УДК 004.056.53
DOI https://doi.org/10.32838/TNU-2663-5941/2020.3-1/15

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

МЕТОД ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ SMART GRID

У роботі запропоновано метод оцінювання ризиків кібербезпеки інформаційних систем Smart Grid. Показано актуальність цього методу оцінювання ризиків для забезпечення кібербезпеки сучасних електроенергетичних об'єктів з використанням інтелектуальних мереж Smart Grid, оснащених цифровими системами моніторингу, управління, релейного захисту й протиаварійної автоматики. Проведено аналіз, який дає змогу виділити три види інформаційних ресурсів Smart Grid, що підлягають захисту від кібератак. Показано, що для своєчасного виявлення актуальних загроз кібербезпеки, визначення ймовірності їх реалізації, оцінювання збитків у разі їх реалізації, вибору адекватних та економічно обґрунтованих контрзаходів необхідним є розроблення методів оцінювання ризиків кібербезпеки інформаційних систем Smart Grid, а для більш коректної оцінки ризику кібербезпеки складної інформаційної системи необхідно враховувати умови, у яких функціонує кожний складник інформаційної системи, вид інформації, що циркулює в ній, модель загроз, модель порушника. Використовуючи векторну модель, ризики кібербезпеки представлені у вигляді векторів, тому ризик кібербезпеки, спричинений кожною із загроз, можна представити вектором, розташованим у тривимірному лінійному просторі, початок цього вектору співпадає з початком координат, а координати кінця вектору визначаються значеннями ризиків утрати конфіденційності, цілісності й доступності, що спричиняються цією загрозою. Запропонований метод оцінювання ризику кібербезпеки інформаційної системи Smart Grid дає змогу оцінювати ризик складної інформаційної системи залежно від умов, у яких функціонує кожний складник інформаційної системи, виду інформації, що циркулює в ній, моделі загроз, моделі порушника. Використання запропонованого методу дає можливість розроблення апаратно-програмних комплексів для автоматизації розрахунку ризику інформаційних систем Smart Grid, а також створення систем підтримки прийняття рішень з метою забезпечення кібербезпеки інформаційних систем Smart Grid.

Ключові слова: *кібербезпека, ризик, Smart Grid, інформаційна система, метод, модель.*

Постановка проблеми. Останнім часом у сучасній енергетиці активного розвитку набув напрям Smart Grid. Концепція Smart Grid полягає в тому, щоб зробити «інтелектуальними» генерацію, передавання й розподіл електричної енергії через наповнення електричних мереж сучасними засобами діагностики, електронними системами управління та обліку, алгоритмами, обмежувачами струмів короткого замикання надпровідних ліній та іншими автоматично регульованими технічними процесами.

Упровадження технології інтелектуальних мереж, з одного боку, спрощує й прискорює управління, але, з іншого боку, відкриває доступ до можливих кібератак і неправомірного використанню даних.

Питання забезпечення кібербезпеки сучасних електроенергетичних об'єктів з використанням інтелектуальних мереж Smart Grid, оснащених цифровими системами моніторингу, управління, релейного захисту та протиаварійної автоматики, стають дуже актуальними через новизну й недостатнє дослідження проблеми.

Аналіз останніх досліджень і публікацій. Згідно з дослідженнями [1], можна виділити ключові вимоги, які має забезпечувати нова електроенергетика:

– доступність – забезпечення споживачів енергією згідно з необхідними їм параметрами часу, місця та якості;

– надійність – можливість протистояння енергосистеми фізичним та інформаційним негативним впливам без тотальних відключень або високих витрат на відновлювальні роботи, а також її максимально швидке відновлення (самовідновлення);

– економічність – оптимізація тарифів на поставку та зниження загальносистемних витрат на генерацію й розподілення електричної енергії;

– ефективність – максимізація ефективності використання всіх видів ресурсів і технологій під час виробництва, передачі, розподілу та споживання електроенергії;

– органічність із навколишнім середовищем – зниження негативного впливу на навколишнє середовище;

– безпека – недопущення ситуацій в електроенергетиці, потенційно небезпечних для людей і навколишнього середовища.

Усі приведені вимоги розглядаються як рівнозначні, порядок їх виконання може залежати від особливостей функціонування об'єкта або їх сукупностей.

Виконання цих вимог призводить до виникнення нових особливостей системи, таких як самовідновлення, мотивація активності споживача, супротив негативним впливам, забезпечення надійності електропостачання, різноманіття типів електричних станцій, розширення енергетичних ринків, оптимізація керування активами.

На думку Міністерства енергетики США, інтелектуальним мережам притаманні такі атрибути [2]:

– здатність до самовідновлення після збоїв у подачі електроенергії;

– можливість активної участі споживачів;

– стійкість до фізичного й кібернетичного втручання зловмисників;

– забезпечення необхідної якості переданої електроенергії;

– забезпечення синхронної роботи джерел генерації та вузлів зберігання електроенергії;

– підвищення ефективності роботи енергосистеми загалом.

Проведений аналіз дає змогу виділити три види інформаційних ресурсів Smart Grid, що підлягають захисту:

– персональні дані користувачів Smart Grid (Personal Data);

– технічна інформація, яка надходить від клієнтів мережі (Technical Data);

– інформація про системні збої й помилки, які відбуваються під час роботи мережі (Failures Data).

До вимог, які має реалізовувати система захисту, зараховані:

– запобігання неавторизованому розкриттю інформації, що захищається (конфіденційність);

– забезпечення постійного доступу користувачів до інформації, що захищається (доступність);

– запобігання несанкціонованій зміні інформації, що захищається (цілісність).

Питання оцінювання ризиків кібербезпеки інформаційних систем Smart Grid досліджувалося багатьма науковцями [3–5].

Постановка завдання. Отже, для своєчасного виявлення актуальних загроз кібербезпеки, визначення ймовірності їх реалізації, оцінювання збитків у разі їх реалізації, вибору адекватних та економічно обґрунтованих контрзаходів необхідним є розроблення методів оцінювання ризиків кібербезпеки інформаційних систем Smart Grid.

Для більш коректної оцінки ризику кібербезпеки складної інформаційної системи необхідно враховувати умови, у яких функціонує кожний складник інформаційної системи, вид інформації, що циркулює в ній, модель загроз, модель порушника. Залежно від виду інформації, яка підлягає захисту, та особливостей функціонування інформаційної системи ризики кібербезпеки можуть призводити до порушення конфіденційності, цілісності, доступності інформації або до їх певної комбінації. Для інформаційних систем Smart Grid можлива ситуація, коли критичним є забезпечення доступності й захист від несанкціонованих змін відкритої інформації. У такому разі виникає необхідність визначення ризиків кібербезпеки від утрати саме доступності та цілісності. Усі ці ризики можуть визначатися експертним методом і повинні враховуватися під час розрахунку результуючого ризику кібербезпеки Smart Grid.

Виклад основного матеріалу дослідження. Розглянемо випадок ідентифікації певної загрози. Необхідно визначити ймовірність її реалізації, збитки від її реалізації та спричинені цією загрозою ризики порушення конфіденційності, цілісності, доступності інформації (таблиця 1).

Значення $R_К$, $R_Ц$, $R_Д$, у таблиці 1 обчислюються з виразів:

$$R_К = p \cdot h_К \cdot g_К, \quad (1)$$

$$R_Ц = p \cdot h_Ц \cdot g_Ц, \quad (2)$$

$$R_Д = p \cdot h_Д \cdot g_Д, \quad (3)$$

де коефіцієнти $g_К$, $g_Ц$, $g_Д$, набувають значення 1, якщо загроза призводить до порушення, відпо-

Таблиця 1

Загроза	Імовірність реалізації	Порушення					
		конфіденційності		цілісності		доступності	
		збитки	ризик	збитки	ризик	збитки	ризик
Загроза 1	*p*	$h_К$	$R_К$	$h_Ц$	$R_Ц$	$h_Д$	$R_Д$

відно, конфіденційності, цілісності, доступності, і набувають значення 0 – у протилежному випадку.

Дослідження [6; 7] показують, що ризики кібербезпеки можна представити у вигляді векторів. Отже, ризик кібербезпеки, спричинений кожною із загроз, можна представити вектором, розташованим у тривимірному лінійному просторі. Початок цього вектору співпадає з початком координат, а координати кінця вектору визначаються значеннями ризиків утрати конфіденційності, цілісності й доступності, що спричиняються цією загрозою (рис. 1).

Тоді ризик кібербезпеки, спричинений певною загрозою, можна представити виразом:

$$\vec{R}\left(R_K; R_Ц; R_Д\right), \tag{4}$$

де R_K, $R_Ц$, $R_Д$, – спричинені цією загрозою ризики втрати, відповідно, конфіденційності, цілісності, доступності інформації.

Рис. 1. Векторна модель ризику кібербезпеки

У такому разі величина ризику кібербезпеки, спричиненого певною загрозою, буде визначатися виразом:

$$R = \sqrt{R_K^2 + R_Ц^2 + R_Д^2}\,. \tag{5}$$

Розглянемо випадок наявності N загроз. Необхідно визначити ймовірності їх реалізації, збитки від їх реалізації та спричинені цими загрозами ризики порушення конфіденційності, цілісності, доступності інформації (таблиця 2).

Значення R_{K1}, R_{Kn}, R_{KN},у таблиці 1 обчислюються з виразів:

$$\begin{aligned} &R_{K1} = p_1 \cdot h_{K1} \cdot g_{K1}, \\ &\dots \\ &R_{Kn} = p_n \cdot h_{Kn} \cdot g_{Kn}, \\ &\dots \\ &R_{KN} = p_N \cdot h_{KN} \cdot g_{KN}, \end{aligned} \tag{6}$$

де коефіцієнти g_{K1}, g_{Kn}, g_{KN},набувають значення 1, якщо відповідні загрози призводять до порушення конфіденційності інформації, і набувають значення 0 – у протилежному випадку.

Значення $R_{Ц1}$,... $R_{Цn}$,... R_{KN}, у таблиці 1 обчислюються з виразів:

$$\begin{aligned} &R_{Ц1} = p_1 \cdot h_{Ц1} \cdot g_{Ц1}, \\ &\dots \\ &R_{Цn} = p_n \cdot h_{Цn} \cdot g_{Цn}, \\ &\dots \\ &R_{ЦN} = p_N \cdot h_{ЦN} \cdot g_{ЦN} \end{aligned} \tag{7}$$

де коефіцієнти $g_{Ц1}$,... $g_{Цn}$,... g_{KN}, набувають значення 1, якщо відповідні загрози призводять до порушення цілісності інформації, і набувають значення 0 – у протилежному випадку.

Значення $R_{Д1}$,... $R_{Дn}$,... $R_{ДN}$, у таблиці 1 обчислюються з виразів:

$$\begin{aligned} &R_{Д1} = p_1 \cdot h_{Д1} \cdot g_{Д1}, \\ &\dots \\ &R_{Дn} = p_n \cdot h_{Дn} \cdot g_{Дn}, \\ &\dots \\ &R_{ДN} = p_N \cdot h_{ДN} \cdot g_{ДN}, \end{aligned} \tag{8}$$

де коефіцієнти $g_{Д1}$,... $g_{Дn}$,... $g_{ДN}$, набувають значення 1, якщо відповідні загрози призводять до порушення доступності інформації, і набувають значення 0 – у протилежному випадку.

Використовуючи векторну модель ризику (рис. 2), ризики кібербезпеки R_1,..., R_N спричинені N загрозами, можна представити, відповідно, векторами:

$$\vec{R}_1\left(R_{K1}; R_{Ц1}; R_{Д1}\right), \tag{9}$$

...

$$\vec{R}_N\left(R_{KN}; R_{ЦN}; R_{ДN}\right), \tag{10}$$

Таблиця 2

Загроза	Імовірність реалізації	Порушення					
		конфіденційності		цілісності		доступності	
		збитки	ризик	збитки	ризик	збитки	ризик
Загроза 1	p_1	h_{K1}	R_{K1}	$h_{Ц1}$	$R_{Ц1}$	$h_{Д1}$	$R_{Д1}$
…	…	…	…	…	…	…	…
Загроза n	p_n	h_{Kn}	R_{Kn}	$h_{Цn}$	$R_{Цn}$	$h_{Дn}$	$R_{Дn}$
…	…	…	…	…	…	…	…
Загроза N	p_N	h_{KN}	R_{KN}	$h_{ЦN}$	$R_{ЦN}$	$h_{ДN}$	$R_{ДN}$

де $R_{K1},..., R_{KN}$ – ризики втрати конфіденційності інформації, спричинені, відповідно, загрозами 1, ..., N;

$R_{Ц1},..., R_{ЦN}$ – ризики втрати цілісності інформації, спричинені, відповідно, загрозами 1, ..., N;

$R_{Д1},..., R_{ДN}$ – ризики втрати доступності інформації, спричинені, відповідно, загрозами 1, ..., N.

У такому разі величина ризику кібербезпеки, спричиненого певною загрозою, буде визначатися виразом:

$$R_1 = \sqrt{R_{K1}^2 + R_{Ц1}^2 + R_{Д1}^2}, \quad (11)$$

...

$$R_N = \sqrt{R_{KN}^2 + R_{ЦN}^2 + R_{ДN}^2}. \quad (12)$$

Для визначення ризику кібербезпеки інформаційної системи загалом представимо вектори (9), (10) у вигляді:

$$\vec{R}_1 = \begin{pmatrix} R_{K1} \\ R_{Ц1} \\ R_{Д1} \end{pmatrix}, ..., \vec{R}_N = \begin{pmatrix} R_{KN} \\ R_{ЦN} \\ R_{ДN} \end{pmatrix}. \quad (13)$$

Рис. 2. Застосування векторної моделі для N ризиків

Тоді з урахуванням правила додавання векторів вектор ризику кібербезпеки інформаційної системи загалом буде визначатися виразом:

$$\vec{R} = \vec{R}_1 + ... + \vec{R}_N = \begin{pmatrix} R_{K1} \\ R_{Ц1} \\ R_{Д1} \end{pmatrix} + ... + \begin{pmatrix} R_{KN} \\ R_{ЦN} \\ R_{ДN} \end{pmatrix} = \begin{pmatrix} \sum_{n=1}^{N} R_{Kn} \\ \sum_{n=1}^{N} R_{Цn} \\ \sum_{n=1}^{N} R_{Дn} \end{pmatrix}, \quad (14)$$

де $\sum_{n=1}^{N} R_{Kn}$, $\sum_{n=1}^{N} R_{Цn}$, $\sum_{n=1}^{N} R_{Дn}$ – ризики кібербезпеки складної інформаційної системи загалом від порушення конфіденційності, цілісності, доступності інформації відповідно.

Величина ризику кібербезпеки інформаційної системи загалом, спричиненого N загрозами, з урахуванням збитків від порушення конфіденційності, цілісності, доступності буде визначатися з виразу:

$$R = \sqrt{\left(\sum_{n=1}^{N} R_{Kn}\right)^2 + \left(\sum_{n=1}^{N} R_{Цn}\right)^2 + \left(\sum_{n=1}^{N} R_{Дn}\right)^2}. \quad (15)$$

З урахуванням викладеного структурно-аналітичне відображення методу оцінювання ризику кібербезпеки інформаційної системи Smart Grid представлено в загальному вигляді на рис. 3.

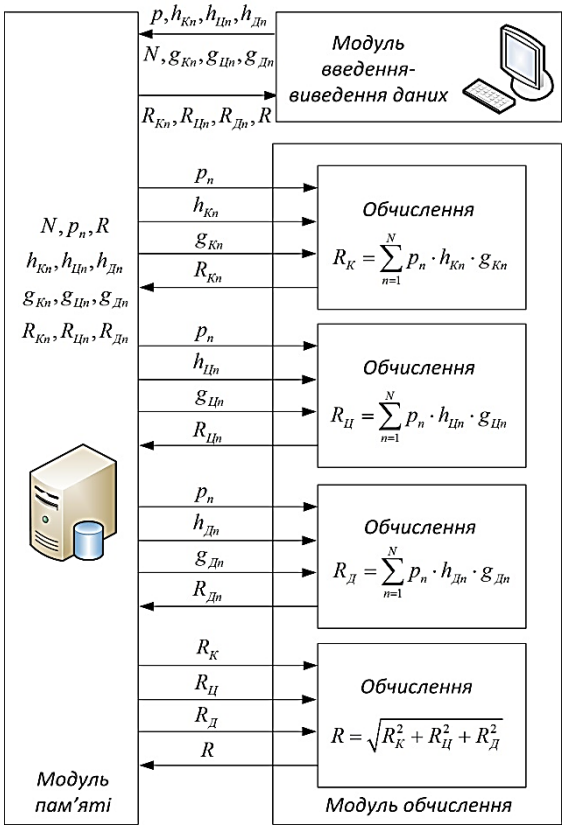

Рис. 3. Структурно-аналітичне відображення методу оцінювання ризику кібербезпеки Smart Grid

Висновки. Отже, у роботі запропоновано метод оцінювання ризику кібербезпеки інформаційної системи Smart Grid, який дає змогу оцінювати ризик складної інформаційної системи залежно від умов, у яких функціонує кожний складник інформаційної системи, виду інформації, що циркулює в ній, моделі загроз, моделі порушника. Використання запропонованого методу дає можливість розроблення апаратно-програмних комплексів для автоматизації розрахунку ризику інформаційних систем Smart Grid, а також створення систем підтримки прийняття рішень з метою забезпечення кібербезпеки інформаційних систем Smart Grid.

Список літератури:

1. European Smart Grids Technology Platform. URL: http://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf.
2. Estimating the Costs and Benefits of the Smart Grid. URL: http://www.rmi.org/Content/Files/EstimatingCostsSmartGRid.pdf.
3. Leszczyna R. Standards on cyber security assessment of smart grid. *International Journal of Critical Infrastructure Protection.* 2018. № 22. P. 70–89.
4. Maziku H., Shetty S., Nicol D.M. Security risk assessment for SDN-enabled smart grids. *Computer Communications.* 2019. № 133. P. 1–11.
5. From old to new: Assessing cybersecurity risks for an evolving smart grid / L. Langer, F. Skopik, P. Smith, M. Kammerstetter. *Computers & Security.* 2016. № 62. P. 165–176.
6. Мохор В.В., Гончар С.Ф. Идея построения алгебры рисков на основе теории комплексных чисел. *Електронне моделювання.* 2018. Т. 40. № 4. С. 107–111.
7. Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія. Київ : Альфа реклама, 2019. 176 с.

Honchar S.F. METHOD FOR RISK ASSESSMENT OF CYBERSECURITY OF INFORMATION SYSTEMS OF SMART GRID

The paper proposes a method for risk assessment of cybersecurity of Smart Grid information systems. The relevance of this method of risk assessment to ensure cyber security of modern electricity facilities using smart grids of Grid, equipped with digital monitoring, control, relay protection and emergency automation systems is shown. An analysis has been made to identify three types of Smart Grid information resources to be protected against cyberattacks. It is shown that for timely identification of actual cybersecurity threats, determination of their probability of realization, estimation of losses in case of their implementation, selection of adequate and economically justified countermeasures it is necessary to develop methods for assessing cybersecurity risks of Smart Grid information systems, and for more correct assessment of cybersecurity risk information system , it is necessary to take into account the conditions in which each component of the information system operates, the type of information circulating in it, the model of threats, the model of the offender. Using the vector model, cybersecurity risks are represented as vectors, so the cybersecurity risk caused by each of the threats can be represented by a vector located in three-dimensional linear space, the beginning of this vector coincides with the origin of coordinates, and the coordinates of the end of the vector are determined by the values of risk, caused by this threat. The proposed method for assessing the cybersecurity risk of the Smart Grid information system allows to assess the risk of a complex information system, depending on the conditions in which each component of the information system, the type of information circulating in it, the model of threats, the model of the offender. The use of the proposed method enables the development of hardware and software systems to automate the risk calculation of Smart Grid information systems, as well as the creation of decision support systems to ensure the cybersecurity of Smart Grid information systems.

Key words: *cybersecurity, risk, Smart Grid, information system, method, model.*