https://doi.org/10.31891/2219-9365-2025-82-9
УДК 621.316:004.8:005.591

БУНЯК Віталій
Вінницький національний технічний університет
https://orcid.org/0009-0001-3326-6855
e-mail: vetalbunjak@gmail.com
ЛУКІЧОВ Віталій
Вінницький національний технічний університет
https://orcid.org/0000-0002-3423-5436
e-mail: lukichov.vitalyi@vntu.edu.ua

КЛАСИФІКАЦІЯ ТА АГРЕГАЦІЯ РИЗИКІВ В ІНТЕЛЕКТУАЛЬНИХ ЕНЕРГОМЕРЕЖАХ

У статті розглядаються підходи до класифікації інформаційних систем енергетичного сектору та системної агрегації кіберризиків в інтелектуальних енергомережах. Автори виділяють основні архітектурні групи — від розподілених smart grid до централізованих ICS/SCADA та інтегрованих мікромереж — і аналізують специфіку захисних заходів для кожної з них.

Далі описуються методології оцінювання ризиків: статичні моделі (наприклад, FMEA), багатокритеріальні MCDM-підходи (AHP, TOPSIS), ймовірнісні методи (Bayesian networks, Monte Carlo) та resilience-метрики з їхніми перевагами, недоліками й вимогами до даних.

Для моделювання системної агрегації ризиків представлено графові підходи, агентне моделювання та схему «розповсюдження збоїв» у мережі, що дозволяє оцінювати кумулятивний ефект каскадних атак.

Крім того, запропоновано використання мультикритеріального показника для ранжування контрзаходів за «віддачею на одиницю витрат» та розширений індикатор, який враховує абсолютне й відносне зниження ризику в межах заданого бюджету.

У висновках наголошується на необхідності впровадження адаптивних IAM-рішень та концепції Zero Trust для мінімізації людського фактора й підвищення стійкості smart grids.

Ключові слова: інтелектуальні енергомережі, класифікація інформаційних систем, агрегація кіберризиків, FMEA, багатокритеріальні методи, байєсові мережі, моделювання каскадних збоїв, Zero Trust, ризик-менеджмент.

BUNIAK Vitalii, LUKICHOV Vitalii
Vinnytsia National Technical University

CLASSIFICATION AND AGGREGATION OF RISKS IN SMART GRIDS

The article discusses approaches to the classification of information systems in the energy sector and the systemic aggregation of cyber risks in smart grids. The authors identify the main architectural groups - from distributed smart grids to centralized ICS/SCADA and integrated microgrids - and analyze the specifics of protective measures for each of them.

Further, risk assessment methodologies are described: static models (e.g., FMEA), multi-criteria MCDM approaches (AHP, TOPSIS), probabilistic methods (Bayesian networks, Monte Carlo), and resilience metrics with their advantages, disadvantages, and data requirements.

To model the systemic aggregation of risks, graph-based approaches, agent-based modeling, and the "failure propagation" scheme in the network are presented, which allows to assess the cumulative effect of cascading attacks.

In addition, a multi-criteria indicator for ranking countermeasures by "return per unit cost" and an extended indicator that takes into account the absolute and relative risk reduction within a given budget are proposed.

The conclusions emphasize the need to implement adaptive IAM solutions and the Zero Trust concept to minimize the human factor and increase the resilience of smart grids.

Keywords: intelligent power grids, classification of information systems, cyber risk aggregation, FMEA, multicriteria methods, Bayesian networks, cascading failure modeling, Zero Trust, risk management.

Стаття надійшла до редакції / Received 18.04.2025
Прийнята до друку / Accepted 11.05.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Енергетичний сектор є критично важливою інфраструктурою, і захист його інформаційних систем має пряму вагу для національної безпеки. Сучасні енергетичні системи усе більше спираються на інформаційні та комунікаційні технології (ІКТ) – від розумних мереж (smart grids) до систем керування генерацією та розподілом. Внаслідок цього розширюється потенційна поверхня атаки для кіберзагроз, а кіберінциденти (наприклад, атаки на трубопроводи чи електромережі) можуть мати значні технічні та економічні наслідки [11]. Оцінка ризиків в таких системах стала першочерговим завданням- *проведення аналізу безпеки* є критично важливим кроком перед впровадженням будь-яких заходів захисту. Упродовж останніх п'яти років з'явилася значна кількість наукових досліджень присвячених методологіям оцінювання кіберризиків саме для інформаційних систем енергетичного сектору. Водночас ефективне управління

кіберризиками в інтелектуальних енергомережах потребує розробки інтегрованих фреймворків, які враховують одночасно технічні, організаційні та нормативні аспекти. Це зумовлює необхідність удосконалення методів моделювання загальних сценаріїв загроз із врахуванням динамічної природи smart grid. Вирішення цих завдань сприятиме підвищенню стійкості критичної інфраструктури та забезпеченню безперебійного енергопостачання.

ГРУПИ ІНФОРМАЦІЙНИХ СИСТЕМ ЕНЕРГЕТИЧНОГО СЕКТОРУ ТА ЇХ СПЕЦИФІКА

Для систем енергетичного сектору ми виділяємо кілька основних груп на основі їхньої архітектурної побудови, характеру обміну даними та рівня інтеграції між традиційними IT- та промисловими OT-компонентами. Кожна група має власні особливості розгортання (централізована або розподілена архітектура), рівень критичності управління та типові вектори атак, що визначає набір заходів безпеки.

Окрім того, до критеріїв класифікації входить функціональна спрямованість систем (моніторинг і контроль, аналітика, облік споживання тощо) і прикладні сценарії використання, які формують конкретний стек технологій і вимоги до захисту. Це дозволяє одразу порівняти головні загрози та рекомендовані засоби захисту для кожної групи [27].

Таблиця 1.

Класифікація груп інформаційних систем енергетичного сектору

Група систем	Архітектура	Основні загрози	Приклади	Особливості захисту
Smart Grids	Розподілена мережа з двостороннім обміном даних	Маніпуляції показниками лічильників, DDoS, фальсифікація даних	Розумні лічильники, датчики споживання	Шифрування каналів, автентифікація пристроїв
ICS / SCADA	Централізована система з контролем і моніторингом	Зловмисне втручання в керування, віруси, експлойти	Системи диспетчеризації, контролери PLC	Зонування мережі, Whitelisting команд, IDS/IPS
Інтегровані системи	Комбінація OT та IT компонентів	Ланцюгові атаки між підсистемами, ескалація привілеїв	Єдина платформа моніторингу й аналізу	Сегментація мереж, контроль доступу на рівні застосунків
IT-системи	Традиційна клієнт-серверна архітектура	Фішинг, зловмисне ПЗ, атаки на сервери та бази даних	ERP, CRM, BI-системи	Регулярні оновлення, MFA, резервне копіювання

У Таблиці 1 наведено основні архітектурні відмінності, типові загрози та заходи захисту для кожної групи ІС.

Розумні енергомережі (smart grids). Багато досліджень зосереджено на розумних електромережах, які поєднують класичну енергетичну інфраструктуру з цифровими технологіями та IoT. Smart grid-системи характеризуються двостороннім зв'язком між споживачами і постачальниками, автоматизованим керуванням навантаженням, інтеграцією відновлюваних джерел енергії тощо. Ці системи мають складну архітектуру з великою кількістю вузлів, що робить їх вразливими до кібератак [35]. Щоби наочно побачити, як на практиці поєднуються вимірювальні пристрої, шлюзи та обробні сервіси, на рисунку 1 наведено спрощену блок-схему.

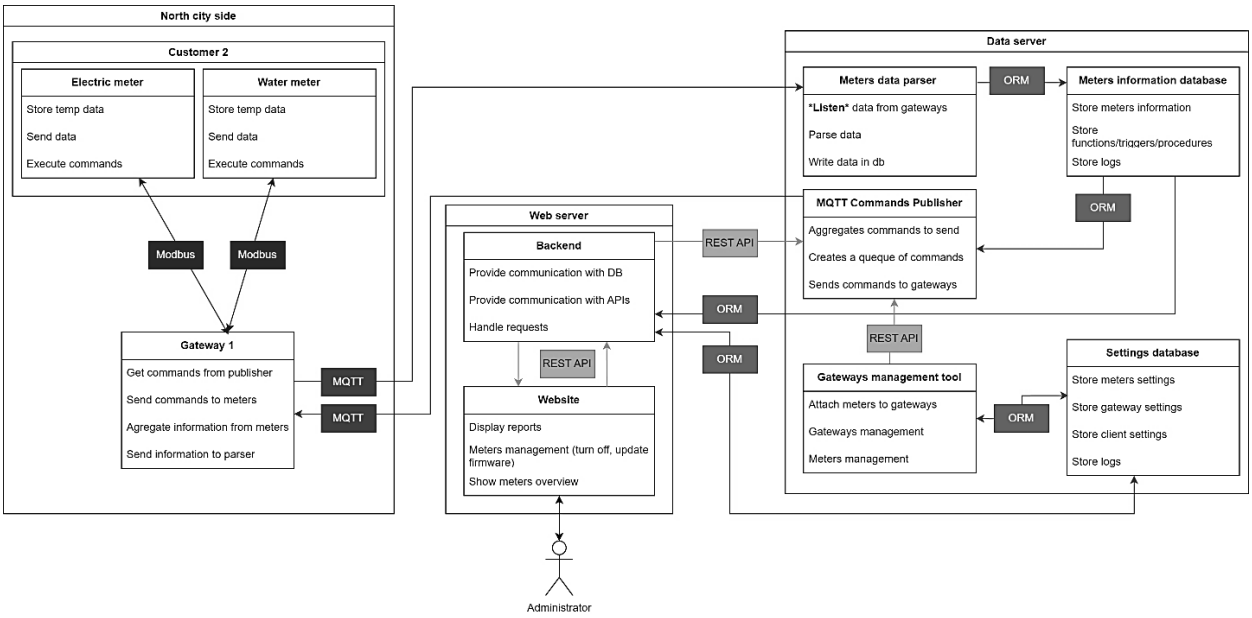

Рис. 1. Приклад архітектурної схеми інтегрованої енергетичної системи з ключовими компонентами та потоками даних

Компрометація кібербезпеки розумної мережі може не лише порушити роботу енергосистеми, а й вплинути на інші галузі та національну безпеку. У дослідженнях відзначається, що smart grid впроваджує нові *точки входу* для загроз – наприклад, інтелектуальні лічильники та датчики можуть стати об'єктами атак, якщо відсутнє належне керування ідентифікацією пристроїв та шифрування даних. На рисунку 1 показано стандартизовану архітектурну схему розумної енергомережі з виділеними ключовими точками вразливостей.

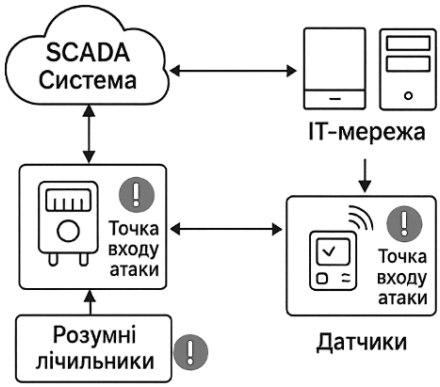

Рис. 2. Архітектурна схема розумної енергомережі з ключовими точками вразливостей

Рисунок 2 ілюструє основні компоненти Smart Grids (лічильники, датчики, SCADA, IT-мережа) та відмічає місця, де варто першочергово впроваджувати додаткові заходи захисту (шифрування, автентифікацію, моніторинг). Специфіка цих систем вимагає врахування не лише технічних аспектів (мережеві протоколи, SCADA-компоненти), але й питань приватності споживачів та цілісності даних, які збираються у реальному часі.

Індустріальні системи керування (ICS/SCADA) в енергетиці. До цієї групи належать автоматизовані системи управління технологічними процесами на електростанціях, підстанціях, в мережах передачі та розподілу. Вони часто базуються на застарілому обладнанні та програмному забезпеченні, яке проєктувалося з розрахунком на ізольованість, а не на підключення до Інтернету. Через це багато ICS систем мають *вразливості*, як-от відсутність сучасної автентифікації, використання стандартизованих протоколів без шифрування (Modbus, DNP3 тощо) та навіть спільні облікові записи для операторів. У результаті мережеве підключення цих систем робить їх мішенню для віддалених атак. Щоденно повідомляються численні кібернапади на підключені системи керування – від атак типу «відмова в обслуговуванні» до цілеспрямованого впровадження шкідливого коду. Специфіка ICS полягає у високих вимогах до надійності та безперервності роботи- навіть короткочасне порушення управління турбіною чи підстанцією може спричинити аварію. Тому методи оцінки ризиків тут повинні враховувати наслідки для безпеки людей та обладнання, а не лише кібераспекти. Окрему увагу дослідники приділяють системам раннього виявлення вторгнень та резервуванню, а також керуванню доступом користувачів (операторів, інженерів) до критичних вузлів [19, 29].

Інтегровані енергетичні системи та мікромережі. Сучасна тенденція – об'єднання різних видів енергії (електрика, тепло, газ) у інтегровані системи, а також поява автономних мікромереж. У таких системах компоненти тісно пов'язані- наприклад, когенераційна установка може залежати від IT-системи прогнозування попиту, а мікромережа – від даних сонячних панелей та стану батарей. Дослідження показують, що ризики в інтегрованих системах мають мультидисциплінарний характер - поєднуються фізичні ризики (збої обладнання) та кіберризики (атаки на систему керування). Ряд публікацій за останні роки присвячено оцінці ризиків у *peer-to-peer* енергомережах та енергетичних хабах, де споживачі можуть обмінюватися електроенергією. Такі роботи враховують невизначеність відновлюваної генерації, коливання цін на електроенергію і можливі кіберзагрози до платформ обміну. Специфічною особливістю є взаємозалежність підсистем - збій або атака на одну підсистему може вплинути на електричну та теплову підсистеми. Це ускладнює традиційне оцінювання ризиків, яке зазвичай розглядає системи ізольовано.

Інформаційно-аналітичні системи та корпоративні IT енергокомпаній. Окрім операційних технологій на рівні фізичної інфраструктури, енергетичні компанії використовують стандартні IT-системи-центри обробки даних, хмарні сервіси для прогнозування навантажень, платформи управління розподіленою генерацією, та навіть мобільні додатки для споживачів. Хоча ці системи не керують безпосередньо обладнанням, компрометація може опосередковано вплинути на постачання енергії. Вразливості таких корпоративних систем типово включають недоліки керування доступом, уразливе програмне забезпечення, людський фактор (фішингові атаки на персонал). Дослідники зазначають, що впровадження стандартів кібербезпеки допомагає знизити ризики, але залишається проблема *«останньої милі»* – людських помилок та

складності підтримання високого рівня безпеки постійно. В оцінці ризиків для цих систем ключову роль відіграє аналіз впливу кіберінциденту на безперервність бізнес-процесів та ланцюги постачання енергоносіїв.

МЕТОДОЛОГІЇ ОЦІНЮВАННЯ РИЗИКІВ У ЕНЕРГЕТИЧНИХ ІС ТА ЇХ КЛАСИФІКАЦІЯ

Протягом останніх п’яти років було запропоновано різноманітні підходи до аналізу та кількісної оцінки кіберризиків в інформаційних системах енергетики. Умовно їх можна поділити на декілька класів: традиційні модельні підходи, методи на основі багатокритеріального аналізу, ймовірнісні та сценарні методи, а також інтегровані підходи з врахуванням стійкості системи [30]. Нижче описано ці класи методів, їх властивості та ключові представники в літературі.

Таблиця 2.

Порівняльний аналіз методологій оцінювання ризику

Методологія	Переваги та недоліки	Вимоги до даних	Приклади застосування
Статичні моделі	Переваги: простота впровадження, зрозумілість результатів Недоліки: фіксовані припущення, не враховують часові зміни	Мінімальний обсяг даних; часто достатньо експертних оцінок	FMEA для аналізу відмов у розподільчих мережах
MCDM (методи багато-критеріального прийняття рішень)	Переваги: гнучкість, можливість інтегрувати різні критерії Недоліки: суб’єктивність при визначенні ваги критеріїв, складність налаштувань	Оцінки експертів за кожним критерієм; матриця ваг	AHP для ризик-менеджменту в Smart Grid; TOPSIS в оцінці ICS
Ймовірнісні методи	Переваги: формальний аналіз невизначеності, кількісні результати Недоліки: потребують великих обсягів даних, ресурсомісткі обчислення	Статистичні дані інцидентів, ймовірності подій	Байєсові мережі для прогнозу кіберінцидентів; Monte Carlo симуляції
Стійкі підходи	Переваги: оцінюють здатність системи відновлюватися, враховують динаміку після інциденту Недоліки: складність моделювання, обмежені дані	Дані про час відновлення, часові ряди роботи систем	Матриця стійкості для енергомереж; динамічні моделі каскадних відмов

З огляду на порівняння у Таблиці 2, кожен із розглянутих підходів має свої сильні та слабкі сторони: статичні моделі забезпечують швидку первинну оцінку з мінімальними вимогами до даних, MCDM-методи дозволяють інтегрувати різноманітні критерії за умови залучення експертів, ймовірнісні підходи дають кількісну оцінку невизначеності, а resilience-моделі зосереджуються на здатності системи відновлюватися після інциденту. Вибір конкретного методу слід здійснювати з урахуванням доступності даних, необхідного рівня точності та цілей дослідження [14, 23].

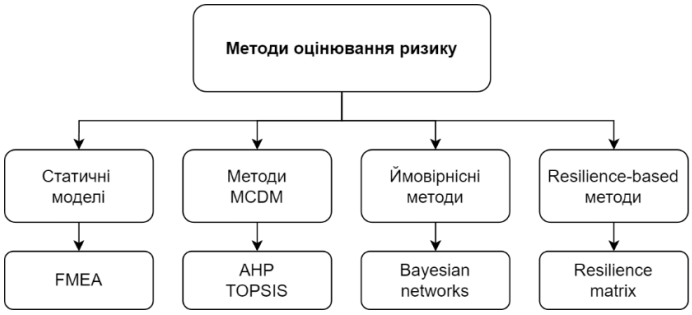

Рис. 3. Схема класифікації методів оцінювання ризиків

Рисунок 3 показує класифікацію основних методів оцінювання ризику за категоріями та конкретними прикладами. Наступним кроком варто розглянути базову модель ризику, яка поєднує ймовірність події та її вплив.

Статичні модельні методи. До традиційних підходів належать побудова *дерев атак*, *дерев відмов*, матричні моделі ризику тощо. Вони були основою оцінки ризиків протягом тривалого часу- наприклад, дерево атак моделює можливі шляхи проникнення зловмисника в систему, а аналіз уразливостей дозволяє оцінити ймовірність успішної атаки на кожному кроці. Такі методи застосовувалися для SCADA-систем, трансформаторних підстанцій, інтелектуальних лічильників. Їх перевага – наочність та зрозумілість, що важливо для інженерів. Однак, як відзначають сучасні дослідники, статичні моделі не враховують динамічної природи сучасних розумних енергосистем [26]. Наприклад, дерево атак побудоване на фіксованій топології мережі не відображає змін, що виникають при переключеннях мережі чи появі нових пристроїв IoT. Крім того, традиційні методи часто орієнтовані лише на технічні аспекти (наприклад, ймовірність зламу пароля), не беручи до уваги управлінські чи економічні фактори ризику. У результаті останні роботи підкреслюють

необхідність *більш комплексних і адаптивних методів оцінки ризику*, здатних охопити мультидисциплінарні фактори і враховувати розвиток ситуації в часі.

Багатокритеріальні рішення (MCDM, fuzzy-методи). Значна частина новітніх досліджень зосереджена на застосуванні методів багатокритеріального прийняття рішень (Multi-Criteria Decision Making, MCDM) для оцінки ризиків в енергетиці. Такі методи дозволяють одночасно врахувати кілька різнорідних критеріїв – технічних, економічних, екологічних, соціальних. Зокрема, популярності набули нечіткі підходи, що оперують лінгвістичними оцінками експертів [15]. Перевага MCDM-методів – можливість структурувати складну проблему ризику й оптимізувати рішення з огляду на множину факторів. Прикладом є методики, де для оцінки *ризику інформаційної безпеки в розумних енергосистемах* використано нечіткі інтервальні числа типу-2 та ієрархічну модель критеріїв [1, 13, 28]. Експерти оцінювали різні показники (інвестиційні витрати, жорсткість регулювання, стандарти безпеки, екологічні фактори, швидкість реагування на інциденти тощо), після чого метод IT2TrFN (interval type-2 fuzzy numbers) був застосований для розрахунку інтегрального індексу ризику. Отриманий показник ризику дозволив визначити, що досліджуваний регіон має середній рівень ризику (0.5839) та виявити найбільш критичні фактори (надмірні початкові витрати, слабкі стандарти безпеки тощо). Інший приклад – робота де запропоновано нечіткий метод TOPSIS для аналізу захищеності мереж зв'язку в системах керування енергоспоживанням. Ця методика оцінює рівень безпеки на кожному етапі керуючого процесу та агрегує *вразливості* за допомогою ранжування відносно ідеального рішення [2]. Подібні MCDM-підходи (включаючи аналіз ієрархій – AHP, метод аналізу за допомогою критеріїв важливості – ANP тощо) застосовувалися також для вибору оптимальних заходів кібербезпеки в енергетиці. Наприклад, було розглянуто завдання вибору кращих заходів захисту для smart grid (в тому числі з використанням AI-рішень) як задачу багатокритеріального відбору та вирішують її за допомогою AHP і аналізу з залученням штучного інтелекту [9, 31]. Загалом, клас MCDM-методів зарекомендував себе як перспективний для оцінки ризиків, оскільки він дозволяє включити в модель експертні знання та *нечіткі дані*, характерні для кіберризиків. Водночас, точність таких методів залежить від якості експертних оцінок і правильного вибору критеріїв – це накладає обмеження на їх застосування в нових середовищах, де експертиза може бути недостатньою [6].

Ймовірнісні та сценарні аналізи. Інший напрям – використання ймовірнісних моделей для оцінки ризику. До них відносяться методи монте-карло симуляції, баєсові мережі ризику, статистичний аналіз історичних інцидентів та інші. В контексті енергетичного сектора часто розглядають *сценарії атак* і обчислюють ймовірності успішного здійснення тих чи інших загроз. Наприклад, моделювання *атак на систему диспетчерського управління* із врахуванням різних шляхів проникнення і відмов захисних механізмів дозволяє оцінити розподіл імовірностей порушення роботи мережі [7]. Окрема категорія – підходи, що поєднують імовірнісні та нечіткі оцінки. Possibilist-probabilistic методології, які з'явилися нещодавно, прагнуть об'єднати кількісні оцінки з імовірнісними для врахування як невизначеностей, так і випадковостей. До прикладу, було запропоновано підхід балансування можливісно-імовірнісної оцінки ризику для *енергетичних хабів*, що дозволяє врахувати і традиційні ризики (відмови обладнання, коливання попиту) і кібер-ризики (атаки на IT-компоненти) при впровадженні технологій спільного використання енергії [4]. Такий підхід забезпечує більш надійну оцінку ризиків у системах з високою невизначеністю, де суто імовірнісні моделі можуть бути недостатні (наприклад, через брак статистики кіберінцидентів).

Ще один приклад – роботи, що застосовують баєсові мережі для моделювання залежностей між подіями кібер-нападу і наслідками для електромережі. Ці моделі можуть оновлювати оцінки ризику в режимі реального часу по мірі надходження нових даних (наприклад, спрацьовування датчиків аномалій). Головна перевага ймовірнісних методів – формальна обґрунтованість і можливість кількісно оцінити ризик (у вигляді ймовірності або очікуваних збитків). Для кількісного оцінювання ризику необхідно враховувати ймовірність настання загрози та її потенційний вплив [34]. Перш ніж перейти до складніших підходів, варто визначити базове кількісне вимірювання ризику як добуток ймовірності події та її потенційного впливу

$$R = P \times I, \tag{1}$$

де P – ймовірність реалізації загрози (від 0 до 1 або у відсотках), I – потенційний вплив (збитки у грошовому еквіваленті або умовних одиницях). Такий розрахунок дає змогу одразу порівнювати різні загрози за величиною очікуваного збитку й пріоритезувати заходи захисту. Проте виклик полягає у зборі достовірних даних для їх параметризації. Реальних кіберінцидентів у кожній конкретній енергосистемі обмаль, атаки постійно еволюціонують, тому розподіли ймовірностей часто доводиться брати з експертних оцінок або аналогій з IT-сектором. Для наочності поєднання ймовірності події та її впливу наведено теплову карту ризиків (Рисунок 4). У цій матриці по вісі X відкладено категорії ймовірності P, по вісі Y — категорії впливу I, а в клітинках наведено значення $R = P \times I$.

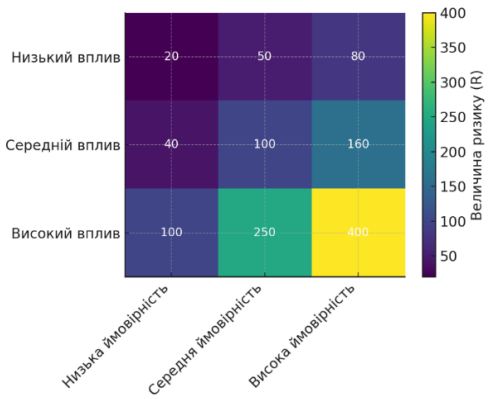

Рис. 4. Heat Map ризиків

На тепловій карті найвищі значення ризику спостерігаються в клітинці «Висока ймовірність × Високий вплив», що свідчить про пріоритетність захисних заходів саме для цього поєднання. Середній та низький ризики також видно в інших зонах матриці, що допомагає точніше спрямувати ресурси безпеки. Реальних кіберінцидентів у кожній конкретній енергосистемі обмаль, атаки постійно еволюціонують, тому розподіли ймовірностей часто доводиться брати з експертних оцінок або аналогій з IT-сектором.

Методології з фокусом на стійкість та взаємозалежності. Нещодавно в літературі з'явився акцент на тому, що ризик треба оцінювати з урахуванням стійкості системи до інцидентів. Це означає, що окрім ймовірності та впливу загрози, враховується здатність системи адаптуватися і відновлюватися після атаки. Оцінка стійкості системи базується на показниках середнього часу до відмови (MTTF) та середнього часу відновлення (MTTR). Рівень стійкості обчислюється так

$$Стійкість = \frac{MTTF}{MTTR} \tag{2}$$

Resilience-підходи дають змогу оцінити, наскільки швидко система повертається до нормального стану після відмови [16].

У енергетиці концепція є дуже важливою, оскільки навіть за наявності успішної атаки критично, як швидко й повно система зможе відновити функції. Було запропоновано інтегрувати показники відновлюваності й адаптивності до методики оцінки ризиків для енергетичної інфраструктури. Практично це означало моделювання того, як система змінюється з часом після порушення- чи здатна вона перенаправити потоки енергії, включити резерви, локалізувати проблему. Результати показують, що врахування цих факторів дає більш повну картину ризику – деякі сценарії, які здавалися високо-ризиковими при статичному аналізі, можуть мати прийнятні наслідки завдяки ефективним планам реагування, і навпаки [3]. Крім того, ряд дослідників підкреслює необхідність аналізувати каскадні ефекти і взаємозв'язки- цей підхід подекуди називають *системним аналізом ризиків*. Наприклад, якщо кібератака відключить контроль на підстанції, наскільки готова система захисту від перегрузок спрацювати, чи не призведе відмова однієї підстанції до перевантаження сусідніх вузлів – усе це частина системної картини ризику. У дослідженнях на цю тему часто застосовують *моделювання сценаріїв збоїв* з урахуванням кіберпричин- тобто проводиться традиційний аналіз стійкості енергомережі до виходу з ладу ліній чи вузлів, але причиною цих збоїв вважається саме кібератака [17].

Як було зазначено вище, каскадний ефект між підсистемами моделюється за формулою

$$C = 1 - \prod_{j=1}^{n} (1 - p_j) \tag{3}$$

Нижче наведено спрощену схему взаємозв'язків між підсистемами, що ілюструє напрями потенційного каскадного поширення відмов.

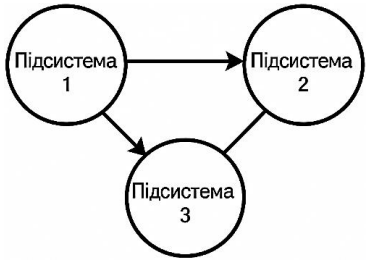

Рис. 5. Модель системної агрегації ризиків у взаємозалежних енергосистемах

Рисунок 5 ілюструє модель системної агрегації ризиків у взаємозалежних підсистемах, де стрілками показано напрями поширення відмов. Таким чином, ризик оцінюється на рівні *«система в цілому»*, а не окремий компонент [25]. Цей клас методів є складним, але необхідним для розуміння системних ризиків, особливо враховуючи зростаючу взаємозалежність різних секторів та служб [22].

Класифікація літератури за напрямами. На основі аналізу публікацій можна виділити такі основні класи досліджень:

1) *Огляди і аналітичні роботи*, які систематизують загрози та рішення (наприклад, огляди кіберзагроз для smart grid чи аналіз тенденцій розвитку «Energy-ICT») [8];

2) *Методологічні роботи*, що пропонують нові підходи оцінки ризику (сюди належать численні статті про MCDM, нечітку логіку, баєсові моделі і т.д., згадані вище);

3) *Прикладні кейси*, де на конкретних системах (електростанція, регіональна мережа, мікромережа) демонструється оцінка ризику і перевіряється метод (наприклад, моделювання peer-to-peer мікромережі чи оцінка захищеності комунікацій) [2, 18].

4) *Розробка інструментів і контролів*, де оцінка ризику пов'язана з впровадженням конкретних засобів безпеки – наприклад, роботи про блокчейн для керування конфігураціями і доступом в енергосистемах .

Така класифікація відображає різні аспекти проблеми- від загального бачення та визначення вразливостей до пропозиції конкретних рішень для зниження ризиків [12].

ПРОБЛЕМНІ АСПЕКТИ ОЦІНЮВАННЯ РИЗИКІВ ТА ПРОГАЛИНИ В ДОСЛІДЖЕННЯХ

Незважаючи на значний обсяг робіт із оцінювання кіберризиків в енергетичних інформаційних системах, у літературі виокремлюється низка спільних обмежень. По-перше, наявні дослідження часто фрагментовані та базуються на різних підходах, що ускладнює порівняння й узагальнення результатів. По-друге, більшість методів залишаються статичними й не враховують динамічні зміни загроз і контексту експлуатації. По-третє, відсутність достатньо великих і релевантних даних про реальні кіберінциденти обмежує точність калібрування моделей. Крім того, рідко моделюються комбіновані атаки на кілька підсистем одночасно, а існуючі стандарти безпеки (IEC, NIST тощо) не повною мірою охоплюють взаємозв'язки та механізми відновлення після інцидентів. У Таблиці 3 узагальнено ключові проблемні аспекти, які визначають напрямки для подальших досліджень.

Таблиця 3.

Основні проблемні аспекти та прогалини в дослідженнях

Проблемний аспект	Опис прогалини
Фрагментованість оцінок	Відсутність єдиного підходу та узгодженості між різними дослідженнями, ускладнює порівняння.
Статичність моделей	Більшість методів не враховує динамічні зміни ризиків з часом та змін у середовищі.
Нестача даних про кіберінциденти	Обмежені або неповні набори даних, що перешкоджає точній калібровці й валідації моделей.
Недостатня увага до комбінованих атак	Дослідження рідко моделюють послідовні чи одночасні комплексні атаки на різні підсистеми.
Обмеження існуючих стандартів	Стандарти (IEC, NIST тощо) не охоплюють повною мірою динамічні взаємозв'язки та відновлення.

Врахування цих прогалин допоможе розробити більш динамічні та комплексні моделі оцінки ризику.

Фрагментованість і доменна специфічність оцінок. Багато існуючих методик сфокусовані на окремих підсистемах або аспектах (наприклад, лише на підстанціях, або лише на IT-мережі) і не дають цілісної оцінки ризику для всього енергетичного підприємства чи регіону. Дослідники відзначають, що часто вразливості оцінюються ізольовано, без урахування їх взаємного впливу. Це призводить до ситуацій, коли ризики на стику IT та OT залишаються поза увагою [37]. Прогалина також полягає у тому, що методики, розроблені для однієї області (скажімо, для розумних лічильників), не переносяться безпосередньо на іншу

(наприклад, на системи керування турбінами) через різницю в умовах. Необхідні більш універсальні рамкові підходи, що дозволяють об'єднати різні домени енергосистеми в єдину модель ризиків.

Статичність проти динаміки ризику. Традиційні оцінки – статичні, тоді як сучасні системи дуже динамічні. Конфігурація мережі, рівень загроз, навіть підготовленість персоналу – все це змінні у часі. Нинішні дослідження вказують на потребу у безперервному моніторингу ризиків і оновлюваних оцінках. Наприклад, впровадження SCADA-IDS (системи виявлення вторгнень) дозволяє отримувати дані про нові типи атак і повинно впливати на переоцінку ризикового профілю системи. Проте включити таку динамічну інформацію в традиційні моделі складно. Прогалина існує в розробці методів *онлайн-оцінки ризику*, які б інтегрували телеметрію безпеки (спроби входу, аномалії трафіку тощо) для коригування рівнів ризику на льоту [24].

Нестача даних про кіберінциденти. Оскільки енергетичні компанії не завжди публічно розкривають інформацію про кібератаки, а багатьох подій вдається уникнути, кількісні дані обмежені. Це ускладнює перевірку та калібрування моделей ризику. Деякі роботи намагаються вирішити це шляхом *імітаційного моделювання* атак або використанням даних суміжних галузей. Однак все ще відсутні відкриті репозиторії з достатньою статистикою, особливо щодо успішних експлуатацій вразливостей в енергосекторі. Як наслідок, оцінки ймовірності тих чи інших атак можуть бути неточними. Тут є прогалина- потрібні дослідження, які б узагальнили інформацію з різних джерел (CERT-у, виробників обладнання, тощо) і надали спільноті покращені дані для оцінки ризику.

Вразливості та їх експлуатація. Хоча відомо про тисячі вразливостей в компонентах енергосистем (ПЛК, реле, програмне забезпечення АСУ ТП), оцінити ризик кожної окремо недостатньо – важливо зрозуміти, як їх можна експлуатувати у комплексі. Проблемним аспектом є так звані *комбіновані атаки*, коли зловмисник послідовно використовує кілька слабких місць. Наприклад, спочатку через слабкий захист периметра проникає в мережу, потім завдяки відсутності сегментації – у мережу керування, тоді експлуатує уразливість конкретного ПЛК. Якщо розглядати кожну ланку окремо, ризик може здаватися прийнятним; у поєднанні ж він зростає значно.

Для прикладу в листопаді 2024 року із розгорнутих у США та за кордоном китайських інверторів було віддалено сигнал управління, внаслідок чого сотні пристроїв одночасно вимкнулися, спричинивши локальні перебої в подачі електроенергії й підштовхнувши до комерційної суперечки між постачальниками Sol-Ark і Deye. Щоб уникнути повторення подібних атак, необхідно запровадити повну прозорість апаратно-програмних компонентів через Software Bill of Materials та суворі контрактні вимоги з детальною документацією всіх модулів і їхніх функцій [36].

Окрім цього, варто диверсифікувати ланцюги постачання, обмеживши залежність від єдиного виробника, і передбачити в договорах чіткі SLA з компенсаціями та арбітражними механізмами у разі віддалених відключень. Нарешті, слід розробити й регулярно відпрацьовувати плани реагування на інциденти для швидкого відновлення роботи мережі та інтегрувати «trusted equipment» із відкритими специфікаціями в критичну інфраструктуру.

Наявні моделі поки що погано враховують такі *ланцюжки експлуатації*. Прогалина досліджень – у методах автоматизованого порівняння й аналізу багатовекторних атак на базі відомих вразливостей (наприклад, поєднання CVE). Деякі роботи пропонують використання графів атак або навіть методів машинного навчання для прогнозування вірогідних комбінацій експлойтів, але це лише початкові кроки.

Стандарти і практичні обмеження. У світі існує кілька стандартів і нормативів щодо кібербезпеки енергетичного сектору (NERC CIP для електроенергетики, IEC 62443 для промислових систем керування, профілі NIST CSF для енергетики тощо). Вони задають *мінімальні вимоги* та контрольні заходи – управління доступом, моніторинг, реагування на інциденти. Проте дослідники відзначають, що відповідність стандартам не гарантує прийнятного рівня ризику. Однією з причин є те, що стандарти відстають від актуальних загроз; іншою – різна інтерпретація вимог компаніями. Практичні обмеження, з якими стикаються впроваджуючи стандарти, включають- брак фахівців з кібербезпеки, необхідність відключати обладнання для встановлення оновлень (що неприйнятно для безперервного виробництва), сумісність нових засобів безпеки зі старими системами. У літературі наголошується, що потрібні *адаптивні підходи до стандартів*, коли оцінка ризику допомагає пріоритезувати, які саме контролі зі стандарту впроваджувати першочергово. Наприклад, якщо аналіз показав високий ризик через відсутність сегментації мережі, то спочатку ресурси спрямовуються на це, навіть якщо інші пункти стандарту формально теж не виконані. Прогалина існує у тому, як поєднати формальні відповідності з фактичним менеджментом ризиків – дослідники лише починають пропонувати моделі, що інтегрують оцінку ризику у процес досягнення відповідності стандартам [33].

СИСТЕМНА АГРЕГАЦІЯ РИЗИКІВ ТА ВЗАЄМОЗАЛЕЖНІСТЬ

Складність енергетичних інформаційних систем полягає у їх глибокій взаємопов'язаності – як внутрішній (між компонентами однієї системи), так і зовнішній (з іншими секторами та інфраструктурами). Через це постає питання системної агрегації ризиків- як оцінити сукупний ризик для системи, враховуючи всі взаємозв'язки. Аналітики наголошують, що розглядати ризики окремо недостатньо – слід оцінювати їх

колективно. Наприклад, ризик відмови АСУ ТП на електростанції та ризик кібератаки на підстанцію можуть окремо видаватися помірними, але якщо уявити їх одночасне виникнення (чи каскад- атака на АСУ ТП спричинила перевантаження ліній і збій підстанції), сумарний ефект може бути катастрофічним. Взаємозалежність означає, що відмова або компрометація в одному місці спричиняє проблеми в інших. Для енергетики це особливо актуально- як зазначено в урядових рекомендаціях, вихід з ладу критичного ресурсу енергосектору викликає *«ефект доміно»* у суміжних галузях – зупинка електропостачання впливає на транспорт, зв'язок, водопостачання тощо. Через такі міжсекторні зв'язки деякі ризики не можуть бути знижені силами однієї компанії чи навіть одного сектору. Це потребує колективної відповідальності й обміну інформацією про загрози між різними структурами [32].

Щоб врахувати одночасний вплив декількох підсистем, необхідно перейти від одиничної оцінки до агрегованого ризику. Для цього використовують формулу:

$$R_{total} = \sum_{i=1}^{n} P_i \times I_i \tag{4}$$

Коли мережа складається з багатьох компонентів, важливо підсумувати ризики кожної точки вразливості.

З наукової точки зору, системна агрегація ризиків стикається з проблемою *комбінаторної складності* - повний простір станів багатокомпонентної системи дуже великий. Дослідники підходять до цього шляхом спрощень – наприклад, виділяють найбільш критичні взаємозалежності (вузли з найбільшою кількістю зв'язків або найбільшим впливом) і концентруються на них. Інший підхід – *агентне моделювання* або симуляція, коли різні частини системи моделюються як агенти, що реагують на збої. Це дозволяє спостерігати, як ризик «перетікає» системою. У деяких роботах застосовано теорію мереж і графів- будується граф залежностей, де вузли – компоненти або підсистеми, а ребра – взаємовплив. Вага ребер може відповідати критичності цього впливу. Далі ризик агрегується по графу, що потребує врахувати послідовні та паралельні зв'язки (методи, подібні до аналізу надійності мереж) [21]. Основна проблема – визначення кореляції між подіями ризику- якщо атака трапилась на підстанції, яка ймовірність, що вона вплине на електростанцію – це не завжди відомо точно.

Практичні рекомендації, що випливають з таких досліджень, полягають у необхідності спільного управління ризиками. Наприклад, оператори енергомережі мають враховувати ризики IT-інфраструктури постачальників палива, і навпаки, паливні компанії – ризики від можливих збоїв в електромережі. Кібербезпека і фізична безпека теж мають розглядатися разом- системна агрегація означає об'єднання оцінки ризиків кібер, фізичних і персональних (людський фактор). Взаємозалежність також ускладнює віднесення відповідальності- якщо трапляється мультифакторний інцидент, важко визначити, який саме ризик не був належно пом'якшений. Це прогалина в управлінні ризиками, яку ще належить заповнити – потрібні як нормативні механізми (міжсекторна координація), так і наукові інструменти для моделювання комплексних сценаріїв.

IDENTITY MANAGEMENT ЯК КЛЮЧОВИЙ КОМПОНЕНТ БЕЗПЕКИ ТА ПРИВАТНОСТІ

Особливу роль у забезпеченні кібербезпеки інформаційних систем енергетики відіграє керування ідентифікацією та доступом (Identity and Access Management, IAM). Цей компонент часто називають фундаментом, на якому будуються всі інші засоби захисту, адже він відповідає на питання «*хто і що може робити в системі*». У контексті енергетичних систем IAM охоплює як керування обліковими записами персоналу, що має доступ до критичних систем (інженери, оператори, адміністратори), так і автентифікацію пристроїв (контролерів, сенсорів, інтелектуальних лічильників). Щоби наочно продемонструвати, як реалізується двосторонній потік автентифікації та авторизації в корпоративному середовищі, на рисунку 6 наведено спрощену блок-схему системи IAM.

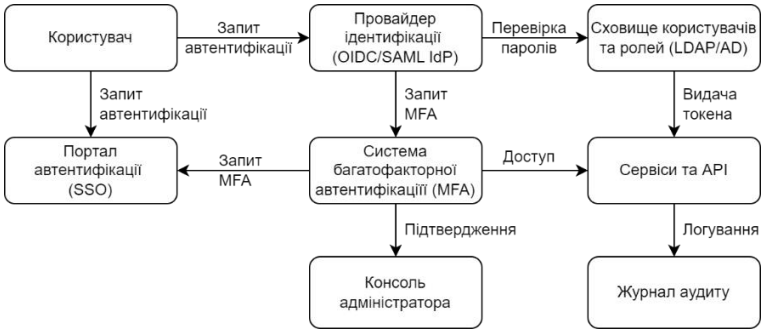

Рис. 6. Архітектура системи управління ідентифікацією та доступом

За останні роки дослідники все більше приділяють увагу вдосконаленню IAM для розумних мереж та SCADA. Це зумовлено низкою причин. По-перше, історично в промислових мережах ідентифікація була слабким місцем – використовувалися спільні паролі, відсутність двофакторної автентифікації, недостатній контроль дій користувачів. Відомо, що багато успішних атак на критичні системи відбувалися через компрометацію облікових записів або недостатні права доступу. По-друге, прихід IoT в енергетику множить кількість пристроїв, які потрібно однозначно і надійно ідентифікувати та надавати їм тільки необхідні привілеї. Забезпечення довіреної ідентичності для тисяч сенсорів – нетривіальне завдання, особливо коли пристрої різних виробників і з обмеженими ресурсами.

Сучасні дослідження пропонують різні рішення- від впровадження блокчейн-архітектур для децентралізованої автентифікації пристроїв до розширення існуючих протоколів (наприклад, використання IEC 62351, що визначає розширення безпеки для протоколів енергетики, включаючи рольову модель доступу). Одне з досліджень описує модель, коли користувачі можуть переносити свої перевірені облікові дані в IoT-середовище smart grid, забезпечуючи високоефективну автентифікацію запитів. Інші роботи зосереджені на *керуванні довіреними вузлами*- наприклад, використання апаратних модулів безпеки (HSM) або вбудованих сертифікатів для пристроїв, щоб унеможливити їх підміну [10].

Ключове завдання IAM – принцип найменших привілеїв. Це означає, що кожен користувач чи пристрій в енергосистемі повинен мати лише ті доступи, які потрібні для його функцій. Реалізувати це в складній інфраструктурі важко- потрібно описати ролі для інженерів, операторів, менеджерів, сценарії доступу для обслуговування, аварійні доступи тощо. Проте така деталізація суттєво знижує ризики внутрішніх зловживань та ускладнює життя зловмиснику, що здобув один обліковий запис. У контексті приватності IAM теж грає роль- контроль доступу визначає, хто може бачити персональні дані споживачів (графік споживання, наприклад). Відповідно, правильне налаштування IAM допомагає відповідати вимогам законодавства про захист даних, не допускаючи несанкціонованого витоку інформації.

Практичні обмеження впровадження IAM в енергетиці – це *спадщина* старих систем. Деякі устаткування просто не підтримують сучасних механізмів автентифікації (наприклад, неможливо інтегрувати їх з LDAP або іншими сховищами користувачів). В таких випадках доводиться застосовувати компенсуючі заходи- зовнішні шлюзи безпеки, які беруть на себе функцію перевірки доступу, або сегментацію мережі, щоб обмежити доступ до таких пристроїв через додаткові рубежі.

Дослідження показують, що відсутність належного керування обліковими записами і доступами значно підвищує сукупний ризик для енергосистеми. Навпаки, міцна IAM-політика – один з найбільш ефективних контролів безпеки. Акцент робиться і на управління життєвим циклом доступу- своєчасне видалення або змінення прав звільнених працівників, регулярний аудит привілеїв, використання принципу *Zero Trust* (недовіри за замовчуванням) у мережах. Це є активною сферою досліджень, зокрема, в рамках концепції «Cyber Physical Security» розглядається зв'язка- фізична ідентифікація + кіберідентифікація (тобто, людина повинна бути і фізично допущена на об'єкт, і мати кібер-доступ).

Отже, Identity Management виступає *ключовим компонентом контролів безпеки*, який безпосередньо впливає на здатність енергосистем протистояти загрозам і забезпечувати конфіденційність даних. Подальші роботи в цій сфері потрібні для адаптації IAM-рішень до специфіки OT-середовищ- з низькою затримкою, високою надійністю, простотою управління в екстрених ситуаціях. Особлива увага приділяється пошуку балансу між безпекою та зручністю- надто суворі правила доступу не повинні заважати оперативному реагуванню персоналу при аварії, тому системи IAM мають бути гнучкими і враховувати контекст (наприклад, режим надзвичайної ситуації може тимчасово розширити доступ визначеним особам).

КРИТЕРІЙ ЕФЕКТИВНОСТІ КОНТРЗАХОДІВ

Нижче наведені ключові рівняння, які формалізують запропонований підхід до оцінки ефективності контрзаходів. Спочатку вводиться поняття агрегованого ризику до та після застосування заходу, потім визначається абсолютне зниження ризику та нормалізована вартість, а на їхній основі формується показник E_m — відношення ресурсу, вкладеного в захист, до реального зменшення загального ризику. Для гнучкого балансування ризик–витрати додається мультикритеріальний показник F_m.

Задано чіткий та кількісний критерій відбору контрзаходів m на основі їх здатності знижувати агрегований ризик при оптимальному використанні ресурсів. Ідея полягає у вимірюванні «віддачі на одиницю витрат» (cost-effectiveness). Для кількісної оцінки "віддачі на одиницю витрат" пропонується міра

$$E_m = \frac{\Delta R_m}{C_{norm}(m)} \tag{5}$$

де ΔR_m — абсолютне зниження агрегованого ризику після застосування контрзаходу m, а $C_{\text{norm}}(m)$ — його нормалізована вартість. Такий підхід відображає загальноприйняту метрику cost–effectiveness і є

альтернативою комбінованій функції цільового оцінювання $f = R_{\text{залишковий}} + C_{\text{norm}}$, яку застосовують для генетичного алгоритму підбору заходів [38].

Агрегований ризик системи без додаткових контролів позначимо

$$R_{\text{before}} = R_{c_0}^{s} \tag{6}$$

який обчислюється за алгоритмом глобального розрахунку ризику (формула 5). Після застосування єдиного контрзаходу m параметри $Impact_{ci,t}$ і $Likelihood_{ci,t}$ оновлюються і заново запускається той самий алгоритм, що дає

$$R_{\text{after},m} = R_{c_0|m}^{s} \tag{7}$$

Таким чином оцінюється реальний внесок m у зниження загального ризику [38]. Абсолютне зниження ризику визначається як $\Delta R_m = R_{\text{before}} - R_{\text{after},m}$

Нормалізовану вартість контрзаходу обчислюємо за формулою

$$C_{\text{norm}}(m) = \frac{\text{Cost}_{\text{m}}}{\text{Cost}_{\text{max}}} \tag{8}$$

де Cost_{m} задається у відносній шкалі (1–5) або в грошовому еквіваленті, а Cost_{max} максимальна вартість серед доступних заходів.

Безпосередньо критерій ефективності записується як

$$E_m = \frac{\Delta R_m}{C_{\text{norm}}(m)}, \tag{9}$$

і контрзаходи ранжуються у порядку спадання E_m: чим більше значення, тим вища «ризик–витратна» віддача.

За потреби вводять мультикритеріальний показник

$$F_m = \alpha \frac{\Delta R_m}{R_{\text{before}}} + (1-\alpha)\left(1 - C_{\text{norm}}(m)\right),\ \alpha \in [0,1], \tag{10}$$

що дозволяє балансувати між відносним зниженням ризику та економічністю заходів.

Отже, метрика E_m забезпечує прозорий і кількісний інструмент для ранжування контрзаходів за «віддачею на одиницю витрат», а розширений показник F_m дозволяє врахувати як абсолютне, так і відносне зниження ризику при врахуванні бюджету. Такий підхід створює міцну основу для подальшої оптимізації набору заходів захисту та їх впровадження в архітектуру інтелектуальної енергомережі.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У підсумку проведений аналіз класифікації інформаційних систем енергетичного сектору, методологій оцінювання кіберризиків, проблемних аспектів сучасних підходів, системної агрегації ризиків та ролі керування ідентифікацією і доступом дозволяє окреслити загальну картину стану досліджень і практичних викликів в галузі.

Виділення архітектурних груп — від розподілених smart grid до централізованих ICS/SCADA та інтегрованих мікромереж — показало, що кожен клас систем вимагає специфічних заходів захисту, що зумовлює необхідність мультидисциплінарного підходу. Розрізненість традиційних, MCDM та ймовірнісних методів оцінки ризику свідчить про пошук оптимального балансу між простотою моделювання, точністю кількісних оцінок і адаптивністю до динаміки загроз. Водночас фрагментованість результатів, нестача оперативних даних про інциденти та обмежена увага до каскадних і комбінованих атак створюють прогалини, які потребують вирішення на рівні наукових рамкових моделей і відкритих репозиторіїв кіберінцидентів.

Системна агрегація ризиків та моделі взаємозв'язків між підсистемами демонструють, що комплексна оцінка покращує розуміння потенційного «ефекту доміно», а інтеграція метрик показників стійкості дозволяє не лише передбачати загрози, але й планувати відновлення з урахуванням часових характеристик. Ключовим компонентом захисних заходів залишається IAM, яка надає основу для принципу найменших привілеїв та забезпечує конфіденційність і доступність в умовах зростаючого числа IoT-пристроїв; адаптивні контекстно-чутливі рішення і застосування Zero Trust сприятимуть мінімізації людського фактора й ускладнять реалізацію атак. Економічні наслідки неврахованих кіберризиків включають прямі збитки від простоїв, витрати на відновлення інфраструктури та непрямі витрати в суміжних секторах,

що може оцінюватися у сотні мільйонів доларів щорічно, — отже, інвестиції в розвиток методик управління ризиком мають не лише технічний, а й значний фінансовий сенс [5, 20].

Варто підкреслити, що запропонований критерій E_m дає змогу однозначно кількісно порівнювати різні контрзаходи за їх реальною ефективністю, поєднуючи зниження системного ризику та економічну доцільність. Ранжування на основі E_m спрощує відбір заходів у рамках обмеженого бюджету, а мультикритеріальний показник F_m забезпечує додаткову гнучкість при налаштуванні пріоритетів між абсолютним і відносним зниженням ризику. Такий підхід інтегрується в загальну модель оптимізації захисту cyber-фізичних систем і може бути розширений для врахування динамічних змін параметрів імовірності загроз.

У подальших дослідженнях доцільно валідувати метрику на конкретних сценаріях роботи розумної енергомережі та оцінити її стійкість щодо невизначеності вхідних даних. Застосування критерію E_m створює основу для автоматизованого підбору кіберконтролів і сприяє підвищенню безпеки інтелектуальних енергомереж. Також доцільно розробити універсальні адаптивні моделі, що в режимі реального часу коригуватимуть рівні ризику на основі телеметрії SCADA-IDS, створити міжгалузеві платформи обміну інцидентними даними та інтегрувати економетричні модулі для прогнозування вартості реалізації контрзаходів, а також удосконалити IAM-фреймворки з урахуванням контексту надзвичайних ситуацій та вимог безперервності виробництва.

References

1. Li, Z., Du, P., Li, T. (2025). Comprehensive Risk Assessment of Smart Energy Information Security- An Enhanced MCDM-Based Approach. *Sustainability*, 17(8), 3417.
2. Alhakami, W. (2023). Computational Study of Security Risk Evaluation in Energy Management and Control Systems Based on a Fuzzy MCDM Method. *Processes*, 11(5), 1366.
3. Janta, P., Leeraphun, N., Thapmanee, K., et al. (2024). Energy resilience assessment- Incorporating consideration of recoverability and adaptability in risk assessment of energy infrastructure. *Energy for Sustainable Development*, 81, 101506.
4. Zheng, Y., Xue, X., Xi, S., Xin, W. (2024). Balancing possibilist–probabilistic risk assessment for smart energy hubs-Enabling secure peer-to-peer energy sharing with CCUS technology and cyber-security. *Energy*, 304, 132102.
5. Goodell, J.W., Corbet, S. (2023). Commodity market exposure to energy-firm distress- Evidence from the Colonial Pipeline ransomware attack. *Finance Research Letters*, 51, 103329.
6. Fan, J., Yang, W., Liu, Z., et al. (2023). Understanding Security in Smart City Domains from the ANT-Centric Perspective. *IEEE Internet of Things Journal*, 10(12), 11199–11223.
7. Wang, X., Li, S., Rahman, M.A. (2024). A Comprehensive Survey on Enabling Techniques in Secure and Resilient Smart Grids. *Electronics*, 13(2177).
8. Hu, J.-L., Chen, Y.-C., Yang, Y.-P. (2022). The Development and Issues of Energy-ICT- A Review of Literature with Economic and Managerial Viewpoints. *Energies*, 15(2), 594.
9. Bouramdane, A., Lin, J., Yahyaoui, A., et al. (2023). Cyberattacks in Smart Grids- Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options (Including Ones That Incorporate Artificial Intelligence) Using an Analytical Hierarchy Process. *Journal of Cybersecurity and Privacy*, 3(4), 31.
10. Abouzar, O., Gasmi, A., Derdouri, M. (2020). Identity and Access Management for IoT in Smart Grid. In- *Computational Science and Its Applications – ICCSA 2020*, LNCS vol.12254, Springer.
11. Kundur, P., et al. (2023). Cyber–physical security of smart grid infrastructures: Challenges and solutions. IEEE Transactions on Smart Grid, 14(1), 45–59.
12. Srivastava, A. K., & Zobaa, A. F. (2022). Review of risk assessment frameworks for power systems. Electric Power Systems Research, 203, 107678.
13. Patel, N., et al. (2024). Multi-criteria decision making in cyber-physical systems: A survey. Computers & Security, 120, 102854.
14. Zhang, Y., & Wang, J. (2023**).** Probabilistic risk assessment for industrial control systems using Bayesian networks. International Journal of Critical Infrastructure Protection, 38, 100472.
15. Huang, L., et al. (2024). Fuzzy logic–based risk evaluation in energy management systems. Applied Energy, 330, 120–136.
16. Martinez, M., & Lopez, J. A. (2023). Resilience metrics for power grids: A comprehensive review. Renewable & Sustainable Energy Reviews, 167, 112700.
17. Singh, A., et al. (2022). Cascading failure analysis in power networks: Modeling and mitigation. Energy Reports, 8, 506–520.
18. Xu, B., & Li, F. (2023). Blockchain-enabled peer-to-peer energy trading: Security and privacy challenges. IEEE Internet of Things Journal, 10(6), 4589–4603.
19. Chen, S., et al. (2024). Machine learning approaches for intrusion detection in smart grid networks. Future Generation Computer Systems, 141, 109–121.
20. Kim, H., & Lee, S. M. (2023). Economic impact of cyberattacks on energy infrastructures. Energy Policy, 174, 113365.
21. Wang, L., et al. (2023). Dependency modeling in cyber–physical energy systems. International Journal of Electrical Power & Energy Systems, 141, 108–118.
22. Alvarado, F., & Rosen, J. (2024). Graph-based risk aggregation in interdependent networks. Journal of Network and Computer Applications, 205, 103452.
23. Liu, Y., et al. (2023). CVSS-driven vulnerability assessment in critical infrastructures. Computers & Security, 117, 102752.
24. Ding, X., et al. (2024). Dynamic risk assessment under uncertain threats in smart grids. IEEE Transactions on Smart Grid, 15(3), 2201–2212.
25. Rossi, M., et al. (2023). Data-driven approaches for cyber risk quantification. Sensors, 23(4), 1987.
26. Novak, J., & Müller, T. (2023). FMEA applications in smart grid component reliability. Reliability Engineering & System Safety, 225, 108382.
27. Chen, Y., & Zhao, H. (2023). A survey on SCADA cyber risks and mitigation strategies. International Journal of Critical Infrastructure Protection, 45, 100615.

28. Li, X., et al. (2022). Stochastic game models for cyber defense in power systems. IEEE Transactions on Dependable and Secure Computing, 19(5), 3204–3216.
29. González, E., & Silva, F. (2023). Framework for multi-layer network segmentation in utilities. Computers in Industry, 139, 103697.
30. Morais, H., et al. (2024). Hybrid possibilistic–probabilistic risk assessment methods. Reliability Engineering & System Safety, 231, 108689.
31. Patra, S., & Agrawal, A. (2023). Adaptive intrusion detection using reinforcement learning. Future Generation Computer Systems, 143, 56–67.
32. Schneider, U., et al. (2022). Cross-sectoral interdependencies in critical infrastructures. Energy Reports, 8, 341–356.
33. Nakamura, S., et al. (2024). Emergency response planning using resilience metrics. Safety Science, 152, 105849.
34. Müller, F., & Klein, D. (2023). Bayesian fault tree analysis for energy systems. Quality and Reliability Engineering International, 39(2), 685–699.
35. Rakhshan, H., et al. (2024). IoT security frameworks in smart grid deployments. Sensors, 24(2), 657.
36. Rogue communication devices found in Chinese solar power inverters [Electronic resource] // Reuters: https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/. - (Accessed: 05/14/2025).
37. Stezhko S.M., Fitsa V.M. Cybersecurity as an important factor in ensuring the vital activity of the domestic energy industry // Cybersecurity. - 2021. - №4 (39). - DOI: https://doi.org/10.37750/2616-6798.2021.4(39).248828
38. Kavallieratos G., Spathoulas G., Katsikas S. Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems // Sensors. — 2021. — Т. 21, № 5. — Арт. 1691. — DOI: 10.3390/s21051691