УДК 04.056

МЕТОДИКА ОЦІНЮВАННЯ КІБЕРРЕЗИЛЬЄНТНОСТІ ЕНЕРГОПІДПРИЄМСТВА

С. Д. Левашова[1,a], Л. Ю. Гальчинський[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

Робота присвячена дослідженню питання кіберрезильєнтності енергетичних підприємств. У ній описано поняття кіберрезильєнтності, висвітлено особливості енергосистем, їхні вразливості, а також розглянуто методику оцінювання кіберрезильєнтності у промислових системах керування. Результати проведеного дослідження можливо застосувати для розробки веб застосунку, що містить опитування для оцінювання кіберрезильєнтності енергосистем і надання рекомендацій щодо її підвищення.

Ключові слова: кіберрезильєнтність, SCADA, енергопідприємство, метрики кіберстійкості, шкала Лайкерта, метод аналізу ієрархій

Вступ

З розвитком інформаційно-комунікаційних технологій (ІКТ) з'являється все більше можливостей у всіх сферах життя: від підвищення ефективності побутових приладів до створення складних механізмів та технологій, які мають глобальні масштаби. Водночас швидка діджиталізація породжує також глобальні загрози, зокрема в секторі об'єктів критичної інфраструктури, створюючи чимало вразливостей, якими можуть скористуватися зловмисники для проведення кібератак. За останні 10 років зафіксовано серію кіберінцидентів проти критичної інфраструктури різних країн – США, Німеччини, Азербайджана, Данії, Індії та ін. Особливої шкоди зазнала Україна, починаючи зі сумнозвісної атаки на енергосистеми у 2015 році й по наш час. Проблема стійкості енергосистем набула особливої актуальності з початком повномасштабної війни в лютому 2022 року, коли країна-агресор поряд із обстрілами енергопідприємств паралельно проводить кібератаки, що нерідко призводять до критичного зниження рівня енергозабезпечення населення. Тому наразі питання кібервідмовостійкості енергосистем як суттєвого елементу виживання критичної інфраструктури є гостроактуальним.

1. Постановка задачі

Мета роботи полягає в розробці методики оцінювання кіберстійкості (кіберрезильєнтності) електроенергетичного підприємства з врахуванням особливостей архітектури SCADA інфраструктури енергосистем та врахуванні знань експертної спільноти. На основі такого системного оцінювання кіберрезильєнтності можна було б давати рекомендації щодо її підвищення.

2. Поняття кібервідмовостійкості

Кіберрезильєнтність (англ. cyber resilience) у своїй основі поєднує два поняття: кіберстійкість та відмовостійкість. Кіберстійкість можна розуміти як здатність системи протистояти та відновлюватися після кіберінцидентів, а відмовостійкість – здатність системи зберігати функціональність при відмовах. Таким чином, кібервідмовостійкість – це здатність організації запобігати інцидентам кібербезпеки, протистояти їм і відновлюватися після них. Організація повинна забезпечувати виконання своїх цілей навіть за умов серйозних кіберзагроз, природних катастроф чи економічних криз [1]. Яка різниця між кібербезпекою та кібервідмовостійкістю? Кібербезпека зосереджена на проактивних діях з метою надання допомоги та підтримки компанії в її боротьбі зі зростаючим поширенням кібератак. Натомість кібервідмовостійкість фокусується на потенціалі, який може мати компанія, щоб максимально обмежити втрати та збитки, відновивши роботу у звичному режимі після кібератаки. Разом з тим ці поняття тісно пов'язані між собою, а джерела концепцій кібервідмовостійкості витікають з понять кібербезпеки [2].

3. Особливості енергосистем

Промислові системи керування (Industrial Control System – ICS) поділяються на системи диспетчерського керування та збору даних (SCADA) та розподілені системи керування (DCS). Енергосистеми можна віднести до тих, що працюють на основі концепції Supervisory Control and Data Acquisition (SCADA), доповнену програмним рішенням мережі для моніторингу та контролю Wide Area Monitoring Systems (WAMS) [3].

[a] anna161levashova@gmail.com

Взаємодія пристроїв у промислових системах керування відбувається на таких рівнях (Рис. 1) [4]:

- Рівень 0 – польові пристрої. Містить датчики та виконавчі механізми (тискові сенсори, двигуни тощо);
- Рівень 1 – контролери введення/виведення (I/O) та програмовані логічні контролери (PLC/RTU). Вони обробляють сигнали від датчиків Рівня 0 та передають команди на виконавчі механізми;
- Рівень 2 – наглядові комп'ютери (Supervisory Computers) та SCADA-сервери. Відповідають за збір, зберігання, обробку даних із контролерів Рівня 1 та відображення оператору через людино-машинний інтерфейс (HMI);
- Рівень 3 – рівень керування виробництвом. Використовується для збору статистики, аналізу продуктивності та прогнозування можливих відмов;
- Рівень 4 – рівень планування виробництва. Відповідає за управління бізнес-процесами та стратегічне планування.

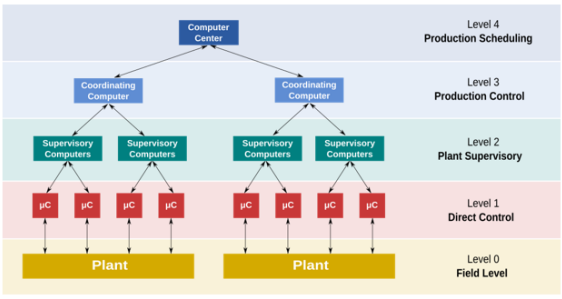

Рис. 1. Структура рівнів промислового керування

Основними елементами SCADA є [5]:
Control Centre – центр управління, що містить: людино-машинний інтерфейс (HMI) для оператора; інженерну станцію (EWS) для глибшого аналізу та налаштувань; головний термінальний блок (MTU), що приймає та відправляє дані з/до віддалених пристроїв та віддалений термінальний блок (RTU), який збирає дані з датчиків, вимірювальних приладів та передає їх у MTU (або навпаки, отримує команди від центру керування для керування обладнанням).

Компоненти WAMS [3]: глобальна навігаційна супутникова система (GNSS) для забезпечення синхронізації часу; концентратор фазорних даних (PDC), що збирає інформацію від PMU – фазорних вимірювальних пристроїв, що фіксують електричні параметри (напругу, струм, частоту, фазу) з часовою синхронізацією GNSS.

Та на верхньому рівні диспетчерського управління виділяють: центральний диспетчерський офіс (CDO), офіс диспетчеризації міжрегіонального рівня (IDO) та регіональний диспетчерський офіс (RDO).

З огляду на компоненти та їх взаємодію, можна виділити потенційні кіберзагрози:

1. Атаки з підробкою даних – навмисне внесення помилкових даних в віддалений термінальний блок (RTU), фазорні вимірювальні пристрої (PMU) та каналів зв'язку;
2. Атаки на синхронізацію часу – втручання у роботу глобальної навігаційної супутникової системи для забезпечення синхронізації часу (GNSS);
3. Атаки відмови в обслуговуванні – перевантаження серверів моніторингу;
4. Динамічні атаки на систему – перехоплення та повторне передавання старих даних;
5. Комплексні атаки – поєднання кількох вищезгаданих атак.

4. Метрики стійкості

Оцінка кіберрезильєнтності, як і для будь-яких складних систем, потребує системного підходу. Так, наприклад, при дослідженні сейсмічної стійкості було виокремлено чотири компоненти системи, яку слід вважати стійкою: міцність (robustness), надлишковість (redundancy), винахідливість (resourcefulness) і швидкість реагування (rapidity) – відому як методологію «чотирьох R». Як методологічну основу даний підхід можна застосувати і до кіберрезильєнтності енергосистем. На основі показників R4 було створено загальну структуру кібервідмовостійкості та розроблено методологію обчислення відповідних метрик стійкості, адаптованих до ІКС, у тому числі об'єктів критичної інфраструктури. Кожен із чотирьох показників поділяється на фізичні, організаційні та технічні метрики, які, у свою чергу, деталізуються на більш вузько направленими підметриками. Отже, загалом існує чотири стратегічні показники стійкості, метрики дванадцяти вимірів та відповідна кількість оперативних підметрик для оцінки кіберрезильєнтності ІКС. [6, 7]

5. Методика оцінювання

5.1. Анкета для опитування

Дані для оцінки ІКС збираються за якісним підходом шляхом опитування n експертів. Існує чотири шкали вимірювання (оцінювання) в залежності від типів змінних (безперервні та дискретні). Серед них: номінальна (категоріальна), порядкова (ординальна), інтервальна та шкала співвідношення. Для оцінювання розробляється анкета, яка використовує шкалу Лайкерта, змінні якої дискретні, а шкала вимірювання – інтервальна. В опитуванні використовуватимуться дві змінні: Оцінка від користувача (від 1 до 5) та Оцінка рівня впевненості у відповідях (від 0 до 3) (таблиці 1 та 2 відповідно). [8, 7]

Варіанти відповіді на питання – «Завжди»,«Зазвичай», «Іноді», «Рідко» та «Ніколи» означають відповідно 100%, 75%, 50%, 25% та 0% часу. А варіанти впевненості – «Висока впевненість», «Помірна впевненість», «Низька впевненість» та «Відсутність впевненості» означають, що користувач був приблизно на 100%, 67%, 33% та 0% впевнений у своїй відповіді відповідно [7]. Опитування міститиме n питань. Для проведення дослідження реалізується веб застосунок з метою опитування експертів/працівників енергосистем, який буде містити відповідні питання по метрикам стійкості з відповідями за шкалою Лайкерта.

Таблиця 1. Оцінка від користувача (1–5)

	Варіанти відповіді на питання				
Відповідь користувача	Завжди	Зазвичай	Іноді	Рідко	Ніколи
Змінна по шкалі Лайкерта	5	4	3	2	1

Таблиця 2. Оцінка рівня впевненості у відповідях (0–3)

	Варіанти впевненості			
Відповідь користувача	Висока впевненість	Помірна впевненість	Низька впевненість	Відсутність впевненості
Змінна по шкалі Лайкерта	3	2	1	0

5.2. Обробка даних

Позаяк змінні знаходяться в різних шкалах, використовується метод [9] для приведення їх до одної шкали. Формула перетворення:

$$Y = (B - A)\,\frac{x - a}{b - a} + A$$

де

- x – значення, що конвертується;
- a, b – мінімальне та максимальне значення початкової шкали $[0, 3]$ (тобто $a = 0,\ b = 3$);
- A, B – мінімальне та максимальне значення нової шкали $[1, 5]$ (тобто $A = 1,\ B = 5$);
- Y – сконвертоване значення в новій шкалі.

5.3. Обчислення оцінки кіберрезильєнтності

Результати опитування потребують релевантного алгоритму для вирахування оцінки кіберрезильєнтності. Кожен з показників та метрик має різний ступінь важливості з точки зору експертів. Тому, щоб «урівноважити» їх використовується метод ієрархічного аналізу (AHP), адаптований під R4-показники та метрики [7]. У AHP парні порівняння m критеріїв між собою формують матрицю C розміром $m \times m$. Кожний елемент відображає суб'єктивне порівняння критеріїв C_i та C_j. Матриця парних порівнянь має вигляд:

$$C = \begin{bmatrix} 1 & c_{12} & \cdots & c_{1m} \\ \frac{1}{c_{12}} & 1 & \cdots & c_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{c_{1m}} & \frac{1}{c_{2m}} & \cdots & 1 \end{bmatrix}$$

де:

$$C_{ji} = \frac{1}{C_{ij}}$$

Нормалізована матриця C_N обчислюється за формулою:

$$C_N(i, j) = \frac{C_{ij}}{\sum_{k=1}^{m} C_{ij}}$$

Ваги критеріїв отримуються як нормалізований правий власний вектор матриці C:

$$W = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{bmatrix}$$

причому:

$$w_i = \frac{1}{m} \sum_{j=1}^{m} C_N(i, j)$$

Для перевірки узгодженості обчислень обчислюють коефіцієнт узгодженості (CR):

$$CR = \frac{CI}{RI}$$

причому:

$$CI = \frac{\lambda_{\max} - m}{m - 1}$$

де:

- $\lambda_{\max}$ – домінантне власне значення матриці C;
- RI – випадковий індекс (таблиця з [10]).

Порівняння вважають прийнятним, якщо $CR \leq 0.1$.

6. Метрики кіберрезильєнтності

Для обчислення метрик кіберрезильєнтності було використано методологію [7]. Нехай $S_{i_{u_n}}$ та $CL_{i_{u_n}}$ позначають кількісне значення за шкалою Лайкерта відповіді користувача та перетворений бал рівня впевненості при відповіді на питання Q_i користувачем u_n відповідно. Припускається, що є n експертів, які дають відповіді $u_1, u_2, \ldots, u_n$.

Далі для кожної підметрики обраховується Expected Composite Score (ECS) – середнє зважене відповідей експерта (користувача) за такою формулою:

$$ECS_{M_{D_{SM_{u_n}}}} = \frac{\sum_{i=1}^{q} S_{i_{u_n}} \times CL_{i_{u_n}}}{\sum_{i=1}^{q} CL_{i_{u_n}}} \qquad (1)$$

Потім ці результати агрегуються геометричним середнім Overall Composite Score (OCS) за формулою:

$$OCS_{M_{D_{SM}}} = \left[\prod_{j=1}^{n} ECS_{M_{D_{SM_{u_j}}}}\right]^{\frac{1}{n}} \quad (2)$$

Далі у кожному домені D для метрики M підметрики SM підсумовуються з урахуванням ваг (метод AHP) – $D_{D_{M_{SM_i}}}$. Тоді Domain Score (DS):

$$d_{M_D} = \sum_{i=1}^{N} OCS_{M_{D_{SM_i}}} \times W_{M_{D_{SM_i}}} \quad (3)$$

Чотири основні метрики обчислюються як зважена сума доменних балів із вагами фізичного організаційного та технічного доменів:

$$R_i = w_{\text{phy}} \times d_{R_{i_{\text{phy}}}} + w_{org} \times d_{R_{i_{\text{org}}}} + w_{tech} \times d_{R_{i_{\text{tech}}}} \quad (4)$$

Після цього кожна метрика нормалізується:

$$R_{i_N} = \frac{R_i - 1}{4} \quad (5)$$

Далі знаходимо мінімальний очікуваний рівень обслуговування, який повинен підтримуватися системою у випадку кібератаки Critical Service Functionality (CSF):

$$CSF = SP_{\min} = \sum_{i=1}^{4} w_{r_i} \times R_{iN} \quad (6)$$

Після інциденту рівень функціональності описується експоненційною моделлю:

$$Q_R(t) = SP_{\min} \times e^{rt}, \quad (7)$$

$$r = \frac{1}{T} \ln\left(\frac{1}{SP_{\min}}\right) \quad (8)$$

де T – розрахунковий період відновлення.

Загальна кіберрезильєнтність визначається як:

$$R = \left[\frac{1}{T}\right]\left[\frac{1}{r}\right] SP_{\min}(e^{rT} - 1) \quad (9)$$

7. Висновки

У даному дослідженні розглядались поняття кіберрезильєнтності та особливості функціонування SCADA/WAMS-інфраструктури в енергосистемах. Також виокремлено типові кібератаки на енергосистеми та, на їх основі, адаптовано R4-методологію для оцінки кіберрезильєнтності енергопідприємства. Досліджено застосування шкали Лайкерта, методу аналізу ієрархій для обчислення ECS, OCS, DS, CSF та, нарешті, загальної кіберрезильєнтності. Проробблена робота є основою для проведення дослідження через опитування експертів/працівників енергосистеми задля оцінки кіберрезильєнтності енергопідприємства та надання подальших рекомендацій для її покращення.

Перелік використаних джерел

1. *IBM Corporation.* What is cyber resilience? — URL: https://www.ibm.com/think/topics/cyber-resilience.
2. *Гальчинський Л., Личик В.* Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження) // Інформаційні технології та суспільство. — 2023. — Вер. — 2 (8). — С. 27—33. — URL: https://journals.maup.com.ua/index.php/it/article/view/2665.
3. *Leirbukt A., Scholtz E., Paduraru S.* Taming the electric grid: Continuous improvement of wide-area monitoring for enhanced grid stability. — 2008. — Січ.
4. Research on Real-time Data Acquisition Technology Based on Distribution Automation Technology / X. Lu, Y. Gu, C. Liu, Q. Ye, K. Chen // IOP Conference Series: Earth and Environmental Science. — 2021. — Січ. — Т. 632. — С. 042006.
5. *Yadav G., Paul K.* Architecture and security of SCADA systems: A review // International Journal of Critical Infrastructure Protection. — 2021. — Т. 34. — С. 100433. — ISSN 1874-5482. — URL: https://www.sciencedirect.com/science/article/pii/S1874548221000251.
6. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities / M. Bruneau, S. Chang, R. Eguchi, G. Lee, T. O'Rourke, A. Reinhorn, M. Shinozuka, K. Tierney, W. Wallace, D. Winterfeldt // Earthquake Spectra - EARTHQ SPECTRA. — 2003. — Листоп. — Т. 19.
7. *Haque M. A., Shetty S., Krishnappa B.* ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems //. — 05.2019.
8. *Navarro D., Foxcroft D.* 2. A brief introduction to research design //. — 01.2025. — С. 15—42. — ISBN 978-1-80064-937-8.
9. *IBM Corporation.* Transforming different Likert scales to a common scale. — URL: https://www.ibm.com/support/pages/transforming-different-likert-scales-common-scale.
10. *Saaty T.* Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy/network process // Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales - Serie A: Matematicas. — 2008. — Січ. — Т. 102. — С. 251—318.