УДК 005.334:621.311.243
UDC 005.334:621.311.243

DOI:10.33744/0365-8171-2025-117.2-394-406

ІНТЕГРАЦІЯ МОДЕЛІ SURE-RM В СИСТЕМУ УПРАВЛІННЯ ІТ-РИЗИКАМИ ПРОЄКТІВ ВІДНОВЛЮВАНОЇ ЕНЕРГЕТИКИ

INTEGRATION OF THE SURE-RM MODEL INTO THE IT RISK MANAGEMENT SYSTEM OF RENEWABLE ENERGY PROJECTS

Строкань Дмитро Володимирович*, аспірант, Черкаський державний технологічний університет , e-mail: StrokanD@gmail.com, тел. +380 93 423 88 02, Україна, 18001, м. Черкаси, вул. Байди Вишневецького, 34.*

https://orcid.org/0000-0002-0293-1170

Ткаченко Валентин Федорович, *кандидат технічних наук, доцент, Черкаський державний технологічний університет, e- mail: v.tkachenko@chdtu.edu.ua*

https://orcid.org/0000-0003-2592-1423

Анотація. Швидка цифровізація об’єктів відновлюваної енергетики формує новий клас ризиків, пов’язаних з інформаційною безпекою, цілісністю даних та стійкістю операційних процесів. В умовах зростання потужностей сонячних і вітрових електростанцій, інтеграції інтелектуальних систем керування та віддалених каналів моніторингу підвищується залежність бізнес-показників від надійності ІТ-/ОТ-ландшафтів. Наявні міжнародні стандарти управління ризиками (ISO 31000, ISO/IEC 27005, NIST RMF) не враховують повною мірою географічну розподіленість активів, сезонність генерації, гібридність SCADA-інфраструктур і специфіку взаємодії з ринковими та метеорологічними API. У статті запропоновано модель SURE-RM – структурований, практично орієнтований підхід до управління ІТ-ризиками у ВДЕ-проєктах. Модель охоплює повний життєвий цикл: від формування реєстру активів та сканування загроз до аналітики контексту, розробки і впровадження планів реагування та оцінювання ефективності прийнятих заходів. Особлива увага приділяється кількісному методу оцінювання ризику (P×I×D×C), який забезпечує прозору пріоритизацію сценаріїв та оптимізацію витрат на контрзаходи. Запропоновані артефакти (реєстр активів, каталог загроз, теплові карти ризиків, playbooks) інтегруються з методологіями PMBOK, PRINCE2 та Agile, що робить модель сумісною з традиційним та гнучким управлінням проєктами. На демонстраційному прикладі сонячної електростанції потужністю 10 МВт показано практичні кроки побудови карти загроз, ранжування ризиків та вибору стратегії реагування, що дозволяє знизити середній час простою, прискорити відновлення даних SCADA та зменшити фінансові втрати. SURE-RM забезпечує структуроване залучення зацікавлених сторін, формує метрики ефективності (MTTR, RTO, RPO, покриття MFA) та сприяє узгодженню із зовнішніми аудитами. Модель може масштабуватися для портфеля об'єктів різних типів генерації, підтримує актуалізацію каталогу загроз і автоматизацію аналітики. Розширена анотація відображає наукову новизну, практичну корисність і потенційні напрями подальших досліджень, серед яких – калібрування ймовірнісних моделей на основі історичних інцидентів, розроблення автоматизованих панелей моніторингу та економічна оцінка ефективності контрзаходів у довгостроковій перспективі.

Ключові слова. управління ризиками, кібербезпека, відновлювана енергетика, SURE-RM, SCADA, OT/IT, ICS, оцінка ризику, операційна стійкість.

Вступ. Сучасний етап розвитку енергетики характеризується масштабним переходом до відновлюваних джерел енергії (ВДЕ), що спричинено глобальними викликами зміни клімату, зростанням вартості традиційних енергоносіїв та необхідністю підвищення енергетичної незалежності держав. Інтеграція сонячних, вітрових, біоенергетичних та гібридних потужностей супроводжується глибокою цифровізацією виробничих процесів – від використання інтелектуальних систем моніторингу і керування до впровадження хмарних платформ для збирання та аналітики даних [1]. Таке перетворення створює принципово новий ландшафт ризиків, де інформаційна безпека й операційна стійкість стають не менш важливими, ніж класична технічна надійність обладнання.

Постановка проблеми полягає у тому, що цифрові сервіси, необхідні для ефективного функціонування ВДЕ-проєктів, одночасно є потенційними точками вразливості. Втрата конфіденційності даних SCADA-системи, збої у віддаленому доступі чи компрометація хмарних акаунтів можуть призвести до простою генерації, недоотримання прибутку та, у крайніх випадках, до дестабілізації енергосистеми регіону. Традиційні підходи до управління ризиками орієнтовані переважно на фінансово-економічні або техніко-експлуатаційні аспекти та недостатньо враховують комплексність IT/OT-інфраструктур відновлюваних електростанцій. Відсутність галузевих стандартів, здатних інтегрувати специфіку кіберзахисту з вимогами проєктного менеджменту, формує науково-практичний розрив, що стримує ефективне управління IT-ризиками.

Актуальність обраної теми зумовлена низкою факторів. По-перше, частка ВДЕ в енергобалансі України та світу стрімко зростає, і будь-які простої або порушення технологічного процесу прямо відображаються на економічних показниках [2]. По-друге, у галузі спостерігається збільшення кількості кібератак на об'єкти критичної інфраструктури – приклади атак на сонячні ферми у США, інциденти з вітровими турбінами у Європі демонструють глобальність проблеми. По-третє, динамічний розвиток нормативного середовища (вимоги ISO, IEC, регуляторні акти ЄС та НКРЕКП) змушує операторів ВДЕ-об'єктів доводити належний рівень управління ризиками при аудитах та сертифікаціях. По-четверте, збільшення кількості розподілених майданчиків і залучення підрядників підвищують ймовірність людських помилок та ускладнюють централізований контроль.

Аналіз останніх досліджень і публікацій свідчить, що в науковій літературі існує значний пласт напрацювань щодо загальних методів управління ризиками. Стандарти ISO 31000 [3] та ISO/IEC 27005 [4] описують процеси ідентифікації, оцінювання та реагування, однак не деталізують специфіку ОТ-середовищ енергетики. Концепція NIST RMF [5] пропонує структурований підхід до управління інформаційною безпекою, але потребує адаптації під виробничі процеси ВДЕ. Моделі FAIR та OCTAVE забезпечують кількісну та процесну оцінку ризику, однак їх імплементація у малих та середніх ВДЕ-проєктах ускладнюється значними витратами ресурсів[6].

Додатково слід відзначити, що сучасні підходи до оцінювання ризиків часто ігнорують контекст проєктного управління: обмежені строки будівництва, багаторівневу систему підрядників, інтеграцію з ринковими сервісами (біржі, прогнозування ціни) та потребу у швидкому відновленні після інциденту. Відсутність єдиного підходу ускладнює комунікацію між інженерно-технічними службами, менеджментом та аудиторами.

Мета даної роботи – розробити та апробувати модель SURE-RM, яка поєднує класичні принципи управління ризиками з доменно-орієнтованими практиками для IT/OT-ландшафтів ВДЕ-проєктів.

Завдання дослідження полягають у:

- визначенні ключових викликів управління IT-ризиками в контексті відновлюваної енергетики;
- порівнянні існуючих міжнародних стандартів і методологій;
- формуванні структурованої моделі, що охоплює етапи Scan, Understand, Respond, Evaluate;
- демонстрації застосування моделі на прикладі сонячної електростанції;
- обґрунтуванні метрик ефективності та напрямів подальшого вдосконалення.

Таким чином, запропонована у статті модель покликана заповнити прогалину між високорівневими стандартами та практичними потребами експлуатації ВДЕ-потужностей, забезпечити узгодженість управлінських рішень і створити підґрунтя для автоматизації процесів ризик-менеджменту в умовах цифрової трансформації енергетики.

Виклад основного матеріалу дослідження.

Модель SURE-RM (Scan – Understand – Respond – Evaluate – Risk Management) створена як відповідь на специфічні виклики управління ризиками в IT-/OT-середовищі проєктів відновлюваних джерел енергії [2]. Вона інтегрує напрацювання стандартів ISO 31000,[3] ISO/IEC 27005,[4] NIST RMF та практичний досвід експлуатації СЕС, ВЕС, біогазових установок. Концепція передбачає:

- Цілісність охоплення активів – врахування серверів SCADA, мережевого обладнання, хмарних платформ, інтерфейсів до ринкових API, мобільних клієнтів.
- Циклічність управління – неперервний процес від ідентифікації до вдосконалення.
- Прозорість та повторюваність – кількісне оцінювання дозволяє ранжувати ризики за зрозумілими критеріями.
- Інтеграція з проєктним менеджментом – сумісність із PMBOK, PRINCE2, Agile.
- Можливість автоматизації – формування реєстрів, теплових карт та дашбордів.

Концепція передбачає принципи, які узагальнені у Таблиці 1

Перший етап SCAN – інвентаризація активів і загроз. Мета етапу – створити повний каталог активів і можливих загроз. Реєстр включає сервери, контролери, мережеві комутатори, інвертори, VPN-шлюзи, облікові записи користувачів, хмарні сервіси, засоби прогнозування генерації. Кроки етапу:

- Мережеве сканування (Nmap, Nessus) – виявлення відкритих портів і сервісів.
- Аудит конфігурацій – перевірка політик доступу, паролів, журналів.
- Інтерв’ювання персоналу – збір інформації про неформальні процедури.
- Класифікація загроз – технічні збої, людський фактор, зловмисні дії, форс-мажори.

Результатом є карта активів та загроз (Рисунок 1), яка показує взаємозв'язки між вузлами і критичні точки впливу.

Таблиця 1 – Принципи та очікуваний ефект впровадження SURE-RM
Table 1 – Principles and expected effect of implementing SURE-RM

Принцип	Зміст	Очікуваний ефект
Комплексність	Урахування SCADA, мережевих вузлів, мобільних клієнтів, хмарних сервісів	Єдиний реєстр ризиків
Життєвий цикл	Від інвентаризації до моніторингу KPI	Постійне вдосконалення
Прозорість	Кількісне оцінювання P×I×D×C	Обґрунтоване ранжування
Узгодженість	Сумісність із PMBOK, PRINCE2, Agile	Зручність інтеграції
Автоматизація	Підтримка дашбордів, SIEM, API	Зменшення ручної роботи

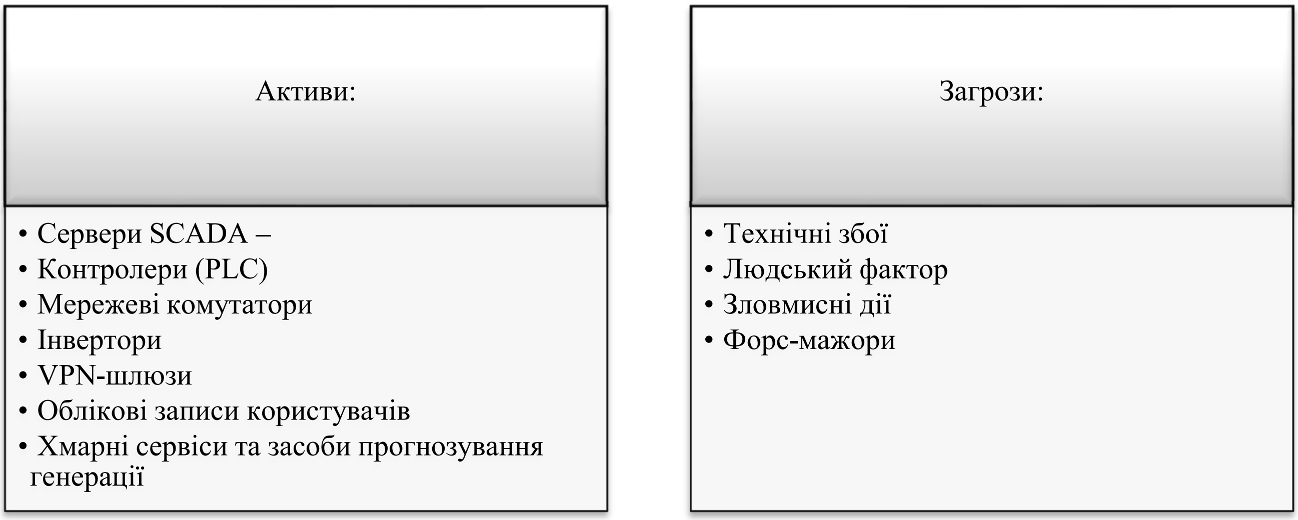

Рисунок 1 **–** Карта активів і загроз проєктів відновлювальної енергетики
Figure 1 **–** Asset and threat map of renewable energy projects

Наступний етап understand – аналіз контексту і вразливостей. Ціль даного етапу зрозуміти бізнес-цінність активів та специфіку ризиків. Метою даного етапу є розуміння як бізнес-контексту функціонування відновлюваного енергетичного об'єкта, так і технічних характеристик його IT/OT-інфраструктури, що дозволяє сформувати обґрунтовані параметри ризиків. Передусім слід визначити, які бізнес-цілі та показники безпосередньо залежать від IT/OT-ландшафту:

- Фінансові KPI: щоденний дохід від генерації електроенергії, штрафи за невиконання балансуючих зобов'язань, витрати на простої.

- Нормативні вимоги: регламенти НКРЕКП, стандарти ISO 27001/27005, галузеві протоколи кібербезпеки (наприклад, NERC CIP для критичної інфраструктури).
- Вимоги страхових компаній: наявність політик резервного копіювання, планів реагування на інциденти, журналів кіберподій.
- Інтереси стейкхолдерів: інвестори, державні органи, підрядники з обслуговування.

Розуміння бізнес-контексту дозволяє не лише виявити, які активи є критичними, а й оцінити можливі наслідки інцидентів з точки зору фінансів, регуляторного впливу чи репутаційних втрат. На етапі Технічного аналізу вразливостей проводиться аудит IT-/OT-середовища:

- Перевірка конфігурацій SCADA: наявність облікових записів із надмірними правами доступу, відсутність журналювання критичних подій, використання небезпечних протоколів (наприклад, Modbus без шифрування).
- Аналіз журналів подій (логів): пошук аномальної активності, повторних спроб автентифікації, нестандартних з’єднань ззовні.
- Тестування на проникнення (penetration testing): імітація атак для виявлення слабких місць у мережевій інфраструктурі, VPN-шлюзах та системах доступу.
- Інвентаризація вразливостей: використання сканерів (Nessus, OpenVAS) для отримання CVE-репортів і визначення рівня критичності.

Кожен сценарій ризику оцінюється за чотирма параметрами:

- P – Ймовірність (Probability): наскільки ймовірно, що сценарій реалізується в даних умовах (від 0 до 1);
- I – Вплив (Impact): наскільки серйозними будуть наслідки для бізнесу (фінансові втрати, простої, штрафи, пошкодження обладнання - чим більший вплив, тим вищий бал – пропонується шкала від 1 до 5);
- D – Виявленість (Detectability): наскільки легко або складно виявити інцидент. Низька виявленість означає більшу небезпеку, адже інцидент може тривалий час залишатися непоміченим (чим нижча виявленість, тим вищий бал – пропонується шкала від 1 до 5);
- C – Контрольованість (Controllability): наскільки компанія може контролювати ризик (наявність резервних каналів, захисних систем, планів реагування). Якщо контрольованість низька, бал є вищим (чим нижчий рівень контролю, тим вищий бал) пропонується шкала від 1 до 5.

Для розрахунку рівня ризику використовується формула:

$$R = P \times I \times D \times C$$

Де:

- R– інтегральний бал ризику;
- P – ймовірність реалізації ризику;
- I – ступінь впливу на бізнес;
- D – виявленість ризику (чим нижча виявленість – тим вищий бал);
- C – контрольованість ризику (чим нижчий рівень контролю – тим вищий бал).

У таблиці наведено приклади розрахунку ризиків для типових сценаріїв на сонячній електростанції.
Отримані значення дозволяють:

- виділити сценарії з найвищим рівнем ризику (наприклад, відмова інвертора – R=14.4), які потребують першочергових заходів;
- класифікувати ризики на високі, середні та низькі (за діапазоном балів, наприклад: 100–150 – високі; 50–99 – середні; <50 – низькі);

- сформувати пріоритети у планах реагування (етап RESPOND).

Аналіз дає змогу виявити сценарії з найвищим балом R та сформувати пріоритети.

Таблиця 2 – Приклад кількісної оцінки ризиків для сонячної електростанції
Table 2 – Example of quantitative risk assessment for a solar power plant

Сценарій	P(0-1)	I (1-5)	D	C	R
Несанкціонований доступ до SCADA	0.4	5	2	3	12
Відмова інвертора	0.3	4	3	4	14.4
Збій каналу VPN	0.2	3	2	3	3.6

Етап RESPOND – розробка стратегій реагування. Після того, як на попередньому етапі були виявлені та пріоритизовані ризики, наступним кроком є визначення та впровадження стратегій реагування. Основною метою етапу RESPOND є перетворення результатів аналізу ризиків у конкретні заходи, що здатні знизити ймовірність їх реалізації або мінімізувати наслідки. На цьому етапі формується цілісна система реагування, яка охоплює як технічні, так і організаційні аспекти, а також включає елементи автоматизації та комунікаційного менеджменту.

Одним із ключових принципів етапу є пріоритизація заходів. Формально вона базується на значенні ризику R=P×I×D×C, однак остаточне рішення враховує також бізнес-контекст, зокрема можливі фінансові втрати, регуляторні наслідки чи вплив на безпеку персоналу. Важливим правилом є пропорційність заходів: витрати на впровадження контролів не повинні перевищувати очікуваних втрат, за винятком випадків, коли йдеться про обов’язкові регуляторні вимоги.

Для управління ризиками застосовують чотири базові стратегії: уникнення (avoid), зменшення (mitigate), передача (transfer) та прийняття (accept). Наприклад, ризики з найвищими балами (понад 120) потребують негайного реагування, що може включати як тимчасові заходи ізоляції, так і довгострокові архітектурні зміни. Сценарії середнього рівня (60–119) обробляються шляхом планових заходів зі зменшення ризику, а малозначні ризики (нижче 30) можуть бути залишені під моніторинг із фактичним прийняттям.

Реалізація стратегій реагування охоплює цілу низку технічних і організаційних дій. До технічних заходів належить сегментація мереж із відокремленням OT-компонентів від офісних систем, застосування багатофакторної автентифікації для віддаленого доступу, впровадження систем виявлення вторгнень та SIEM-рішень, регулярне створення резервних копій і контроль їхньої цілісності, а також централізований патч-менеджмент. Організаційний блок включає розробку регламентів зміни конфігурацій, політики управління доступом за принципом найменших привілеїв, навчання персоналу та формування контрактних умов із постачальниками і підрядниками.

Ключовим інструментом реалізації реагування є playbook — стандартизований сценарій дій для конкретного типу інциденту. Типовий playbook містить опис умов його запуску, перелік негайних кроків локалізації інциденту, подальші дії з усунення причини та відновлення роботи системи, а також процедури комунікації й звітності. Наприклад, playbook для атаки типу ransomware на сервер SCADA передбачає автоматичне блокування підозрілих процесів, ізоляцію уражених вузлів, відновлення даних з перевірених копій і повідомлення регулятора в установлений строк. Важливо, щоб кожен playbook був інтегрований із системами автоматизації (SOAR), що скорочує час реагування і зменшує ризик людських помилок.

Ефективність заходів оцінюється через концепцію резидуального ризику. Для цього використовується коефіцієнт ефективності контролю, що дозволяє обчислити залишковий рівень ризику після впровадження заходів. Якщо початкове значення ризику R становило 120 балів, а комплекс заходів забезпечив зниження на 60%, то резидуальний ризик дорівнюватиме 48 балам, що переводить його в середню категорію.

Важливою складовою є регулярне тестування ефективності реагування. Для цього застосовуються різні практики: tabletop-навчання для менеджерів, відпрацювання сценаріїв аварійного відновлення на тестових середовищах, періодичне penetration-тестування, а також контрольовані перевірки працездатності резервних систем. Такі вправи дозволяють не лише підтвердити дієвість розроблених заходів, а й удосконалювати їх за результатами практичного застосування.

Оцінка результативності етапу RESPOND здійснюється за допомогою низки ключових показників: середній час до відновлення (MTTR), середній час до виявлення (MTTD), відсоток інцидентів, що були оброблені в межах визначених SLA, а також частка автоматизованих процесів реагування. Регулярний аналіз цих показників створює основу для постійного вдосконалення системи реагування.

Таким чином, етап RESPOND перетворює абстрактні значення ризиків на конкретні та вимірювані дії. Він поєднує технічні, організаційні та управлінські аспекти, що забезпечує практичну здатність компанії протистояти інцидентам і гарантувати неперервність генерації електроенергії у проєктах відновлюваної енергетики.

Завершальним елементом моделі SURE-RM є етап EVALUATE, який забезпечує неперервний контроль ефективності впроваджених заходів та їх адаптацію до змін у середовищі функціонування відновлюваних енергетичних об’єктів. Основна мета цього етапу полягає у створенні замкнутого циклу управління ризиками, коли результати оцінювання постійно враховуються при оновленні політик безпеки, процедур реагування та технічних налаштувань. Моніторинг здійснюється у кількох взаємопов’язаних площинах:

- Технічний моніторинг. Використання систем SIEM, OT-IDS та журналів подій дозволяє в автоматизованому режимі фіксувати всі інциденти, спроби вторгнень чи відхилення від нормальної поведінки обладнання. Автоматизація збору даних знижує ймовірність пропуску критичного інциденту.
- Аналітичний моніторинг. Дані, зібрані в реальному часі, інтегруються у візуальні дашборди (Power BI, Grafana). Це дає змогу керівництву й інженерам одночасно спостерігати за станом безпеки та оперативно приймати рішення.
- Організаційний моніторинг. Передбачає регулярні (щомісячні, щоквартальні, щорічні) огляди ключових метрик і аудитів відповідності вимогам міжнародних стандартів (ISO 27001, ISO/IEC 27005). Такі огляди дозволяють коригувати стратегії безпеки, визначати потребу у додаткових інвестиціях чи навчанні персоналу.

Для забезпечення об’єктивності оцінки застосовуються конкретні кількісні показники — KPI, що характеризують ефективність управління ризиками. У таблиці 3 наведено приклади метрик, які пропонується використовувати в межах моделі SURE-RM.

Як видно з таблиці, для практичної оцінки ефективності управління ризиками використовуються різні типи метрик: оперативні (наприклад, MTTR), технічні (рівень впровадження багатофакторної автентифікації), інцидентні (кількість критичних подій) та нормативні (відповідність ISO 27001). Кожен показник виконує специфічну функцію:

- MTTR (Mean Time to Recovery) — показує, наскільки швидко організація здатна відновити роботу після інциденту. Якщо MTTR перевищує 4 години, це свідчить про недостатню ефективність playbook-ів чи відсутність автоматизації.
- MFA Coverage — демонструє ступінь впровадження багатофакторної автентифікації, що є одним із ключових контролів проти несанкціонованого доступу. Досягнення рівня ≥ 90 % означає, що переважна більшість користувачів захищені додатковим фактором.
- Кількість критичних інцидентів — найжорсткіший показник, адже його цільове значення дорівнює нулю. Виявлення навіть одного критичного інциденту є сигналом для термінового перегляду системи захисту.
- Відповідність ISO 27001 — інтегральний показник, що відображає узгодженість внутрішніх процесів із міжнародними вимогами. Якщо рівень нижчий за 85 %, організація має розробити дорожню карту для досягнення відповідності.

Таблиця 3 – Метрики ефективності SURE-RM
Table 3 – SURE-RM performance metrics

Показник	Ціль	Періодичність
MTTR	≤ 4 години	щомісяця
MFA Coverage	≥ 90 %	щокварталу
Кількість критичних інцидентів	0	постійно
Відповідність ISO 27001	≥ 85 %	щороку

Етап Evaluate не обмежується збором даних. Він забезпечує зворотний зв’язок для всієї моделі SURE-RM. Результати моніторингу стають підставою для:

- оновлення реєстру ризиків (етап Scan);
- перегляду оцінок імовірності та впливу (етап Understand);
- корекції планів реагування (етап Respond).

Таким чином, управління ризиками набуває циклічного характеру, що відповідає концепції PDCA (Plan-Do-Check-Act), широко застосовуваної у стандартах ISO. Етап Evaluate є ключовим для забезпечення стійкості ВДЕ-проєктів у довгостроковій перспективі. Він дозволяє не лише контролювати ефективність впроваджених заходів, але й своєчасно адаптувати систему управління ризиками до нових викликів. Поєднання автоматизованого моніторингу, візуалізації результатів та регулярних аудитів забезпечує прозорість процесів і створює підґрунтя для прийняття обґрунтованих управлінських рішень.

Апробація моделі SURE-RM для керування іт-ризиками на сонячної електростанції потужністю 10 мВт. Пілотне впровадження проведено на сонячній електростанції потужністю 10 МВт (124 активи: 56 інверторів, 4 сервери SCADA, комутатори, шлюзи, облікові записи операторів). Ідентифіковано 47 ризиків, 12 із них критичних.

Загальна характеристика об’єкта Сонячна електростанція (СЕС) потужністю 10 МВт розташована в центральному регіоні України, займає площу близько 18 гектарів та має понад 30 000 фотомодулів, об’єднаних у 56 стрінгів через інвертори середнього класу. Керування виконується за допомогою SCADA-системи з віддаленим доступом для операторів і сервісних інженерів. Електростанція під’єднана до хмарної платформи прогнозування генерації та біржових API для торгівлі надлишками енергії. Наявність великої кількості віддалених з'єднань, підрядників та сторонніх сервісів формує значний спектр ризиків.

Підготовчий етап (інвентаризація та початкова оцінка). Під час стартового аудиту було сформовано реєстр 124 активів, серед яких:

- 56 інверторів Huawei SUN2000,
- 4 сервери SCADA (2 основних, 2 резервних),
- 18 мережевих комутаторів і маршрутизаторів,
- 2 VPN-шлюзи для віддаленого доступу,
- 62 облікові записи користувачів (оператори, інженери, підрядники).

Ідентифіковано 47 первинних ризиків, серед яких: компрометація облікових даних, несанкціоноване втручання у налаштування інверторів, помилки у плануванні бекапів, потенційні збої мережевого обладнання, вплив стихійних явищ (гроза, підвищений рівень пилу, температура). Для 12 сценаріїв оцінка R за формулою $P \times I \times D \times C$ перевищувала 100 балів, що класифікувалось як критичний рівень.

Впроваджені контрзаходи (етап Respond) На основі теплової карти ризиків розроблено комплекс дій:

1. Підвищення рівня автентифікації
   - увімкнено багатофакторну автентифікацію (MFA) для SCADA, VPN, хмарного моніторингу;
   - запроваджено політику зміни паролів кожні 90 днів.
2. Сегментація мережі та контроль доступу
   - впроваджено VLAN поділ виробничої мережі (SCADA, інвертори) та офісного сегменту;
   - використано ACL для обмеження трафіку між сегментами.
3. Резервування та бекапи
   - налаштовано автоматичне копіювання журналів та архівів даних SCADA кожні 15 хвилин на географічно віддалений сервер;
   - протестовано сценарії відновлення даних (RTO – 2 год).
4. Моніторинг і реагування
   - впроваджено SIEM-систему для агрегації логів з серверів, комутаторів, VPN;
   - створено playbooks реагування: блокування користувача, ізоляція вузла, перевірка журналів.
5. Фізичний захист і персонал
   - інстальовано камери з аналітикою руху та датчики відкриття шаф;
   - проведено навчання персоналу з кібергігієни.

Результати апробації (етап Evaluate). Протягом шести місяців після впровадження модель пройшла перевірку під час реальних подій:

- інцидент VPN: спроба входу з неавторизованої IP-адреси була заблокована системою MFA, інженер отримав сповіщення і активував playbook;
- помилка конфігурації інвертора: відхилення в роботі було автоматично зафіксовано SIEM і усунуто протягом 25 хв.

Основні досягнуті KPI:

- частка активів із ввімкненою MFA – 95 % (до впровадження – 20 %);
- середній час відновлення (MTTR) скорочено з 8 годин до 3 годин;
- кількість критичних інцидентів – 0;
- відповідність внутрішнім політикам та ISO 27001 – 88 %.

Економічний ефект. Моделювання показало, що середньорічний очікуваний збиток від простоїв скоротився приблизно на 42 %. При вартості простою 1 МВт близько 80 USD/година економія становить понад 200 тис. грн на рік. Витрати на впровадження заходів окупаються менш ніж за 9 місяців.

Висновки апробації. Використання SURE-RM забезпечило системне зниження ризиків, підвищення прозорості процесів і готовності до аудиту. Позитивний досвід дає змогу масштабувати модель на інші об'єкти портфеля та інтегрувати її з системами моніторингу виробітку, ERP та фінансовими модулями. Середній бал ризику до і після впровадження відображено на (Рисунок 2).

Вжиті заходи:

- багатофакторна автентифікація SCADA і VPN;
- VLAN-сегментація виробничих та офісних мереж;
- автоматизоване резервне копіювання кожні 15 хв;
- централізований моніторинг журналів SIEM.

Результати:

- зниження критичних ризиків на 60 %,
- скорочення MTTR з 8 до 3 год,
- відповідність політикам безпеки – 88 %.

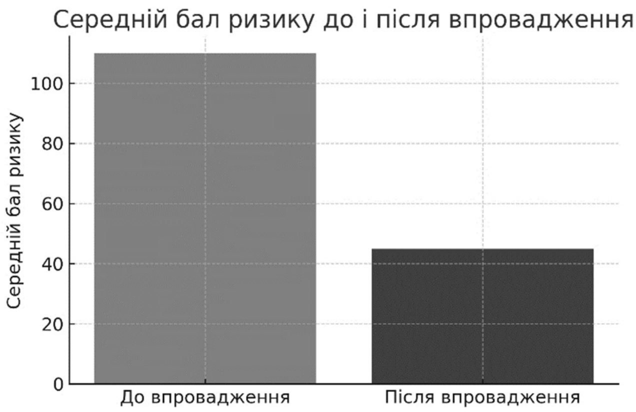

Рисунок 2 – Середній бал ризику до і після впровадження
Figure 2 – Average risk score before and after implementation

Висновки. Розвиток відновлюваної енергетики в умовах цифрової трансформації економіки вимагає якісно нового підходу до управління ризиками [7]. Масштабна інтеграція SCADA, телеметричних платформ, хмарних сервісів, віддалених API для торгівлі енергією та прогнозування генерації формує складне IT-/OT-середовище, де втрата контролю над даними чи збій у процесах може призвести до значних економічних втрат і порушення стабільності енергосистеми. Запропонована модель SURE-RM довела свою ефективність у вирішенні цього виклику, поєднавши класичні принципи управління ризиками зі специфічними потребами ВДЕ-проєктів.

Теоретичне обґрунтування: сформовано наукові передумови для адаптації стандартів ISO 31000, ISO/IEC 27005 та NIST RMF до домену ВДЕ. Визначено ключові чинники ризику – географічна розподіленість активів, залежність від хмарних сервісів, велика кількість підрядників, обмежені можливості фізичного контролю.

Розробка моделі SURE-RM: Виокремлено чотири взаємопов’язані етапи: Scan (ідентифікація активів та загроз), Understand (контекст і вразливості), Respond (розробка стратегій), Evaluate (моніторинг і вдосконалення). Запроваджено кількісний метод оцінки $R = P \times I \times D \times C$, що забезпечує прозору пріоритизацію ризиків.

Практичне впровадження: створено артефакти (реєстр активів, теплові карти, playbooks реагування), що інтегруються з методологіями PMBOK, PRINCE2 та Agile. Розроблено набір KPI (MTTR, RPO, RTO, MFA Coverage) для вимірювання ефективності.

Апробація на СЕС 10 МВт: побудовано каталог 124 активів, ідентифіковано 47 ризиків, із них 12 критичних. Впроваджено багатофакторну автентифікацію, сегментацію мереж, резервне копіювання, SIEM-моніторинг. Скорочено середній час відновлення з 8 до 3 год, знижено критичні ризики на 60 %, досягнуто відповідності політикам безпеки на рівні 88 %. Змодельований економічний ефект показав зниження очікуваних збитків від простоїв більш ніж на 40 %, окупність витрат – менше року.

Методологічні переваги: модель забезпечує єдину «мову ризиків» для технічного персоналу, менеджменту, аудиторів. Сумісність із проєктним підходом полегшує інтеграцію у фази планування, будівництва та експлуатації. Масштабованість дозволяє застосовувати модель як на одиничному об’єкті, так і в портфелі станцій різних типів генерації.

Наукова та практична новизна: новизна полягає в розробці гібридної моделі, що одночасно враховує специфіку IT/OT-ландшафтів ВДЕ та вимоги проєктного менеджменту. Практична цінність – готовність до впровадження у промислових умовах, що підтверджено апробацією на реальній СЕС. Модель дозволяє оптимізувати ресурси, мінімізувати ризики простоїв і підтримувати регуляторну відповідність.

Перспективи подальших досліджень: калібрування ймовірнісних моделей – збір статистики інцидентів на різних типах ВДЕ для формування бази ймовірностей та підвищення точності оцінок. Інтеграція машинного навчання – розробка предиктивних моделей на основі логів SCADA та метеоданих для прогнозування збоїв і підвищення готовності.

Модель SURE-RM продемонструвала, що системне управління IT-ризиками в проєктах відновлюваної енергетики можливе без надмірної складності, якщо застосовувати структурований, життєво-цикловий та практично орієнтований підхід. Її впровадження дозволяє:

- зменшити кількість критичних інцидентів і час простою;
- підвищити операційну стійкість та надійність генерації;
- забезпечити прозорість взаємодії зі стейкхолдерами та аудиторами;
- інтегрувати ризик-менеджмент у щоденні бізнес-процеси.

Подальша робота над автоматизацією, прогнозуванням та економічним обґрунтуванням зробить SURE-RM не лише інструментом контролю, а й ключовим елементом стратегії сталого розвитку енергетичних компаній.

Перелік посилань

1. Семко І.Б., Строкань Д.В., Бєлов О.Є. Project, Program, Portfolio Management. P3M-2022: Тези доповідей VII Міжнародної науково-практичної конференції : [у 2т.]. // Відповідальний за випуск П.О. Тесленко – Том 2. Одеса.: ІШІР, 2022. С. 77–80 с.

2. Строкань Д.В., Ткаченко В.Ф. Модель SURE-RM для управління іт-ризиками в проєктах відновлюваної енергетики матеріали XXII міжнародної конференції «Управління проєктами у розвитку суспільства» Київ: КНУБА, 2025. С. 267-271

3. ISO 31000:2018. Risk management – Guidelines. Geneva: International Organization for Standardization, 2018. 30 p.

4. ISO/IEC 27005, Information technology — Security techniques — Information security risk management, International Organization for Standardization, 2018.

5. National Institute of Standards and Technology (NIST). Framework for Risk Management in Information Technology (RMF). Gaithersburg, MD, 2018.

6. Данченко О.Б., Строкань Д.В., Цифрова енергетика в Україні - розбудова інноваційного майбутнього. Матеріали Міжнародної науково-практичної конференції Project, Program, Portfolio Management. P3M-2024: Тези доповідей IX Міжнародної науково-практичної конференції : [у 2т.]. // Відповідальний за випуск П.О. Тесленко — Том 1. — Одеса.: Інститут штучного інтелекту та робототехніки, 2024.- 255, с.200-205.

7. Приходько, І., Ігнатишин , В., & Приходько , Ю. (2024). Особливості розвитку відновлюваної енергетики в Україні та світі. *Економіка та суспільство*, (62).

INTEGRATION OF THE SURE-RM MODEL INTO THE IT RISK MANAGEMENT SYSTEM OF RENEWABLE ENERGY PROJECTS

Strokan Dmytro V. PhD student, Cherkasy State Technological University, e-mail: StrokanD@gmail.com, tel. +380 93 423 88 02, Ukraine, 18001, Cherkasy, Baydy Vyshnevetskoho St., 34. https://orcid.org/0000-0002-0293-1170

Tkachenko Valentin F., Candidate of Technical Sciences, Associate Professor, Cherkasy State Technological University, e-mail: v.tkachenko@chdtu.edu.ua, https://orcid.org/0000-0002-7008-7274

Abstract. The rapid digitalization of renewable energy facilities is creating a new class of risks related to information security, data integrity, and operational process resilience. With the growth in solar and wind power plant capacity, integration of intelligent control systems, and remote monitoring channels, the dependence of business indicators on the reliability of IT/OT landscapes is increasing. Existing international risk management standards (ISO 31000, ISO/IEC 27005, NIST RMF) do not fully take into account the geographical distribution of assets, seasonality of generation, hybridity of SCADA infrastructures, and the specifics of interaction with market and meteorological APIs. The article proposes the SURE RM model - a structured, practically oriented approach to IT risk management in renewable energy projects. The model covers the full life cycle: from the formation of an asset register and threat scanning to context analytics, development and implementation of response plans, and evaluation of the effectiveness of the measures taken. Special attention is paid to the semi-quantitative risk assessment method (P×I×D×C), which provides transparent prioritization of scenarios and optimization of costs for countermeasures. The proposed artifacts (asset register, threat catalog, risk heat maps, playbooks) are integrated with PMBOK, PRINCE2 and Agile methodologies, which makes the model compatible with traditional and agile project management. A demonstration example of a 10 MW solar power plant shows practical steps for building a threat map, ranking risks and choosing a response strategy, which allows reducing the average downtime, accelerating SCADA data recovery and reducing financial losses. SURE RM provides structured stakeholder engagement, generates performance metrics (MTTR, RTO, RPO, MFA coverage) and facilitates coordination with external audits. The model can be scaled for a portfolio of facilities of different generation types, supports threat catalog updating and analytics automation. The extended abstract reflects the scientific novelty, practical utility and potential directions for further research, including calibration of probabilistic models based on historical incidents, development of automated monitoring panels and economic assessment of the effectiveness of countermeasures in the long term.

Keywords: risk management, cybersecurity, renewable energy, SURE-RM, SCADA, OT/IT, ICS, risk assessment, operational resilience.

References

1. Semko I.B., Strokan D.V., Belov O.E. Project, Program, Portfolio Management. P3M-2022: Abstracts of the VII International Scientific and Practical Conference: [in 2 volumes]. // Responsible for the publication P.O. Teslenko – Volume 2. Odesa.: ISHIR, 2022. P. 77–80 p.

2. Strokan D.V., Tkachenko V.F. SURE-RM model for it risk management in renewable energy projects Materials of the XXII international conference “Project Management in the Development of Society” Kyiv: KNUBA, 2025. P. 267-271

3. ISO 31000:2018. Risk management – Guidelines. Geneva: International Organization for Standardization, 2018. 30 p.

4. ISO/IEC 27005, Information technology — Security techniques — Information security risk management, International Organization for Standardization, 2018.

5. National Institute of Standards and Technology (NIST). Framework for Risk Management in Information Technology (RMF). Gaithersburg, MD, 2018.

6. Danchenko O.B., Strokan D.V., Digital energy in Ukraine - development of an innovative future Proceedings of the International Scientific and Practical Conference Project, Program, Portfolio Management. P3M-2024: Abstracts of the IX International Scientific and Practical Conference: [in 2 vols.]. // Responsible for the publication P.O. Teslenko — Volume 1. — Odesa.: Institute of Artificial Intelligence and Robotics, 2024.- 255, p.200-205.

7. Prykhodko, I., Ignatyshyn, V., & Prykhodko, Yu. (2024). Features of the development of renewable energy in Ukraine and the world. Economy and Society, (62).

Дата надходження до редакції 13.06.2025.