end{aligned} \tag{3}$$

де кожний ризик R_i представлений графіком функції (*2*) і визначається ймовірністю або можливістю P_i настання випадкової події, що може призвести до певних наслідків h_i (точки 1, 2, 3), рисунок 2. Припустимо, що наслідками у даному випадку будуть збитки.

Визначимо максимальні значення наслідків $h_{1m},\dots,h_{im},\dots,h_{nm}$ для кожного ризику відповідно.

Максимальні значення наслідків можуть бути визначені, наприклад експертним шляхом, як максимальні збитки, що можуть бути завдані активам компанії (матеріальні, нематеріальні, людські).

Ймовірності виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику визначається з графіку, як координати точок перетину (точки 4, 5, 6) графіків ризиків з лініями рівнів відповідних максимальних наслідків, тобто $p_{1m},\dots,p_{im},\dots,p_{nm}$, рисунок 2.

У випадку дії *n ризиків із множини (3) значення сумарного наслідку не буде перевищувати суми максимальних наслідків для кожного із n* ризиків. Це означає, що максимальне

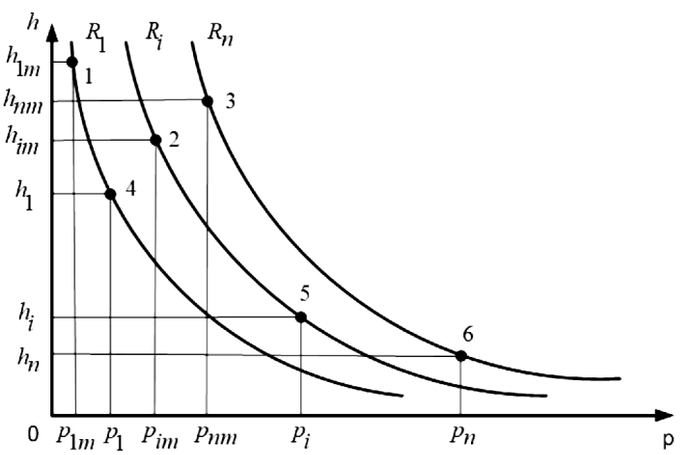

Рисунок 2 — Визначення сумарного ризику

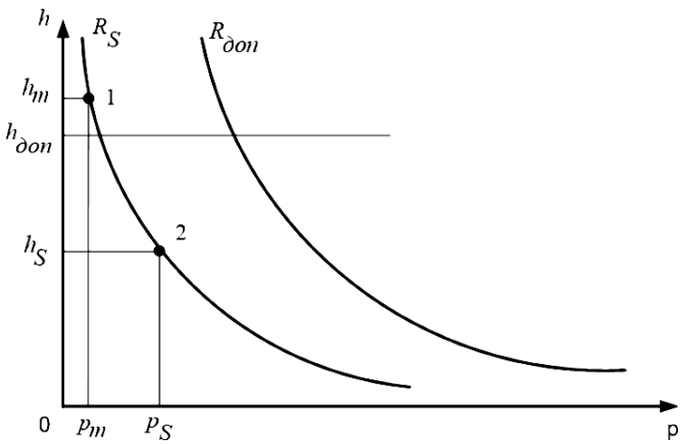

Рисунок 3 — Графік сумарного ризику

значення сумарного наслідку буде дорівнювати сумі максимальних наслідків для кожного із n ризиків:

$$h_m = h_{1m} + \ldots + h_{nm} = \sum_{i=1}^{n} h_{im}. \quad (4)$$

Дія одного або декількох ризиків не виключає дії інших ризиків у той же період часу. З огляду на це, можемо констатувати, що події, які призводять до ризиків являються сумісними подіями. На підставі цього, ймовірність виникнення події, що призводить до дії n ризиків з максимальними наслідками для кожного ризику, визначається, як сума ймовірностей цих подій без ймовірності їх добутку:

$$p_m = \sum_{i=1}^{n} p_{im} - \sum_{i,j} p_{im}p_{jm} + \sum_{i,j,k} p_{im}p_{jm}p_{km} + \ldots + (-1)^{n-1} \cdot \prod_{i=1}^{n} p_{im}. \quad (6)$$

Сумарний ризик дії n ризиків на підставі виразів (4) і (6) буде визначатися виразом:

$$R_S = h_m \cdot p_m. \quad (7)$$

Використовуючи вираз (7), задаючи значення p від 0 до 1, будуємо графік функції, рисунку 3:

$$h(p) = \frac{R_S}{p}. \quad (8)$$

Ймовірність p_S сумарної дії n ризиків визначається на підставі виразу (6), заміною p_{im} на p_i. Отримаємо вираз:

$$p_S = \sum_{i=1}^{n} p_i - \sum_{i,j} p_i p_j + \sum_{i,j,k} p_i p_j p_k + \ldots + (-1)^{n-1} \cdot \prod_{i=1}^{n} p_i. \quad (9)$$

Величину наслідків h_S у випадку дії сумарного результуючого ризику знаходимо, як ординату точки 2, рисунок 3.

Отримані результати дозволяють здійснювати оцінювання ризику. Метою оцінювання ризику є сприяння прийняттю рішень. Оцінювання ризику включає порівняння результатів аналізу ризику до встановлених критеріїв ризику для визначення необхідності додаткових дій, варіантів обробки ризику.

Якщо у якості критерію для визначення варіантів обробки ризику вибрано рівень ризику $R_{доп}$, то порівнюються ризики R_S і $R_{доп}$. У випадку застосування у якості критерію величини наслідків $h_{доп}$ — використовуються значення наслідків h_S і $h_{доп}$.

Перевагою даного методу визначення сумарного ризику є наочність і простота розрахунків.

Аналітичний метод оцінки сумарного ризику

Як зазначалося вище, ризик R визначається як ймовірність або можливість p настання випадкової події, що призводить до певних наслідків h, і може описуватися виразом (1).

Нехай існує множина із n ризиків:

$$R = \{R_1 = p_1 \cdot h_1, \ldots, R_i = p_i \cdot h_i, \ldots, R_n = p_n \cdot h_n\}, \quad (10)$$

де кожний ризик R_i визначається ймовірністю або можливістю p_i настання випадкової події, що може призвести до певних наслідків h_i.

Визначимо максимальні значення наслідків для кожного ризику. Отримуємо множину максимальних наслідків:

$$h_m = \{h_{1m}, \ldots, h_{nm}\}. \quad (11)$$

Як було показано вище, події, які призводять до ризиків являються сумісними подіями.

Максимальне значення сумарного наслідку у випадку дії *n ризиків буде визначатися з виразу (4).*

Ймовірність p_{im} виникнення кожної i—тої події, що призводить до відповідних максимальних наслідків h_{im} в умовах дії ризиків R_i, *визначається з виразу:*

$$p_{im} = \frac{R_i}{h_{im}}. \quad (12)$$

Ймовірність виникнення події, що призводить до дії ризиків з максимальними наслідками для кожного ризику, визначається з виразу (6). При цьому враховуємо, що події сумісні.

Сумарний ризик R_S дії n ризиків, на підставі виразів (4) і (6), буде визначатися виразом (7). Ймовірність p_S сумарної дії n ризиків визначається з виразу (9).

Таким чином, величина наслідків h_S у випадку дії сумарного результуючого ризику буде визначатися з виразу:

$$h_S = \frac{R_S}{p_S}. \quad (13)$$

Якщо у якості критерію для визначення варіантів обробки ризику вибрано рівень ризику, то використовується значення, отримане з виразу (7). У випадку застосування у якості критерію величини наслідків — використовується значення, отримане з виразу (13).

Розрахунок сумарного ризику двох ризиків

Розглянемо обчислення суми ризиків запропонованим методом для випадку двох ризиків, $n = 2$.

Нехай існує два ризики, які визначаються наступним чином:

$$R_1 = p_1 \cdot h_1;\ R_2 = p_2 \cdot h_2. \quad (14)$$

Визначимо максимальні значення наслідків h_{1m} і h_{2m} для кожного із ризиків R_1 і R_2 відповідно.

Максимальне значення сумарного наслідку буде дорівнювати сумі максимальних наслідків для кожного із ризиків:

$$h_m = h_{1m} + h_{2m}. \quad (15)$$

Ймовірності виникнення подій, що призводять до максимальних наслідків в умовах дій ризиків R_1 і R_2, визначаються відповідно:

$$p_{1m} = \frac{R_1}{h_{1m}};\ \ p_{2m} = \frac{R_2}{h_{2m}}. \quad (16)$$

Ймовірність виникнення події, що призводить до дії ризиків R_1 і R_2 з максимальними наслідками h_{1m} і h_{2m} *в умовах дії кожного ризику відповідно, визначається, як сума ймовірностей цих подій без ймовірності їх добутку:*

$$p_m = p_{1m} + p_{2m} - p_{1m} \cdot p_{2m}. \quad (17)$$

Сумарний ризик дії ризиків R_1 і R_2, на підставі виразів (15) і (16) буде визначатися виразом:

$$R = h_m \cdot p_m. \quad (18)$$

З урахуванням виразу (16) вираз (17) можна представити у вигляді:

$$p_m = \frac{R_1}{h_{1m}} + \frac{R_2}{h_{2m}} - \frac{R_1 \cdot R_2}{h_{1m} \cdot h_{2m}} = \frac{R_1 \cdot h_{2m} + R_2 \cdot h_{1m} - R_1 \cdot R_2}{h_{1m} \cdot h_{2m}}. \quad (19)$$

Підставивши вирази (15) і (19) у вираз (18), отримаємо вираз для визначення сумарного ризику:

$$R = (h_{1m} + h_{2m}) \cdot \left(\frac{R_1 \cdot h_{2m} + R_2 \cdot h_{1m} - R_1 \cdot R_2}{h_{1m} \cdot h_{2m}} \right), \quad (20)$$

або після перетворень:

$$R = R_1 + R_2 + R_1 \cdot \frac{h_{2m}}{h_{1m}} + R_2 \cdot \frac{h_{1m}}{h_{2m}} - R_1 \cdot R_2 \cdot \left(\frac{1}{h_{1m}} + \frac{1}{h_{2m}} \right). \quad (21)$$

На підставі (21), з урахуванням (14) і (17) отримаємо вираз для визначення наслідків, у випадку дії сумарного результуючого ризику R:

$$h = \frac{R_1 + R_2 + R_1 \cdot \frac{h_{2m}}{h_{1m}} + R_2 \cdot \frac{h_{1m}}{h_{2m}} - R_1 \cdot R_2 \cdot \left(\frac{1}{h_{1m}} + \frac{1}{h_{2m}} \right)}{p_1 + p_2 - p_1 \cdot p_2}. \quad (22)$$

Нехай максимальні наслідки h_{1m} і h_{2m} ризиків R_1 і R_2 будуть однаковими, тобто $h_{1m} = h_{2m} = h_m$. *Тоді вираз (21) можна представити у вигляді:*

$$R = 2 \cdot \left(R_1 + R_2 - \frac{R_1 \cdot R_2}{h_m} \right). \quad (23)$$

У випадку рівності ризиків, тобто $R_1 = R_2 = R_0$, вираз (21) можна представити у вигляді:

$$R = R_0 \cdot \left(2 + \frac{h_{2m}}{h_{1m}} + \frac{h_{1m}}{h_{2m}} - R_0 \cdot \left(\frac{1}{h_{1m}} + \frac{1}{h_{2m}} \right) \right), \quad (24)$$

де $h_{1m} \neq 0$ і $h_{2m} \neq 0$.

У випадку рівності максимальних збитків, тобто $h_{1m} = h_{2m} = h_m$, і рівності ризиків, тобто $R_1 = R_2 = R_0$, вираз (21) можна представити у вигляді:

$$R = 2 \cdot R_0 \cdot \left(2 - \frac{R_0}{h_m} \right), \quad (25)$$

де $h_m \neq 0$.

Висновки

Запропоновані методи дають можливість визначати сумарний ризик кібербезпеки об'єктів критичної інфраструктури, сумарні збитки в результаті дії множини кіберзагроз, сумарну величину збитків в результаті дії однієї кіберзагрози за певний період часу, ймовірність виникнення максимальних втрат в результаті дії множини кіберзагроз. На основі запропонованих методів можливо будувати системи підтримки прийняття рішень щодо застосування заходів по зменшенню ризику.

Список використаної літератури

1. Terje Aven. Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*. 2016. V. 253. № 1. P. 1–13.

2. 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. V. 53. P. 61–73.

3. Mokhor V., Bakalynskyi O., Bohdanov O., Tsurkan V. Interpretation of the simple risk level dependence of its implementation in the terms of analytic geometry. *Information technology and security*. 2017. V. 5. № 1. P. 71–82.

4. Bochkovskyi A., Gogunskii V. Development of the method for the optimal management of occupational risks. Eastern-European *Journal of Enterprise Technologies*. 2018. V. 1, № 3 (97). P. 6–13.

5. Prokopenko T., Grigor O. Development of the comprehensive method to manage risks in projects related to information technologies. *Eastern-European Journal of Enterprise Technologies*. 2018. № 2(3) (92). P. 37–43.

6. Мохор В. В., Гончар С. Ф. Идея построения алгебры рисков на основе теории комплексных чисел. *Электронное моделирование*. 2018. 40. № 4, С. 107–111.

7. Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*. V. 56. 2016. P. 1–27.

8. Martin Eling, Jan Wirfs. What are the actual costs of cyber risk events? *European Journal of Operational Research*. 2019. V. 272, № 3. P. 1109–1119.

9. 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*. V. 14. 2016. P. 43–57.

10. 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*. V. 74. 2018. P. 323–339.

11. 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*. V. 102. 2018. P. 14–22.

12. Jinsoo Shin, Hanseong Son, Gyunyoung Heo. Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET. *Nuclear Engineering and Technology*. V. 49. № 3. 2017. P. 517–524.

References

1. Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13.

2. Jain, P., Pasman, H. J., Waldram, S., Pistikopoulos, E. N., Mannan, M. S. (2018). Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. *Journal of Loss Prevention in the Process Industries*, No. 53, 61–73.

3. Mokhor, V., Bakalynskyi, O., Bohdanov, O., Tsurkan, V. (2017). Interpretation of the simple risk level dependence of its implementation in the terms of analytic geometry. *Information Technology and Security*, 5(1), 71–82.

4. Bochkovskyi, A., Gogunskii, V. (2018). Development of the method for the optimal management of occupational risks. *Eastern-European Journal of Enterprise Technologies*, 3(97), 6–13.

5. Prokopenko, T., Grigor, O. (2018). Development of the comprehensive method to manage risks in projects related to information technologies. *Eastern-European Journal of Enterprise Technologies*, 2(3), 37–43.

6. Mokhor, V., Honchar S. (2018). The idea of the construction of the algebra of risks on the basis of the theory of complex numbers. *Electronic modeling*, 40(4), 107–111.

7. Cherdantseva, Yu., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, No. 56, 1–27.

8. Eling, M., Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, 272(3), 1109–1119.

9. Young, D., Lopez Jr., J., Rice, M., Ramsey, B., McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, No. 14, 43–57.

10. Alali, M., Almogren, A., Mehedi Hassan, M., Rassan, I., Alam Bhuiyan, Z. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*, No. 74, 323–339.

11. Radanlieva, P., De Rourea, Ch., Nicolescub, R., Huthb, M., Mantilla Montalvoc, R., Cannadyc, S., Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, No. 102, 14–22.

12. Shin. J., Son, H., Heo, G. (2017). Cyber security risk evaluation of a nuclear I&C using BN and ET. *Nuclear Engineering and Technology*, 49(3), 517–524.

Methods for the Total Risk Assessment of Cybersecurity of Critical Infrastructure Facilities

Mokhor V[1]., Gonchar S[1]., Dybach O[2].

[1] *Pukhov Institute for Modeling in Energy Engineering, NAS of Ukraine, Kyiv, Ukraine*

[2] *State Enterprise "State Scientific and Technical Center for Nuclear and Radiation Safety" Kyiv, Ukraine*

The paper presents the analysis of national and foreign literature on the methods of cybersecurity risk assessment including critical infrastructure facilities. It is stated that cybersecurity and risk assessment are an important issue of critical infrastructure facilities. The paper proposes graphical and analytical methods for assessing the total cybersecurity risk of I&C systems including critical infrastructure facilities. These total risk assessment methods are based on determining the maximum values of consequences for each risk. It is shown that the maximum values of cyber threat effects can be determined by expert means, as the maximum losses that can be caused to the company assets. The proposed methods make it possible to determine the total cybersecurity risk of critical infrastructure, the total losses due to multiple cyber threats, the total losses due to a single cyber threat for a certain period of time, the likelihood of maximum losses due to multiple cyber threats. There are the advantages of these methods for assessing total risk. Based on the proposed methods, it is possible to develop a methodology for assessing the cybersecurity risks of I&C systems including critical infrastructure facilities, and build decision support systems for the application of risk reduction measures. The economic feasibility of applying these or other risk treatment measures, both organizational and technical, is defined by evaluating the cost of such measures with the maximum amount of losses due to the total risk.

Keywords: total risk, cybersecurity, critical infrastructure facilities, cyber threat, risk assessment method

Методы оценки суммарного риска кибербезопасности объектов критической инфраструктуры

Мохор В. В[1].,Гончар С. Ф[1]., Дыбач А. М[2].

[1] *Институт проблем моделирования в энергетике им. Е. Пухова НАН Украины, г. Киев, Украина*

[2] *Государственное предприятие «Государственный научно-технический центр по ядерной и радиационной безопасности», г. Киев, Украина*

В работе приведены результаты анализа отечественной и зарубежной литературы по теме методов оценки рисков кибербезопасности, в том числе объектов критической инфраструктуры, отмечается, что обеспечение кибербезопасности и оценка рисков кибербезопасности является важной проблемой объектов критической инфраструктуры. В работе предложено графический и аналитический методы оценки суммарного риска кибербезопасности информационных систем, в том числе объектов критической инфраструктуры. Указанные методы оценки суммарного риска базируются на определении максимальных значений последствий для каждого риска. Показано, что максимальные значения последствий киберугроз могут быть определены экспертным путем, как максимальные убытки, которые могут быть нанесены активам компании. Предложенные методы дают возможность определять суммарный риск кибербезопасности объектов критической инфраструктуры, суммарные убытки в результате действия множества киберугроз, суммарную величину убытков в результате действия одной киберугрозы за определенный период времени, вероятность возникновения максимальных потерь в результате действия множества киберугроз. Приведены преимущества данных методов оценки суммарного риска. На основе предложенных методов возможно разработать методологию оценки рисков кибербезопасности информационных систем, в том числе объектов критической инфраструктуры, строить системы поддержки принятия решений по применению мер по уменьшению риска. Определение экономической целесообразности применения тех или иных мер по обработке риска, включая как организационные, так и технические, осуществляется оценочным сравнением стоимости таких мероприятий с максимальной величиной убытков в результате действия суммарного риска.

Ключевые слова: суммарный риск, кибербезопасность, объекты критической инфраструктуры, киберугроза, метод оценки риска.

Отримано 24.04.2019