

МОДЕЛЮВАННЯ КАСКАДНОГО ПОШИРЕННЯ КІБЕРЗАГРОЗ У ВЗАЄМОЗАЛЕЖНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Вінницький національний технічний університет

Анотація

У роботі запропоновано графову модель каскадного поширення кіберзагроз у взаємозалежних інформаційних системах об'єктів енергетичної інфраструктури, зокрема в системах автоматизованого обліку з розумними лічильниками. Формалізовано механізм передачі збоїв між підсистемами на основі ймовірнісних характеристик зв'язків та агрегованого ризику. Показано, що врахування каскадних ефектів суттєво підвищує оцінку системного ризику порівняно з ізольованим аналізом окремих компонентів. Запропоновано застосування критерію ефективності контрзаходів для ранжування захисних заходів з урахуванням каскадних сценаріїв.

Ключові слова: каскадні кіберзагрози, графова модель, агрегація ризиків, критична інфраструктура, розумні лічильники, кіберфізичні системи, управління ризиками інформаційної безпеки.

Abstract

The paper proposes a graph-based model for cascading cyber threat propagation in interdependent information systems of energy infrastructure, including automated metering systems with smart meters. The failure propagation mechanism between subsystems is formalized using probabilistic link characteristics and aggregated risk. It is shown that accounting for cascading effects significantly increases systemic risk estimates compared to isolated component analysis. The application of a countermeasure effectiveness criterion for ranking protective measures considering cascading scenarios is proposed.

Keywords: cascading cyber threats, graph model, risk aggregation, critical infrastructure, smart meters, cyber-physical systems, information security risk management.

Вступ

Сучасні енергетичні системи дедалі глибше інтегрують інформаційні та комунікаційні технології, формуючи складні кіберфізичні комплекси. Інфраструктура розумного обліку (Advanced Metering Infrastructure, AMI), що включає розумні лічильники електроенергії, газу та води, шлюзи-концентратори, комунікаційні мережі та серверні платформи, є одним із найбільш розгалужених сегментів такої інфраструктури. Станом на кінець 2023 року у світі встановлено понад 1,06 млрд розумних лічильників, і ця кількість стрімко зростає [1]. Водночас розширення мережевої інфраструктури збільшує поверхню атаки: компрометація одного вузла може спричинити каскадний ефект, що поширюється на суміжні підсистеми - від рівня лічильника через шлюз до серверних додатків та систем SCADA [2].

Традиційні методи оцінки ризиків розглядають компоненти ізольовано, що не відображає реальної картини загроз у взаємозалежних системах. Як показує практика, атака типу Man-in-the-Middle на незахищений канал між лічильником і шлюзом може не лише спотворити дані обліку, а й стати точкою входу для подальшого проникнення в систему диспетчерського управління [3]. Статистика за 2023 рік свідчить, що 38% атак на розумні лічильники становили MITM-атаки, 27% - DoS-атаки, 19% - підrobка ідентифікаторів пристроїв [6]. Це зумовлює потребу в моделях, що враховують каскадне поширення загроз та дозволяють оцінювати кумулятивний ризик на рівні системи в цілому.

Метою роботи є розробка графової моделі каскадного поширення кіберзагроз у взаємозалежних інформаційних системах енергетичної інфраструктури та інтеграція цієї моделі з критерієм ефективності контрзаходів для оптимального розподілу ресурсів захисту.

Формалізація графової моделі каскадного поширення загроз

Інформаційну систему енергетичного об'єкта представимо як орієнтований зважений граф $G = (V, E, W)$, де $V = \{v_1, v_2, \dots, v_n\}$ - множина вузлів (компонентів системи), $E \subseteq V \times V$ - множина спрямованих ребер, що відображають залежності між підсистемами, а $W: E \rightarrow [0, 1]$ - функція ваг, яка визначає

ймовірність передачі збою від одного вузла до іншого. Типовими вузлами для АМІ-інфраструктури є: розумні лічильники (газові, електричні), шлюзи-концентратори, комунікаційна хмара, серверний додаток та SCADA-система [4].

Для кожного вузла визначається базовий ризик як добуток ймовірності реалізації загрози та потенційного впливу. Агрегований ризик системи обчислюється як сума внесків усіх компонентів [5]:

$$R_{total} = \sum_{i=1}^n P_i \times I_i, \quad i = 1, \dots, n \quad (1)$$

Каскадний ефект моделюється через механізм передачі збоїв між зв'язаними вузлами. Якщо вузол скомпрометований, ймовірність поширення загрози на суміжний вузол визначається вагою відповідного ребра. Кумулятивна ймовірність каскадного збою для вузла, що залежить від n підсистем, обчислюється за формулою [5]:

$$C = 1 - \prod_{j=1}^n (1 - p_j), \quad j = 1, \dots, n \quad (2)$$

де p_j - ймовірність передачі збою від j -го вузла-джерела. Ця формула відображає принцип: навіть якщо кожна окрема ймовірність передачі невелика, за наявності кількох залежностей кумулятивний ризик зростає суттєво.

Каскадні сценарії в інфраструктурі розумного обліку

Типова архітектура АМІ передбачає багаторівневу структуру: розумні лічильники передають дані на шлюз-концентратор через протоколи Modbus або LoRaWAN, шлюз пересилає агреговану інформацію до комунікаційної хмари через MQTT, а серверний додаток обробляє та візуалізує дані [1]. Кожен рівень є потенційною точкою входу для зловмисника, а вразливості класифікуються згідно з CWE: жорстко прописані облікові дані (CWE-798), незахищена передача (CWE-319), відсутність автентифікації (CWE-306) тощо [6]. На рис. 1 представлено графову модель каскадного поширення загроз у типовій АМІ-архітектурі з вагами ребер.



Рис. 1. Графова модель каскадного поширення загроз в АМІ-інфраструктурі

Розглянемо каскадний сценарій. Зловмисник здійснює атаку на рівні розумного лічильника, використовуючи вразливість жорстко прописаних облікових даних. Отримавши доступ, він маніпулює показниками та, використовуючи незахищений канал передачі, поширює атаку на шлюз-концентратор. Через шлюз, який агрегує дані від десятків лічильників, зловмисник отримує можливість впливати на комунікаційну хмару, а через неї - на серверний додаток та потенційно на SCADA-систему [3]. Прикладом реального інциденту є масштабна кібератака в Швеції у 2023 році, коли зловмисники здійснили MITM-атаку на незахищені канали передачі даних з розумних лічильників, що спричинило збитки понад 5 млн євро [6].

Важливо зазначити, що каскадний характер такого сценарію принципово змінює профіль ризику системи. На відміну від ізольованої атаки, яка впливає лише на один компонент, каскадне поширення загрози мультиплікативно збільшує потенційний збиток на кожному наступному рівні архітектури. Зокрема, шлюз-концентратор, який обслуговує десятки або сотні лічильників, стає критичною точкою ескалації: його компрометація надає зловмиснику доступ одразу до всього пулу підключених пристроїв та відкриває шлях до вищих рівнів інфраструктури. Класифікація вразливостей за CWE підтверджує цю закономірність - поєднання CWE-798 (жорстко прописані облікові дані на лічильнику), CWE-319 (незахищена передача між лічильником і шлюзом) та CWE-306 (відсутність автентифікації на рівні хмарного сервісу) формує безперервний ланцюг експлуатації, де кожна наступна вразливість стає доступною лише після використання попередньої. Саме такі багатовекторні ланцюги атак, що не можуть бути виявлені при ізольованому аналізі окремих компонентів, обґрунтовують необхідність графового підходу до моделювання кіберзагроз.

У графовій моделі цей сценарій формалізується як послідовність ребер: v_1 (лічильник) $\rightarrow v_2$ (шлюз) $\rightarrow v_3$ (хмара) $\rightarrow v_4$ (сервер) $\rightarrow v_5$ (SCADA). Наприклад, якщо ймовірності передачі збою становлять $p_{12} = 0,4$, $p_{23} = 0,3$, $p_{34} = 0,2$, то за формулою (2) кумулятивна ймовірність каскадного ураження серверного рівня становить $C = 1 - (1-0,4)(1-0,3)(1-0,2) = 1 - 0,336 = 0,664$. У табл. 1 наведено порівняння ізольованої та каскадної оцінки ризику для кожного вузла.

Таблиця 1.

Порівняння ізольованої та каскадної оцінки ризику вузлів АМІ

Вузол (компонент)	P_i	I_i	R_i ізольов.	R_i каскадн.	Приріст ризику
v_1 Лічильник	0,40	80	32,0	32,0	-
v_2 Шлюз	0,25	150	37,5	82,5	+120%
v_3 Хмара	0,15	200	30,0	78,6	+162%
v_4 Сервер	0,10	300	30,0	199,2	+564%
v_5 SCADA	0,05	500	25,0	332,0	+1228%
Разом (R_{total})	-	-	154,5	724,3	+369%

Як видно з табл. 1, ізольована оцінка дає сумарний ризик 154,5 ум. од., тоді як каскадна модель - 724,3 ум. од. (приріст +369%). Найбільш вразливим є рівень SCADA: його каскадний ризик у 13 разів перевищує ізольований, оскільки він залежить від усіх попередніх ланок. Це кількісно підтверджує необхідність саме системного підходу до оцінки ризиків.

Інтеграція з критерієм ефективності контрзаходів

Для практичного застосування графової моделі пропонується її поєднання з критерієм ефективності контрзаходів. Після застосування контрзаходу m параметри ймовірності та впливу оновлюються у відповідних вузлах, що змінює ваги ребер та кумулятивні ймовірності каскадних збоїв. Ефективність контрзаходу оцінюється через критерій [5]:

$$E_m = \frac{\Delta R_m}{C_{norm}(m)} \quad (3)$$

де ΔR_m - абсолютне зниження агрегованого ризику (з урахуванням каскадних ефектів) після застосування контрзаходу m , а $C_{norm}(m)$ - нормалізована вартість заходу. Ранжування контрзаходів за спаданням E_m дозволяє обрати заходи з найвищою «віддачею на одиницю витрат». Ключова відмінність від ізольованого підходу полягає в тому, що ΔR_m обчислюється з перерахунком каскадних ймовірностей за формулою (2), а не лише як зниження локального ризику окремого вузла [5].

Застосування цього підходу до АМІ-інфраструктури демонструє, що захист шлюзу-концентратора (впровадження взаємної автентифікації, шифрування TLS, використання LoRaWAN з вбудованим наскрізним шифруванням) має непропорційно високу ефективність. Цей вузол є точкою агрегації для десятків лічильників та одночасно точкою доступу до хмарної інфраструктури, тому посилення захисту саме на цьому рівні мультиплікативно зменшує кумулятивний каскадний ризик для всіх наступних рівнів системи. За потреби балансування між абсолютним і відносним зниженням ризику застосовується мультикритеріальний показник [7]:

$$F_m = \alpha \cdot \frac{\Delta R_m}{R_{before}} + (1 - \alpha) \cdot (1 - C_{norm}(m)), \quad \alpha \in [0,1] \quad (4)$$

що дозволяє налаштовувати пріоритети залежно від стратегічних чи бюджетних вимог конкретного енергетичного об'єкта.

Висновки

Запропонована графова модель каскадного поширення кіберзагроз дозволяє формалізувати взаємозалежності між компонентами інформаційних систем енергетичної інфраструктури та оцінити кумулятивний ризик, що виникає внаслідок послідовної компрометації вузлів. Числовий приклад для типової АМІ-архітектури (табл. 1) продемонстрував, що сумарний каскадний ризик (724,3 ум. од.) у 4,7 рази перевищує ізольовану оцінку (154,5 ум. од.), що кількісно підтверджує недостатність ізольованого підходу.

Інтеграція графової моделі з критерієм ефективності контрзаходів E_m забезпечує кількісну основу для оптимального розподілу ресурсів захисту з урахуванням каскадних сценаріїв. Показано, що в багаторівневій АМІ-інфраструктурі з розумними лічильниками пріоритетним є захист вузлів агрегації (шлюзів-концентраторів), оскільки вони мультиплікативно впливають на ризик усіх наступних рівнів.

Перспективи подальших досліджень включають валідацію моделі на цифрових двійниках реальних енергомереж, розробку адаптивних алгоритмів перерахунку каскадних ризиків у реальному часі на основі телеметрії SCADA-IDS, а також дослідження синергетичних ефектів комбінованих контрзаходів у контексті архітектури Zero Trust для промислового Інтернету речей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. IoT Analytics. Smart electricity meter market 2024: Global adoption landscape [Електронний ресурс] / IoT Analytics Research Blog, 21 лютого 2024. - Режим доступу: <http://iot-analytics.com>.
2. NIST. Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid / NISTIR 7628, National Institute of Standards and Technology, 2010.
3. Chan A., Zhou J. On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628 // IEEE Communications Magazine. - 2013. - Vol. 51, No. 1. - P. 58–65.
4. Kavallieratos G., Spathoulas G., Katsikas S. Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems // Sensors. - 2021. - Vol. 21, No. 5. - Art. 1691.
5. Буняк В.М., Лукічов, В.В. Класифікація та агрегація ризиків в інтелектуальних енергомережах. Вимірювальна та обчислювальна техніка в технологічних процесах. 2025. №82(2). С. 59–71. <https://doi.org/10.31891/2219-9365-2025-82-9>
6. Буняк В.М., Лукічов, В.В. Захист даних у системах обліку лічильників. Сучасні технології безпеки та інтеграція «Дії». Вимірювальна та обчислювальна техніка в технологічних процесах. 2025. №81(1). С. 445–455. <https://doi.org/10.31891/2219-9365-2025-81-56>
7. Буняк В.М., Лукічов В.В. Аналіз теоретичних властивостей критерію ефективності контрзаходів в енергомережах. Матеріали науково-практичної конференції «Кібербезпека енергетики», Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, 28 травня 2025 р. Київ: ІПМЕ ім. Г.Є.Пухова НАН України, 2025. С. 79-80.

Буняк Віталій Михайлович - аспірант кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: vetalbunjak@gmail.com

Науковий керівник: **Лукічов Віталій Вікторович** - канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Vitalii M. Buniak - Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vetalbunjak@gmail.com

Supervisor: **Vitalii V. Lukichov** - Cand. Sc. (Eng.), Associate Professor of Information Security Department, Vinnytsia National Technical University, Vinnytsia.