ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Платформа управління ризиками в енергетичних компаніях»

на здобуття освітнього ступеня магістр
за спеціальності 124 Системний аналіз
(код,найменування спеціальності)
освітньо-професійної програми Інтелектуальні системи управління
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Юрій Яременко
(підпис) *(ім'я, ПРІЗВИЩЕ здобувача)*

Виконав:
здобувач вищої освіти
група САДМ-61 Юрій Яременко
(ім'я, ПРІЗВИЩЕ)

Керівник Ігор Патракеєв
к.т.н.
доцент
(ім'я, ПРІЗВИЩЕ)

Рецензент:
(ім'я, ПРІЗВИЩЕ)

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інформаційних систем та технологій
Ступінь вищої освіти магістр
Спеціальність 124 Системний аналіз
Освітньо-професійна прорама Інтелектуальні системи управління

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІСТ
_____ Каміла СТОРЧАК

"____" _____2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Яременку Юрію Вікторовичу
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Платформа управління ризиками в енергетичних компаніях
керівник кваліфікаційної роботи: Ігор Патракеєв к.т.н., доцент
(ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від " 30 " жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи «26» грудня 2025 р.
3. Вихідні дані кваліфікаційної роботи:
   1. Особливості функціонування енергетичних компаній.
   2. Методи управління ризиками в енергетичному секторі.
   3. Сучасні ІТ-рішення у сфері ризик-менеджменту.
   4. Алгоритми прогнозування та оцінювання ризиків.
   5. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
   1. Дослідження теоретичних основ управління ризиками в енергетичних компаніях.
   2. Аналіз існуючих інформаційних систем та підходів до автоматизації ризик-менеджменту.
   3. Розроблення та впровадження прототипу платформи управління ризикам
5. Перелік ілюстраційного матеріалу: *презентація*
6. Дата видачі завдання «30» жовтня 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір технічної, наукової та методичної літератури	30.10 – 05.11	
2.	Дослідження теоретичних основ управління ризиками	06.11 – 12.11	
3.	Аналіз інформаційних систем та цифрових рішень	13.11 – 19.11	
4.	Проєктування платформи управління ризиками	20.11 – 26.11	
5.	Реалізація програмного прототипу	27.11 – 10.12	
6.	Тестування та оцінювання ефективності	11.12 – 15.12	
7.	Формування висновків	16.12 – 18.12	
8.	Підготовка презентації та доповіді	19.12 – 22.12	
9.	Оформлення магістерської роботи	23.12 – 26.12	

Здобувач вищої освіти _____ Юрій Яременко
(підпис) *(ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ігор Патракеєв
(підпис) *(ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття ступня магістр: 73 стор., 13 рис., 13 табл., 45 джерел.

Мета роботи – розроблення концепції та програмного прототипу платформи управління ризиками в енергетичних компаніях, що забезпечує підтримку процесів ідентифікації, аналізу, оцінювання та моніторингу ризиків на основі сучасних інформаційних технологій.

Об'єкт дослідження – процеси управління ризиками в енергетичних компаніях.

Предмет дослідження – методи, моделі, алгоритми та інформаційні технології, що застосовуються під час побудови цифрових платформ управління ризиками.

Короткий зміст роботи.

У першому розділі проведено узагальнений аналіз сутності ризиків в енергетичній галузі та факторів, що їх визначають. Розглянуто ключові джерела небезпек, пов'язані з технологічними процесами, цифровими системами, організаційними та зовнішніми впливами. Сформовано підходи до класифікації ризиків та визначено методологічні основи їх ідентифікації й оцінювання з урахуванням сучасного рівня цифровізації енергетики.

У другому розділі досліджено сучасні інформаційні системи та інструменти, які використовують для моніторингу, аналізу та підтримки рішень у сфері управління ризиками. Описано можливості SCADA/EMS, систем кіберзахисту, телеметричних комплексів, IoT-рішень, платформ обробки великих даних і прогнозних моделей. Проаналізовано їхні переваги та виявлено наявні обмеження, що обґрунтовує потребу у створенні єдиної інтегрованої цифрової платформи ризик-менеджменту.

У третьому розділі представлено концепцію такої платформи та описано створений програмний прототип. Розроблено структуру даних, логіку роботи функціональних модулів та алгоритми оцінювання ризику.

Ключові слова: ризик, управління ризиками, енергетичний сектор, інформаційні системи, цифрова платформа, оцінювання, прототип.

ABSTRACT

The text part of the qualifying work for obtaining a bachelor's degree: 73 pp., 13 fig., 13 tables, 45 sources.

The purpose of the thesis is to develop the concept and a software prototype of a risk management platform for energy companies that supports the processes of identifying, analysing, assessing, and monitoring risks using modern information technologies.

The object of research is the risk management processes in energy companies. The subject of research is the methods, models, algorithms, and information technologies applied in the development of digital platforms for risk management.

Summary of the work.

The first chapter presents a theoretical analysis of the essence, nature, and classification of risks in the energy sector. It identifies the main factors influencing their occurrence and outlines key approaches to qualitative and quantitative risk assessment. The impact of technological, cyber, organisational, and natural factors on the reliability of energy infrastructure is examined.

The second chapter provides an analysis of modern information systems used to support risk management processes. Operational control systems, monitoring and analytical solutions, cybersecurity technologies, and data collection and processing tools are reviewed. The limitations of existing solutions and the need for an integrated digital platform for comprehensive risk assessment are identified.

The third chapter proposes the architecture of the risk management platform and presents its software prototype. The data structure, functional modules, and mechanisms for risk assessment are described. The results of testing the main components of the developed software are provided.

Keywords: risk, risk management, energy sector, information systems, digital platform, assessment, prototype.

Зміст

ВСТУП

Енергетичний сектор у сучасних умовах відіграє ключову роль у забезпеченні стабільного функціонування економіки, соціальної інфраструктури, промисловості, транспорту, систем зв'язку та оборонного комплексу. Електроенергетика є фундаментальною складовою життєдіяльності сучасного суспільства, і будь-яке порушення її роботи може призвести до значних технічних, економічних та соціальних наслідків. З огляду на це, питання підвищення надійності, безпеки та стійкості енергетичних систем є пріоритетними як на національному, так і на міжнародному рівнях.

Сучасні енергетичні компанії функціонують у середовищі, де поєднуються традиційні технічні ризики, викликані експлуатацією складних інженерних систем, та нові ризики, що виникають унаслідок цифровізації галузі. На зміну класичним технологічним процесам приходять інтелектуальні енергетичні мережі, автоматизовані системи керування, цифрові вимірювальні комплекси, аналітичні модулі прогнозування та інструменти оперативного моделювання стану мереж. Усе це формує нове інформаційно-технологічне середовище, в якому навіть дрібні збої можуть призвести до масштабних і непрогнозованих наслідків.

Управління ризиками в енергетиці зазнало суттєвих змін під впливом цифрової трансформації. Якщо раніше акцент робився переважно на технічних аспектах — стан обладнання, фізичний ресурс, профілактичні ремонти, то сьогодні значну частку ризиків становлять інформаційні та цифрові загрози. Впровадження SCADA/EMS-систем, IoT-пристроїв, інтелектуальних лічильників, систем дистанційного керування та автоматизації, цифрових двійників, аналітичних платформ на основі великих даних і машинного навчання суттєво підвищило ефективність керування енергетичними процесами, але водночас зробило енергетичну інфраструктуру залежною від якості програмного забезпечення, точності телеметрії, рівня кіберзахисту та надійності каналів зв'язку.

Особливої актуальності питання управління ризиками набуває в умовах зростання частоти кіберінцидентів. Сучасні кіберзагрози здатні не лише

порушувати конфіденційність або доступність інформації, але й безпосередньо впливати на фізичний стан енергетичного обладнання. Атаки на SCADA/EMS, віддалене втручання у роботу підстанцій, маніпуляція телеметричними даними, використання програм-вимагачів, компрометація промислових контролерів — це нові, високотехнологічні типи ризиків, що потребують принципово іншого підходу до управління безпекою.

Зростає і вплив зовнішніх факторів. Зміни в кліматі призводять до збільшення кількості погодних явищ, що загрожують енергетичній інфраструктурі. Збройні конфлікти, диверсії, терористичні атаки та руйнування об’єктів критичної інфраструктури становлять прямі фізичні ризики, що вимагають інтегрованих систем оцінювання вразливостей та моделювання сценаріїв розвитку подій.

У цьому контексті управління ризиками в енергетиці перестає бути окремою функцією та перетворюється на багаторівневий процес, який охоплює:

— моніторинг стану енергетичних об’єктів у реальному часі;
— збір і аналіз великих масивів даних;
— прогнозування поведінки систем і ризикових подій;
— розроблення рекомендацій для керівного персоналу;
— автоматизоване реагування у критичних ситуаціях;
— інтеграцію з корпоративними IT-системами;
— забезпечення кіберзахисту на всіх рівнях.

Сучасний ризик-менеджмент в енергетиці вже неможливо уявити без застосування інформаційних технологій. Оцінювання ризиків здійснюється за допомогою цифрових платформ, математичного моделювання, машинного навчання, прогнозних методів, систем виявлення аномалій та аналітичних інструментів. Накопичені дані про події, технологічні параметри, погодні умови, аварійність, навантаження, сигнали захисту та інші параметри дозволяють формувати комплексні моделі ризикової поведінки системи.

У міжнародній практиці розроблено низку стандартів, які визначають принципи побудови систем управління ризиками: ISO 31000, ISO/IEC 27001, IEC 62443, NERC CIP, COSO ERM та інші. Вони підкреслюють необхідність інтеграції

ризик-менеджменту у всі бізнес-процеси організації, забезпечення циклічного оновлення ризикових моделей, адаптації до зовнішнього середовища та належного рівня інформаційної безпеки.

Незважаючи на наявність сучасних методологічних підходів, більшість енергетичних компаній використовують фрагментовані або застарілі системи управління ризиками. Це ускладнює аналіз, призводить до розрізненості інформації, унеможливлює побудову цілісної картини ризикового середовища й ускладнює прийняття важливих оперативних рішень. Виникає потреба у єдиній цифровій платформі, здатній об’єднати всі процеси ризик-менеджменту в одному інформаційному просторі.

Сукупність факторів наведених вище обумовлює актуальність даної магістерської роботи, спрямованої на створення інтегрованої цифрової платформи управління ризиками, яка відповідатиме сучасним вимогам енергетичного сектору та забезпечуватиме високий рівень автоматизації процесів оцінювання, аналізу, моніторингу та прогнозування ризиків.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ОСНОВИ УПРАВЛІННЯ РИЗИКАМИ В ЕНЕРГЕТИЧНОМУ СЕКТОРІ

1.1 Теоретичні підходи до визначення ризиків в енергетичному секторі та роль інформаційних технологій

Енергетичний сектор у сучасному світі становить складну, багаторівневу систему, що об’єднує технологічні, економічні, організаційні та цифрові компоненти, які взаємодіють між собою у режимі реального часу. Його стійкість та надійність визначають не лише ефективність роботи окремих енергетичних підприємств, але й функціонування національної економіки, соціальної інфраструктури, промислових комплексів, транспорту, систем зв’язку й інших секторів, залежних від стабільного електропостачання. У таких умовах управління ризиками стає ключовим елементом для забезпечення безпеки та безперервності роботи енергетичних компаній, а впровадження сучасних інформаційних технологій є необхідною передумовою підвищення рівня ефективності даного процесу.

У науковій літературі ризик розглядається як багатовимірне явище, що поєднує в собі імовірність виникнення небажаної події та величину можливих негативних наслідків. Проте в енергетичному секторі ризик набуває значно складнішого змісту, оскільки енергетична система є інтегрованою структурою з високим ступенем взаємозалежності між елементами. Будь-яке відхилення в роботі одного компонента може спричинити каскадні ефекти і призвести до суттєвих технологічних та економічних наслідків. Наявність цифрових технологій у структурі енергетичних компаній значною мірою змінює природу ризиків, адже IT-системи стають одночасно ключовими інструментами управління і важливими джерелами вразливостей.

Однією з основних характеристик сучасної енергетики є її цифрова трансформація. Активне застосування IT-рішень, таких як SCADA/EMS системи, автоматизовані системи управління технологічними процесами, геоінформаційні

системи, інтелектуальні датчики, IoT мережі, прогнозні аналітичні модулі, цифрові двійники, технології великих даних і машинного навчання, створює нові можливості для вдосконалення управління ризиками. Водночас ці технології формують новий спектр ризиків, що пов’язані з цифровою вразливістю, надійністю даних, коректністю алгоритмів та безпекою інформаційних потоків.

Цифровізація енергетики спричиняє появу нового типу ризикового середовища, де класичні технічні ризики переплітаються з інформаційними, кібернетичними та алгоритмічними ризиками. Наприклад, некоректна робота алгоритму в системі прогнозування навантажень може спричинити неправильний вибір режимів роботи обладнання, що своєю чергою може призвести до перевантаження або аварії. Аналогічно, кібератака на систему SCADA може призвести не просто до втрати даних, а й фізичне порушення роботи обладнання. Таким чином, ризик в енергетиці сьогодні — це не лише технічна категорія, але й наслідок складної взаємодії компонентів системи.

Розуміння природи ризиків в енергетиці вимагає врахування її системної сутності. Енергетичні процеси є невід’ємно пов’язаними ланцюгами трансформації енергії. Кожний із них має власні ризики, які можуть бути як локальними, так і системними. Сутність системного ризику полягає в тому, що він не обмежується межами одного компоненту інфраструктури, а поширюється всією системою внаслідок структурних зв’язків між компонентами. Наприклад, вихід з ладу трансформаторної підстанції може призвести до перевантаження суміжних ліній електропередач, збільшення аварійних режимів роботи генераторів або порушення балансу в мережі, залежно від конфігурації системи.

Ключовим аспектом, що відрізняє сучасний підхід до ризиків в енергетиці від класичного, є вплив інформаційних технологій на всі рівні управління та експлуатації інфраструктури. Якщо у минулому інформаційні системи виконували допоміжні функції, то сьогодні вони є невід’ємною складовою більшості технологічних процесів. SCADA/EMS контролюють параметри та стан роботи обладнання, передають команди керування, здійснюють диспетчеризацію, забезпечують аварійне відключення та координацію роботи підсистем. Аналітичні

модулі обробляють величезні масиви даних у режимі реального часу, виявляючи аномалії. Інтелектуальні датчики передають критично важливу інформацію про навантаження, температуру, частоту та напругу. У таких умовах будь-який збій даних чи алгоритму може стати причиною значного ризику.

Інформаційні технології суттєво змінюють механізм формування ризиків. Наприклад, наявність IoT-пристроїв у мережі дозволяє здійснити моніторинг із безпрецедентною точністю, але водночас створює десятки тисяч точок потенційного кібернетичного проникнення. Використання машинного навчання підвищує точність прогнозів, але разом із цим створює ризики неправильного навчання моделі, помилкових висновків або некоректних рішень через невірні початкові дані. Застосування цифрових двійників дозволяє відтворювати поведінку системи та оцінювати її стійкість, але потребує значної кількості якісних даних та складних алгоритмів, які також можуть стати джерелом ризиків.

Однією з основних проблем сучасної енергетики є невідповідність між зростаючою складністю цифрових систем та традиційними методами управління ризиками. Велика кількість існуючих моделей управління ризиками орієнтовані на технічні відмови обладнання або на обробку статистичних даних за минулі періоди. У цифровому середовищі ці моделі є недостатніми, оскільки ризики часто виникають як наслідки взаємодії алгоритмів, інформаційних потоків та мережевих структур. Керування ризиками в енергетиці сьогодні має базуватися на інтеграції даних з різних джерел: SCADA, систем технічного обслуговування, IoT-пристроїв, метеорологічних служб, інформаційних систем прогнозування навантажень, систем кіберзахисту та бізнес-аналітики. Без об’єднання цих джерел даних неможливо сформувати цілісну сферу ризикового середовища. Саме тому цифрові платформи управління ризиками стають ключовими елементами сучасного енергетичного сектору.

У сучасних енергетичних компаніях інформаційні технології стали ключовою частиною організації виробничих процесів, моніторингу стану обладнання, координації оперативно-технологічного управління та забезпечення інформаційної взаємодії між підрозділами. Саме тому роль інформаційних

технологій у створенні ризикового середовища значно зросла, а ризики, пов’язані з цифровими технологіями, почали відігравати одну з ключових ролей у загальній структурі ризиків в енергетиці.

Цифрові системи керування енергетичними процесами створюють багатоканальне середовище обробки інформації, в якому дані збираються, передаються, аналізуються та використовуються для прийняття рішень. Якість цих даних, їх актуальність, повнота та достовірність є ключовими чинниками ефективності роботи енергетичної системи. Будь-яке пошкодження даних, затримка сигналів чи втрата інформаційних пакетів може призвести до погіршення точності регулювання режимів функціювання мережі, а у найгіршому варіанті — призвести до некоректного здійснення команд керування та аварійних ситуацій.

Ризики, пов’язані з інформаційними технологіями, охоплюють широкий спектр: від програмних помилок і збоїв у роботі обладнання до кібернетичних атак і некоректної роботи автоматизованих систем. Наприклад, збій у роботі датчиків IoT, які вимірюють навантаження або температурні параметри, може призвести до передачі недійсних даних у SCADA-систему. У свою чергу, SCADA може передати некоректні команди виконавчим механізмам, що створює ризик перевантаження або порушення режимів роботи обладнання. Таким чином, навіть незначне програмне чи апаратне пошкодження в цифровому компоненті може перетворитися у масштабний технологічний ризик.

Цифровізація призвела до того, що енергетичні компанії стали залежними не лише від фізичного стану обладнання, а й від стану та якості програмного забезпечення, інформаційних систем і цифрових процесів. Збільшення кількості точок взаємодії між технологічними та інформаційними системами призвело до зростання рівня ризиків. У великій кількості випадків ризики мають комплексний характер, коли взаємодія декількох систем формує нову, складну і важко прогнозовану ризикову ситуацію. Наприклад, відмова в роботі телеметричного сервера може призвести до втрати даних про задані параметри мережі, що призведе до прийняття некоректних рішень автоматизованими системами регулювання.

Інформаційні технології відіграють і позитивну роль у зменшенні ризиків. Завдяки цифровим платформам стало можливим провести більш глибокий аналіз даних, моделювати потенційні ситуації та прогнозувати можливі сценарії розвитку подій. Такі системи дають змогу виявити аномалії в реальному часі, вчасно попередити персонал та автоматично активувати механізми захисту. У поєднанні з сучасними методами штучного інтелекту та машинного навчання цифрові системи здатні більш ефективно підтримувати процеси керування ризиками, зокрема шляхом класифікації загроз, визначення тенденцій та формування рекомендацій щодо врегулювання.

Однак застосування інтелектуальних алгоритмів також пов’язане з певними ризиками. Моделі машинного навчання потребують значної кількості правильних даних, точність яких критично залежить від якості налаштування параметрів, вибору алгоритмів та підготовки тренувальних вибірок. У разі некоректного навчання моделі або неправильної інтерпретації результатів може виникнути ризик прийняття рішень, які не відображають реальної ситуації. Це може призвести до небезпечних помилок, якщо система приймає рішення без участі оператора.

Одним із головних аспектів сучасного середовища ризиків є значне зростання кібернетичних загроз. Згідно з міжнародними звітами, енергетика входить у трійку найбільш атакованих галузей через свою критичність та можливість отримання реальних фізичних наслідків у разі успішної атаки. Кібератаки на енергетичні компанії можуть бути спрямовані на: порушення конфіденційності даних, блокування доступу до систем, підміну команд керування, дестабілізацію процесів або навіть фізичне виведення з ладу обладнання. Особливу небезпеку становлять атаки на промислові контролери, через які здійснюється керування підстанціями, генераторами та лініями електропередач.

Кібернетичні загрози посилюються тим, що енергетичні компанії мають розгалужену IT-інфраструктуру, яка включає в себе: мережеві маршрутизатори, VPN сервери, сервери SCADA, історичні бази даних, аналітичні системи, хмарні сервіси, мобільні застосунки персоналу та десятки тисяч датчиків і лічильників, які взаємодіють з центральними платформами. Кожен із цих елементів є потенційною

точкою входу для кібератаки. Це потребує створення комплексних систем кіберзахисту, інтеграції SOC/SIEM-рішень, застосування інструментів виявлення аномальної активності та аналізу поведінкових патернів у мережах.

Зв’язок між цифровими технологіями та ризиками стає ще більш очевидним, якщо розглядати питання моніторингу енергетичної інфраструктури. Традиційні системи контролю параметрів мережі вже не можуть забезпечити необхідний рівень точності та оперативності. Сучасні мережі потребують використання синхронізованого вимірювання які здатні передавати дані з мілісекундною точністю. Такі пристрої збирають необхідну інформацію для аналізу стану енергосистеми, визначення режимів роботи, оцінювання стійкості та прогнозування можливих відхилень. Проте збільшення кількості даних пристроїв суттєво посилює ризик їх виходу з ладу або втручання у канали зв’язку.

Для управління ризиками на основі інформаційних технологій необхідне створення інтегрованих систем, що можуть об’єднувати дані з різних джерел, здійснювати комплексний аналіз, забезпечувати модельну підтримку рішень та формувати ситуаційну обізнаність у реальному часі. Традиційні системи ризик-менеджменту, засновані на ручному введенні даних, періодичному аналізі та експертних рішеннях, є недостатніми для забезпечення належного рівня безпеки в умовах динамічних цифрових загроз.

Інформаційні технології стають одним із головних інструментів для побудови сучасних платформ управління ризиками. Такі платформи здатні збирати інформацію в режимі реального часу, аналізувати її на основі алгоритмів машинного навчання, формувати індикатори ризиків, прогнозувати розвиток подій, відображати дані у зручній формі та забезпечувати підтримку прийняття рішень для операторів.

Створення цифрової платформи управління ризиками в енергетичних компаніях є складним процесом, який вимагає інтеграції різних видів інформаційних систем: SCADA, ERP, SOC/SIEM, систем диспетчеризації, аналітичних платформ, інтелектуальних датчиків, IoT-пристроїв, систем управління технічним обслуговуванням та IT-інфраструктурою. Об’єднання даних

систем створює багатошарову інформаційну модель, здатну відображати стан енергооб'єктів, виявляти потенційні ризики та забезпечувати ефективні механізми реагування.

Важливим аспектом управління ризиками в енергетичному секторі є розуміння взаємозв'язку між технологічними та інформаційними процесами, які формують основу сучасної діяльності енергетичних компаній. У минулому технологічні процеси були більш ізольованими від IT-середовища, проте сьогодні межа між ними практично зникла. Усі елементи енергетичної інфраструктури починаючи від генераторів та підстанцій до побутових лічильників. Все це є частиною великої цифрової екосистеми, у якій інформація циркулює постійно й безперервно. Цифрові технології відіграють ключову роль в сфері енергетики, відкривши можливості для переходу до інтелектуальних мереж, гнучкого балансування попиту та пропозиції, оптимізації енергетичних потоків та підвищення ефективності енергоспоживання.

Водночас, цифровізація висунула перед енергетичними компаніями нові складні завдання, серед яких — необхідність забезпечення стійкості, точності та цілісності інформаційних потоків. У цій системі кожен елемент відіграє ключову роль у створенні ризикової ситуації, і саме тому сучасне управління ризиками потребує комплексного підходу, що враховує всі взаємозв'язки між компонентами.

Сучасні інформаційні системи, що використовуються в енергетиці, включають десятки різнорівневих модулів, покликаних підтримувати роботу технологічного циклу. На базовому рівні функціонують засоби автоматизації та контролю: промислові контролери, сенсори, датчики та пристрої релейного захисту. На вищих рівнях працюють SCADA-системи, що забезпечують централізоване керування та моніторинг. Ще вище розташовані EMS — системи управління енергетичними режимами, які займаються плануванням балансів, оптимізацією навантажень і прогнозуванням. Паралельно діють системи кіберзахисту, призначені для виявлення та нейтралізації зовнішніх і внутрішніх загроз. Над усім цим знаходяться аналітичні платформи, здатні виконувати складні математичні розрахунки й моделювання на основі великих масивів даних.

Кожний із даних рівнів має власні ризики. Наприклад, промислові контролери схильні до фізичних збоїв, викликаних зносом обладнання чи перепадами напруги. SCADA-системи можуть бути вразливими до кібератак, помилок у програмному забезпеченні, проблем із синхронізацією даних та відмов серверів. Аналітичні платформи залежать від точності алгоритмів, правильності та точності вхідних даних та стабільності роботи баз даних. Інформаційні мережі можуть бути порушені внаслідок зовнішніх атак або внутрішніх технічних несправностей.

Усі ці фактори створюють складну матрицю ризиків, яку важко аналізувати без використання сучасних цифрових інструментів. Саме тому впровадження платформ управління ризиками, побудованих на основі інтеграції даних, машинного аналізу та автоматизованого прогнозування, стає ключовим напрямом розвитку енергетичних підприємств.

Одним із найбільш суттєвих джерел ризику в цифровій енергетиці є обробка великих масивів даних. Постійне збільшення кількості датчиків, інтелектуальних лічильників та IoT-пристроїв призводить до того, що енергетичні компанії щоденно отримують терабайти інформації. Обробка таких обсягів даних потребує потужних обчислювальних засобів, а сама система має бути надзвичайно стійкою до збоїв. У разі втрати або пошкодження даних можуть виникнути значні проблеми, пов’язані з неправильним прогнозуванням навантажень, недостовірним визначенням стану обладнання чи неправильним оцінюванням рівня ризику.

Питання якості даних є додатковою проблемою. У багатьох випадках дані можуть бути неповними, або спотвореними через технічні несправності чи втручання. Низька якість даних є одним із головних ризиків цифрової енергетики, оскільки на її основі будуються важливі моделі та алгоритми. Якщо вихідні дані є некоректними, то аналітичні системи можуть формувати неправильні рекомендації, що сприятиме прийняттю неефективних або небезпечних рішень.

У таких умовах надзвичайно важливою стає побудова системи верифікації, валідації та очищення даних. Такі системи дозволяють покращити якість

інформаційних потоків та зменшити ризики, пов’язані з використанням недостовірної інформації.

Ще одним важливим напрямом, що формує ризикове середовище в енергетиці, є зростаюча складність інформаційних мереж. Сучасні енергетичні компанії використовують широкий спектр комунікаційних технологій починаючи від застарілих протоколів промислової автоматизації до сучасних систем передачі даних у хмарі. Кожен тип мережі має свої ризики, і побудова єдиного захищеного інформаційного контуру є складним технічним завданням. Загрози можуть виникати внаслідок неправильної конфігурації мережевого обладнання, відсутності актуальних оновлень, недотримання правил кібербезпеки або використання небезпечних каналів зв’язку.

Однак, ризики інформаційної безпеки в енергетиці можна віднести до категорії системних ризиків, оскільки вони впливають не лише на цифрову інфраструктуру, а й можуть спричинити реальні фізичні загрози. Це відрізняє енергетичний сектор від багатьох інших галузей, де кіберінциденти зазвичай обмежуються втратами інформації або фінансів.

Особливу небезпеку становлять складні цілеспрямовані атаки, що використовують вразливості у промислових протоколах, системах авторизації та механізмах керування. Такі атаки можуть бути спрямовані на підміну даних, блокування доступу до систем, введення некоректних команд управління, порушення режимів роботи обладнання або об’єкти фізичної інфраструктури. У більшості випадків такі атаки побудовані за принципом багаторівневого проникнення та можуть тривалий час залишатися непоміченими, створюючи додаткові ризики.

Управління ризиками в цих умовах вимагає застосування сучасних інструментів кібербезпеки: механізмів виявлення загроз у реальному часі, аналізу поведінкових аномалій, побудови профілів активності, використання технологій глибокого пакувального аналізу, систем сегментації мережі та контролю доступу. Без застосування даних засобів забезпечити необхідний високий рівень кіберзахисту енергетичних компаній неможливо.

Ще одним ключовим елементом є кадровий фактор. У сучасній енергетиці більшість ризиків пов’язана з людськими помилками, які часто виникають через недосконаліть інтерфейсів систем, недостатній рівень підготовки персоналу або відсутність стандартизованих процедур. Персонал має працювати з великою кількістю цифрових інструментів, і некоректне використання навіть одного з них може призвести до великих ризиків. Складність сучасних систем потребує підвищення рівня цифрової грамотності працівників, регулярного навчання та впровадження механізмів мінімізації людського фактору.

У межах цифровізації виникає потреба у створені комплексних інтегрованих систем управління ризиками, що здатні забезпечити повний цикл управління починаючи від виявлення ризику до його оцінювання, аналізу, контролю та моніторингу. Розроблення таких систем є складним процесом, що передбачає використання сучасних інформаційних технологій, алгоритмів прогнозування, моделей машинного навчання, систем обробки великих даних, хмарних платформ та інструментів візуалізації.

Управління ризиками в енергетичній галузі не може розглядатися у відриві від загальної концепції функціональної безпеки. Функціональна безпека включає в себе широкий спектр питань, пов’язаних із забезпеченням надійності роботи систем управління, їх здатності адекватно реагувати на зовнішні та внутрішні впливи, підтримувати коректні режими роботи та уникати неконтрольованих відхилень. Однак, більшість сучасних енергетичних систем працює під управлінням складних програмно-апаратних комплексів, які реалізують логіку керування всіма технологічними процесами, виникає необхідність оцінювання стабільності та стійкості цих комплексів у різноманітних ситуаціях.

Інформаційні технології забезпечують інструменти для глибокого аналізу функціональної безпеки. За допомогою сучасних методів цифрового моделювання, таких як моделювання сценаріїв відмов, симуляція аварійних режимів, аналіз чутливості та оптимізація параметрів, можна отримати більш точне уявлення про поведінку системи у випадку реалізації певного ризику. У свою чергу, побудова цифрових двійників дозволяє відтворити фізичний стан обладнання у віртуальному

середовищі та моделювати його роботу з високою точністю, що є критично важливим для прогнозування можливих відмов і визначення оптимальних методів реагування.

Одним із ключових елементів сучасного цифрового ризик-менеджменту є використання інструментів прогнозної аналітики. Прогнозна аналітика дозволяє аналізувати історичні дані, визначати закономірності, виявляти приховані кореляції та будувати моделі, здатні прогнозувати ймовірність ризикових подій. Завдяки використанню алгоритмів машинного навчання стало можливим створювати адаптивні моделі, які самовдосконалюються на основі нових даних. У контексті енергетики такі моделі можуть застосовуватися для прогнозування навантажень, визначення оптимальних режимів роботи обладнання, прогнозування зносу та ймовірності відмов, оцінювання рівня напруги в мережах та виявлення можливих критичних ситуацій.

Суттєвою перевагою цифрових технологій є можливість переходу від реактивного до проактивного управління ризиками. Традиційні підходи передбачали реагування на події після їх настання, тоді як сучасні інформаційні інструменти дозволяють передбачити небажані ситуації до того, як вони перейдуть у фазу активності. Наприклад, аналіз даних може виявити тенденцію до перегріву трансформатора або появу ознак аномального навантаження, що дає можливість виконати профілактичні дії до настання аварії. У випадку кіберзагроз сучасні системи здатні виявляти аномальну поведінку в мережі ще до того, як відбудеться спроба проникнення чи саботажу.

Додатковою особливістю сучасного ризикового середовища в енергетиці є необхідність інтеграції різних інформаційних систем. Складність управління ризиками полягає в тому, що технологічні процеси, бізнес-процеси, інформаційні системи, аналітичні модулі та системи кібербезпеки часто функціонують автономно, створюючи інформаційні розриви. Без інтеграції цих систем неможливо забезпечити цілісне бачення ситуації. Наприклад, система SCADA містить інформацію про технологічні параметри, SOC/SIEM — про інформаційні загрози, ERP — про ресурси та персонал, а аналітичні модулі — про прогнозні

сценарії. Лише інтегрована цифрова платформа керує цими даними як цілісною системою і дозволяє формувати повний спектр ризиків.

Інтеграція інформаційних систем є важливим кроком до формування повноцінного централізованого ризик-менеджменту. З'єднання всіх джерел інформації в одному цифровому просторі дає можливість створити основу для побудови реєстру ризиків, їх автоматичного оцінювання по рівню пріоритетності та створенню рекомендацій. Крім того, інтегрована система дає змогу відстежувати зміни у ризиковому середовищі в режимі реального часу, оновлювати моделі ризиків та адаптувати стратегії управління відповідно до цих змін.

Важливим аспектом управління ризиками є також рівень автоматизації. У цифрових енергетичних системах автоматизація охоплює широкий спектр процесів починаючи від збору даних до формування управлінських команд. Автоматизовані алгоритми можуть перерозподіляти навантаження, запускати резервні лінії, змінювати режими генерації, активувати релейний захист та виконувати інші дії без участі оператора. Проте така автоматизація створює додаткові ризики, пов'язані з програмними збоями, неправильними налаштуваннями , помилками в алгоритмах або некоректного реагування на нестандартні ситуації. Саме тому важливо забезпечити багаторівневий контроль роботи таких систем і впроваджувати механізми дублювання та резервування.

Не менш важливою складовою сучасного управління ризиками є побудова моделей стійкості енергетичних систем. Сталість системи передбачає її здатність протистояти зовнішнім і внутрішнім факторам, швидко відновитись після відмов та функціонувати в умовах обмеженої доступності ресурсів. Створення таких моделей є можливим лише завдяки сучасним інформаційним технологіям. Методи математичного моделювання, симуляції відмов, аналізу мережевих структур, оцінювання критичних вузлів та аналізу чутливості дозволяють виявити вразливі місця системи та визначити оптимальні стратегії реагування.

Цифрові технології також відкривають можливості для переходу до концепції адаптивного управління ризиками. У такій системі ризики оцінюються та упорядковуються не лише на основі історичних даних, а й на основі поточних

змін у середовищі, поведінки системи та зовнішніх елементів. Система адаптивного управління здатна автоматично налаштовувати свої параметри, модифікувати алгоритми та змінювати стратегії реагування відповідно до змін умов, що дозволяє значно підвищити ефективність ризик-менеджменту.

Сучасні інформаційні технології стали ключовим фактором побудови інтелектуальних енергетичних систем, де ризики аналізуються у реальному часі, а рішення приймаються на основі комплексного аналізу даних. Застосування цифрових інструментів дозволяє не лише виявляти та оцінювати ризики, але й прогнозувати їх розвиток, мінімізувати негативні наслідки та забезпечувати стійкість енергетичної інфраструктури до фізичних, інформаційних та кібернетичних впливів. У таких умовах створення інтегрованих цифрових платформ управління ризиками є необхідною умовою розвитку сучасних енергетичних компаній, їх безпеки та ефективності роботи.

Таким чином, інформаційні технології відіграють ключову роль у формуванні, виявленні, аналізі та управлінні ризиками в енергетичному секторі. Вони забезпечують основу для побудови нових підходів до ризик-менеджменту, що базуються на цифровій інтеграції, автоматизації, штучному інтелекті, глибокій аналітиці та моделюванні. Ці технології дозволяють створювати сучасні інструменти оцінювання ризиків, формувати цілісну картину ризикового середовища, підвищувати точність та якість прогнозування та оптимізувати процеси прийняття рішень, що є критично важливим для забезпечення стійкості та надійності енергетичних систем у сучасних умовах.

1.2 Класифікація ризиків в енергетичному секторі в умовах цифрової трансформації

Енергетичний сектор у сучасних умовах функціонує як складна багаторівнева система, що об’єднує технологічні процеси, цифрову інфраструктуру, розгалужені комунікаційні мережі, автоматизовані системи диспетчерського управління та інтелектуальні механізми аналізу і прогнозування. Через свою взаємозалежність та критичність до зовнішніх і внутрішніх впливів енергетика формує унікальне ризикове середовище, у якому традиційні категорії

ризиків переплітаються з новими типами загроз, пов’язаними з масштабною цифровізацією. Саме тому класифікація ризиків у цифрову епоху є не просто інструментом систематизації, а фундаментальною основою для створення сучасних систем ризик-менеджменту та цифрових платформ управління ризиками.

Цифрова трансформація енергетики призвела до того, що інформаційні технології стали ключовим елементом майже всіх процесів: від моніторингу режимів роботи обладнання до балансування навантаження, прогнозування попиту, управління ресурсами, кіберзахисту й аналітичної підтримки прийняття рішень. Однак одночасно з перевагами, ІТ-компоненти створили нові ризики, які суттєво розширюють традиційні класифікаційні моделі. Це вимагає комплексного підходу, у якому кожен ризик оцінюється не лише як самостійний елемент, але і як частина великої цифрової екосистеми.

Сучасне ризикове середовище енергетики можна охарактеризувати як глибоко інтегроване, де технічні, організаційні, природні, економічні та інформаційно-технологічні ризики взаємодіють між собою через дані, алгоритми, ІТ-системи та технологічну інфраструктуру. Наприклад, технічна відмова обладнання може бути спровокована цифровим збоєм, кіберінцидент може спровокувати помилкове спрацьовування релейного захисту, помилка алгоритму прогнозування здатна створити небезпечний режим роботи мережі, збій телеметрії може призвести до формування некоректних диспетчерських рішень.

У зазначених умовах класифікація ризиків відіграє ключову роль. Вона дозволяє структурувати ризикове середовище, визначити джерела небезпек, встановити потенційні ланцюги впливів та сформувати основу для подальшого побудування цифрової платформи управління ризиками. Варто також враховувати, що упродовж останніх десятиліть зазнав змін сам характер ризиків: вони стали більш динамічними, мережевими, взаємопов’язаними і такими, що виникають на межі взаємодії цифрових і фізичних систем.

Загальну класифікацію ризиків у сучасній енергетиці доцільно представляти у вигляді таких основних груп: технічні, технологічні, інформаційні, кібернетичні, організаційні, економічні, природні, алгоритмічні та інтеграційні ризики. Кожна з

даних груп має власні джерела, механізми впливу та потенційні наслідки, однак у цифрових умовах межі між ними стають умовними. Саме тому сучасна класифікація повинна бути розширеною, інтегрованою та адаптивною.

Таблиця 1.1. Систематизована класифікація ризиків

Група ризиків	**Опис**	**Приклади наслідків у цифровій енергетиці**
Технічні	Фізичні відмови обладнання	аварії трансформаторів, перевантаження ліній
Технологічні	Збої технологічних процесів	порушення частоти, помилки релейного захисту
Інформаційні	Втрата чи спотворення даних	некоректні покази SCADA, телеметричні збої
Кібернетичні	Атаки на IT-інфраструктуру	проникнення у SCADA, шкідливе ПЗ, DDoS
Організаційні	Людський фактор, регламенти	помилки диспетчера, хибні дії персоналу
Економічні	Фінансові наслідки ризиків	збитки від збоїв IT, ціна енергоносіїв
Природні	Стихійні явища	негода, коливання температур, буревії
Алгоритмічні (IT)	Помилки ПЗ і моделей	невірні ML-прогнози, збій алгоритмів
Інтеграційні	Конфлікти між системами	несумісність SCADA–ERP–EMS

Більшість ризиків у цифровій енергетиці мають подвійну природу: фізичну та цифрову. Це означає, що класифікаційних підхід не може обмежуватись класичними ортогональними розподілами на технічні й організаційні загрози. Навіть суто технічна подія сьогодні може виникнути або неправильною телеметрією, або помилками у системах автоматичного регулювання, або затримкою сигналів у цифровому каналі. Цифровий фактор є невід'ємною складовою кожного типу ризику.

Інформаційні ризики та ризики якості даних посідають особливе місце. Усі сучасні системи управління енергетикою — SCADA/EMS, релейний захист, системи прогнозування навантажень, інструменти оптимізації та машинного

навчання — працюють на основі даних, тобто їхня ефективність та якість прямо залежить від точності, синхронності, семантичної коректності та достовірності інформації. Якщо дані недостовірні або неповні, ризики автоматично зростають для всіх рівнів системи.

Таблиця 1.2. Вплив інформаційних технологій на групи ризиків

Група ризиків	Зниження ризику завдяки IT	Зростання ризику через IT
Технічні	діагностика, цифрові двійники	збій датчиків, спотворення даних
Технологічні	автоматизація та оптимізація	помилки алгоритмів
Інформаційні	системи очищення даних	вразливість каналів телеметрії
Кібернетичні	SOC/SIEM, сегментація	нові точки атаки (IoT, PLC)
Організаційні	цифрові інструкції	складність інтерфейсів
Алгоритмічні	точність ML-моделей	неправильне навчання

В епоху цифровізації ризики взаємодіють між собою у вигляді ланцюгових процесів. Ця здатність є однією з ключових для сучасної класифікації. Ризики більше не проявляються ізольовано: вони формуються як наслідок взаємодії цифрових сигналів, алгоритмів, механізмів автоматизації та фізичної інфраструктури. Невеликий цифровий збій може мати масштабні технічні наслідки. І навпаки — технічні відхилення можуть призвести до інформаційної дестабілізації або збою у цифрових платформах.

У сучасних умовах цифрової трансформації енергетичні компанії функціонують у середовищі постійних змін, де ризики проявляються у багатовимірній та взаємопов’язаній формі. Важливою характеристикою цього середовища є те, що навіть базові технічні ризики сьогодні значною мірою залежать від якості та достовірності цифрових даних, надійності алгоритмів, стійкості IT-інфраструктури та стабільності каналів комунікації. Це суттєво ускладнює завдання управління ризиками і вимагає переходу до нових класифікаційних підходів, які враховують інтегровану природу взаємодії технологічних і цифрових компонентів.

Цифрові системи, що забезпечують збір, обробку та передавання даних, фактично формують «нервову систему» сучасної енергетики. Будь-які збої в цих

системах мають потенціал трансформувати один вид ризику в інший, породжуючи ланцюговий ефект. Наприклад, втрата телеметрії або спотворення параметрів напруги може призвести до некоректного спрацьовування алгоритмів релейного захисту, що своєю чергою може згенерувати технічну аварію. Такий взаємозв'язок показує, що інформаційні ризики є не просто окремою категорією — вони є множником, який здатен посилювати або модифікувати всі інші види ризиків.

Окрему увагу привертають кібернетичні ризики, які в енергетичній галузі набувають особливо критичного значення. У сучасних автоматизованих системах SCADA, EMS, DCS і релейного захисту більша частина керування виконується за допомогою цифрових команд. Втручання у ці канали може призвести до помилкових команд, блокування критичних функцій або навмисного створення аварійних режимів. Кіберризики стають одним з фундаментальних елементів сучасної класифікації, оскільки вони здатні одночасно впливати на інформаційні, технологічні та технічні аспекти роботи енергосистеми.

Важливим компонентом ризикового середовища є алгоритмічні ризики, що пов'язані з використанням моделей штучного інтелекту та машинного навчання. Сучасні енергетичні компанії широко використовують моделі прогнозування споживання, оцінювання навантаження, визначення оптимальних режимів роботи обладнання та виявлення аномалій у поведінці мережі. Однак правильність результатів таких моделей повністю залежить від якості даних, правильності їх навчання та стабільності алгоритмів. Невірне навчання або використання неякісних тренувальних вибірок може призвести до систематичних помилок у прогнозах, що може призвести до реальних технічних ризиків. Таким чином, алгоритмічні ризики необхідно віднести до загальної класифікації як окрему категорію, що відображає специфіку сучасної енергетики.

Особливу важливість займають інтеграційні ризики, пов'язані з необхідністю з'єднання між собою різних апаратних та програмних платформ. Енергетичні компанії використовують широкий спектр систем починаючи від SCADA та телеметрії до ERP, CMMS, GIS, DMS і хмарних платформ аналітики. Однак кожна система має власні протоколи, формати даних, вимоги до синхронізації та логіку

роботи. Помилки у процесах інтеграції можуть проявлятися у вигляді конфліктів даних, дублювання інформації, втрати цілісності параметрів або неправильного трактування показників. Подібні збої можуть призвести до великих наслідків, деколи неконтрольованого характеру, оскільки вони впливають на всю інфраструктуру прийняття рішень та управління режимами.

Не менш вагомими залишаються організаційні ризики, які у цифровій енергетиці набувають нових форм. Людський фактор проявляється не лише в традиційних помилках експлуатації, а й у неправильному використанні цифрових інструментів. Неправильне налаштування систем, некоректне введення параметрів, ігнорування процедур безпеки, неправильне інтерпретування візуальних даних усе це створює нові різновиди організаційних ризиків. Проблеми можуть виникати також через неякісну підготовку персоналу, складність інтерфейсів або перевантаженість інформаційних панелей.

Економічні ризики в умовах цифровізації також потребують нового трактування. Сьогодні фінансові втрати можуть бути зумовлені не лише технічними аваріями чи ринковими коливаннями, але й цифровими інцидентами. Наприклад, зупинка інформаційної системи може призвести до збоїв у логістиці, обліку, плануванні або управлінні персоналом. Кіберінциденти можуть призвести до значних витрат на відновлення, штрафів, втрати довіри споживачів або зниження стабільності енергопостачання.

У свою чергу, природні ризики в умовах цифрової трансформації мають подвійну природу. Вони впливають як на фізичну інфраструктуру, так і на цифрові компоненти. Наприклад, буревії чи повені можуть пошкодити не лише електромережу, але й вузли передачі даних, серверні приміщення або базові станції IoT-датчиків, які забезпечують телеметрію.

Цілісність і взаємозалежність усіх цих груп ризиків вимагають створення розширеної, інтегрованої класифікації, яка дозволяє врахувати всю повноту взаємодій між категоріями. У сучасній енергетиці неможливо окремо керувати технічними або цифровими ризиками — це складові єдиної системи які доповнюють один одного.

Крім того, значну роль відіграють ризики якості даних. Оскільки всі сучасні системи управління енергетикою працюють на основі даних, наявність неповних, недостовірних, спотворених або затриманих сигналів може стати ключовою причиною помилкових рішень. Дані є основою для моделей прогнозування, систем балансування, алгоритмів захисту, оцінювання стану мережі, розрахунку оптимальних режимів та роботи диспетчерів. Тому інформаційні ризики в сучасній класифікації є крос-категорією, що впливає на всі інші види ризиків.

Таким чином, в сучасну класифікацію ризиків повинно враховуватись багатовимірність, взаємозалежність та цифрові компоненти кожного виду ризику, а не лише традиційний технічний або організаційний характер загроз. Системний підхід до класифікації є ключовим для подальшого створення цифрової платформи управління ризиками.

У сучасній енергетиці важливо враховувати не лише прямий вплив того чи іншого ризику, але й можливість їхнього каскадного поширення. Системи енергетики є настільки взаємозалежними, що навіть незначне відхилення на одному рівні може створити хвилю небажаних наслідків на іншому.

Такі взаємодії демонструють важливість підходу до класифікації, який враховує не лише природу ризику, але й механізми його трансформації. У цифровій енергетиці ризики майже не проявляються у чистому вигляді. Найчастіше вони набувають змішаного характеру — наприклад, техніко-інформаційного, організаційно-алгоритмічного або кібернетично-технологічного. Це змушує розширювати межі класичних класифікацій і формувати нові, інтегровані групи ризиків.

Варто зазначити, що цифрова трансформація створює не лише нові типи ризиків, але й нові способи їхнього виявлення та мінімізації. Цифрові двійники дають можливість прогнозувати поведінку обладнання за різних режимів роботи, аналітичні моделі дозволяють визначати потенційні точки відмови, а системи раннього виявлення аномалій формують можливість оперативного реагування до настання критичної ситуації. Проте це ще раз підкреслює, що сучасні системи

управління ризиками більше не можуть існувати без інтеграції IT-технологій, і ця інтеграція сама створює новий клас залежностей.

Удосконалена класифікація ризиків допомагає виявляти «вузли вразливості», у яких найбільше перетинаються цифрові й фізичні фактори впливу. Такі вузли часто включають:

— системи релейного захисту та автоматики;

— SCADA та телеметрію;

— моделі прогнозування та оптимізації;

— канали міжсистемної інтеграції;

— цифрові інтерфейси операторів;

— серверні вузли, що зберігають критичні дані;

— IoT-пристрої та смарт-сенсори.

У різних елементах енергетичної інфраструктури одночасно можуть проявлятися кілька категорій ризиків, що робить ці вузли критичними для побудови системи управління ризиками. Усвідомлення цього дозволяє правильно визначати пріоритети, обирати відповідні захисні механізми та прогнозувати потенційні відмови.

Технічні ризики цифрової енергетики часто пов’язані з якістю даних та стабільністю цифрових каналів. Наприклад, системи автоматичного керування навантаженням є чутливими до затримки у передачі сигналів. До алгоритмічних ризиків належать помилки у прогнозних моделях, коли інтелектуальна система формує неправильні управлінські рішення через неточні дані або некоректну поведінку ML-моделі.

Організаційні ризики також залишаються ключовими, оскільки робота з цифровою інфраструктурою потребує високої кваліфікації персоналу. Інженери та диспетчери повинні оперативно інтерпретувати цифрові панелі, графіки, аналітичні модулі й діяти відповідно до сучасних політик інформаційної безпеки. Людський фактор стає критичним у середовищі, де автоматизовані системи здатні виконувати важливі операції без прямого втручання оператора.

Інтеграційні ризики виникають через необхідність взаємодії різнорідних

цифрових платформ, що використовують різні протоколи зв'язку, стандарти безпеки та моделі даних. У разі збою в інтеграції може бути порушена узгодженість інформації, що впливає на коректність прийняття рішень.

Усе це підкреслює необхідність інтегрованої класифікації ризиків, що враховує взаємозв'язок технологічних, інформаційних, алгоритмічних, економічних та організаційних чинників. Така класифікація є основою для побудови цифрової платформи управління ризиками, оскільки дозволяє створити комплексну модель ризикового середовища, яка використовується в алгоритмах оцінювання, аналізу, прогнозування та формування рішень для раннього реагування.

1.3 Методи якісного та кількісного оцінювання ризиків в енергетичному секторі

Ефективне управління ризиками в енергетичному секторі ґрунтується на всебічному аналізі небезпек, що виникають на етапах генерації, передачі, розподілу та споживання електроенергії. Цифровізація значно ускладнила ризиковий ландшафт: окрім технічних і організаційних загроз, необхідно враховувати кіберризики, стабільність IT-інфраструктури, якість телеметрії, роботу алгоритмів та взаємодію цифрових і фізичних компонентів. Саме тому сучасні методи оцінювання ризиків повинні враховувати багатовимірний і динамічний характер цифрової енергетики.

Методи оцінювання ризиків поділяють на якісні та кількісні. Якісні методи застосовуються для первинної ідентифікації небезпек, створення структури ризикового середовища та встановлення пріоритетів. До найпоширеніших належать PHA, HAZOP, метод «What-if» та чек-листи. У цифровій енергетиці ці методи застосовують не лише для аналізу фізичних параметрів, а й для оцінки якості цифрових процесів, достовірності сигналів, затримок телеметрії, стабільності алгоритмів.

Кількісні методи дозволяють отримати числове значення ризику — ймовірність, індекс критичності або математичну модель сценарію. Найчастіше використовують FMEA/FMECA, Fault Tree Analysis (FTA), Event Tree Analysis

(ETA), симуляції Монте-Карло та методи статистичного аналізу. У цифровому середовищі ці методи доповнюються аналізом параметрів телеметрії, даних SCADA/EMS, логів кіберподій та результатів роботи алгоритмів ШІ.

Машинне навчання стало однією з важливих частин сучасного кількісного аналізу: ML-моделі застосовуються для виявлення аномалій, прогнозування відмов, оцінювання технічного стану обладнання, оптимізації режимів роботи мереж та прогнозування параметрів у часових рядах.

Окрему роль займає якість даних. Спотворення або затримки телеметрії можуть призвести до некоректних оцінок ризику, неправильної роботи FMEA або помилкових прогнозів ML-моделей. Тому оцінка ризиків тісно інтегрується з методами контролю якості даних та фільтрами аномалій.

Таблиця 1.3. Порівняння якісних і кількісних методів оцінювання ризиків

Група методів	**Приклади методів**	**Сильні сторони**	**Обмеження**
Якісні	HAZOP, PHA, чек-листи, What-if	Гнучкість, простота, експертність	Суб’єктивність, обмежена точність
Кількісні	FMEA/FMECA, FTA, ETA, Монте-Карло, регресійні моделі	Точність, можливість прогнозування	Складність, потреба у великих даних
Аналітичні (ML/AI)	Кластеризація, нейромережі, anomaly detection	Висока точність, самооновлення моделей	Залежність від якості даних

Сучасні платформи управління ризиками об’єднують в себе одразу декілька методів у цифровому модулі. Наприклад:

— PHA використовується для первинної ідентифікації небезпек,

— FMECA — для обчислення індексу критичності,

— FTA — для аналізу причинно-наслідкових зв’язків,

— ML-алгоритми — для прогнозування відмов у реальному часі.

Завдяки цифровізації оцінювання ризиків переходить від періодичного ручного аналізу до безперервного моніторингу, що забезпечує своєчасне реагування та стійкість енергосистеми до технічних і кібернетичних загроз.

Таким чином, поєднання якісних і кількісних методів створює комплексну основу для управління ризиками в умовах цифрової енергетики, забезпечує точніше прогнозування подій та підтримує прийняття обґрунтованих управлінських рішень.

1.4. Міжнародні стандарти управління ризиками та цифрові моделі безпеки

Управління ризиками в енергетиці неможливо розглядати поза контекстом міжнародних стандартів, які формують методологічну основу забезпечення стабільності, безпеки та надійності критичної інфраструктури. В умовах цифровізації вони забезпечують уніфікований підхід до побудови систем ризик-менеджменту, узгоджують взаємодію між фізичними та цифровими компонентами енергосистем, визначають вимоги до інформаційної безпеки, кіберзахисту та операційної стійкості. Стандартизовані моделі дозволяють зберігати керованість складної архітектури ризиків, що формується на перетині технологічних, інформаційних та організаційних процесів.

Міжнародні стандарти управління ризиками охоплюють як загальні методології, так і спеціалізовані документи для енергетики. До ключових належать ISO 31000, серії ISO/IEC 27000, ISO 55000, ISO 22301, IEC 62443, ISO 27019, а також рекомендації NIST та документи ENTSO-E. Разом вони створюють рамки для побудови сучасних систем ризик-менеджменту, які враховують як технічні, так і кібернетичні аспекти функціонування енергетичних систем.

Таблиця 1.4. Основні міжнародні стандарти управління ризиками

Стандарт	**Призначення**	**Ключові елементи**	**Застосування в енергетиці**
ISO 31000	Загальна методологія ризик-менеджменту	Принципи, рамкова модель	Політика ризиків, інтеграція в процеси
ISO/IEC 27001/27005/27019	Кібербезпека	Контролі, аналіз ризиків	Захист SCADA/EMS, телеметрії
IEC 62443	Промислова кібербезпека	Сегментація, рівні безпеки	Захист PLC, підстанцій, OT

Стандарт	Призначення	Ключові елементи	Застосування в енергетиці
ISO 55000	Управління активами	Життєвий цикл обладнання	Техстан, ремонти, критичність
ISO 22301	Безперервність бізнесу	План відновлення	Реагування на аварії й інциденти
NIST CSF / SP 800-82	Кіберзахист та ICS	Ідентифікація, реагування	SOC/SIEM, операційна стійкість
ENTSO-E	Європейські вимоги	Дані, синхронізація	TSO/DSO сумісність

Стандарт ISO 31000 «Risk Management — Principles and Guidelines» визначає принципи, підходи й етапи управління ризиками, формує основу корпоративної політики ризик-менеджменту, наголошує на необхідності інтеграції процесу управління ризиками в усі бізнес-процеси. Для енергетики це критично, оскільки ризики технологічних систем тісно пов’язані з диспетчерським керуванням, експлуатацією обладнання, плануванням ремонтів і інформаційною безпекою.

Серія ISO/IEC 27000 визначає основні аспекти інформаційної безпеки, керування доступом, захисту даних, безперервності IT-сервісів та кіберстійкості. Для енергетичних компаній, що залежать від цифрових каналів управління і телеметрії, дотримання ISO/IEC 27001, 27005 та спеціалізованого ISO 27019 є стандартизованою умовою безпечної експлуатації систем SCADA, EMS, DCS та інших комплексів автоматизації. ISO 27019, орієнтований саме на підприємства в сфері енергетики, деталізує вимоги до захисту інформаційних потоків, каналів зв’язку й команд керування.

Серія IEC 62443 встановлює вимоги до кібербезпеки промислових систем управління (Industrial Automation and Control Systems). Вона охоплює вимоги до виробників обладнання, інтеграторів та операторів і є критично важливою для енергетики, де використовуються промислові протоколи (Modbus, DNP3, IEC 60870-5-104), які історично не розроблялися з урахуванням кіберзагроз. Ці стандарти визначають принципи сегментації мереж, захисту контролерів, управління уразливостями та виявлення вторгнень.

Значну роль займає також NIST Cybersecurity Framework, який пропонує еталонну модель організації кібербезпеки за циклами ідентифікації активів, захисту, виявлення інцидентів, реагування та відновлення. У країнах, де енергетика є об’єктом високої уваги регуляторів, рекомендації NIST та спеціалізований документ NIST SP 800-82 щодо захисту промислових систем управління використовуються як основа для формування політик кіберзахисту, сегментації мереж та організації моніторингу.

Стандарти ISO 55000 зосереджені на керуванні активами протягом життєвого циклу, що для енергетики напряму пов’язано з надійністю обладнання та плануванням його заміни чи ремонту. Інтеграція цих підходів із цифровими платформами управління ризиками дозволяє поєднувати оцінювання технічного стану, аналіз ризиків та ремонтні стратегії в єдиній системі. Серія ISO 22301, яка регламентує управління безперервністю бізнес-процесів, створює основу для побудови системи реагування на аварії, кіберінциденти та інші деструктивні події, що для сфери енергетики є питанням національної безпеки.

У цифровому середовищі ключову роль займають стандарти ISO/IEC 20000 щодо управління IT-послугами, оскільки енергетичні компанії дедалі більше функціонують як IT-орієнтовані організації, а стабільність цифрових сервісів безпосередньо впливає на надійність інфраструктури в сфері енергетики. Стандарт IEC 61508, присвячений безпеці електронних і програмованих систем, задає вимоги до безпечного виконання функцій автоматики та релейного захисту навіть у разі часткових відмов, що безпосередньо стосується сучасних енергетичних об’єктів.

Управління ризиками в цифровій енергетиці опирається не лише на текстові стандарти, а й на цифрові моделі безпеки, які реалізують їхні вимоги у вигляді алгоритмів, правил та структур даних, інтегрованих у програмні платформи. Такі моделі включають опис загроз, вразливостей, сценаріїв порушення роботи, поведінки системи під час інцидентів, прогнозування аварій на основі методів машинного навчання, оцінки стійкості інфраструктури та ефективності заходів реагування.

На практиці це означає:

— ISO 31000 може реалізовуватись у модулі оцінювання ризиків,

— IEC 62443 — у модулі керування мережевою безпекою,

— ISO 27001 — у модулі політик безпеки та аудиту,

— ISO 22301 — у модулі безперервності бізнес-процесів,

— NIST CSF — у модулі моніторингу та реагування на інциденти.

Однією з ключових тенденцій розвитку стандартів є їх орієнтація на цифрову стійкість, тобто здатність системи адаптуватися до непередбачуваних загроз, підтримувати безперервність функціонування та швидко відновлюватися після інцидентів. Сучасні редакції ISO 31000, ISO/IEC 270xx, IEC 62443 та рекомендації NIST уже враховують потреби інтеграції IT- і OT-середовищ, постійного моніторингу, застосування прогнозних моделей та адаптивного реагування. Цифрові платформи управління ризиками, які використовують ці стандарти як методологічну основу, трансформують управління ризиками з реактивного у проактивне, дозволяючи не лише зафіксувати наслідки, а й спрогнозувати розвиток подій та завчасно впровадити захисні заходи.

Таким чином, міжнародні стандарти з управління ризиками та цифрові моделі безпеки слугують фундаментом сучасного ризик-менеджменту в енергетичній сфері. Вони забезпечують структуровану методологічну базу, дозволяють уніфікувати процедури і підходи, інтегрувати фізичні, кібернетичні та інформаційні компоненти в єдину систему управління ризиками та створюють передумови для організації стійких, захищених і ефективних енергетичних систем у цифровому середовищі.

1.5 Роль цифровізації та IT-інфраструктури у формуванні ризикового середовища енергетики

Цифровізація сектору енергетики стала визначальним чинником, який формує сучасний характер ризикового середовища. Інтеграція систем SCADA/EMS, розгалужених телеметричних каналів, мереж інтелектуальних сенсорів, цифрових двійників, хмарних обчислень та комплексів кіберзахисту

перетворила енергетичну інфраструктуру на багаторівневу кіберфізичну систему. У ній інформаційні й технологічні процеси настільки взаємозалежні, що будь-яке порушення в цифровому контурі практично миттєво відображається на роботі фізичної мережі. Це кардинально змінює принципи ідентифікації ризиків, методи їх оцінювання та підходи до управління ними.

Сучасна IT-екосистема енергетичних компаній являє собою складну архітектуру з безліччю апаратних і програмних компонентів, мережевих каналів та алгоритмічних модулів. Дані, які отримуються із об'єктів генерації, підстанцій, сенсорних систем та комунікаційних вузлів, фактично безперервно передаються в центри диспетчерського керування. У режимі реального часу вони аналізуються, агрегуються та використовуються для прийняття оперативних рішень. За таких умов достовірність, цілісність і своєчасність даних перетворюються на критичні параметри безпеки, однак найменше спотворення чи затримка можуть активувати неправильний алгоритм або спричинити некоректний режим роботи обладнання.

Поглиблення цифровізації істотно збільшує залежність енергетики від програмної логіки, конфігурацій мережевого обладнання, стабільності каналів зв'язку та якості телеметрії. Технічні ризики вже не обмежуються класичними механічними чи електричними відмовами. У сучасних умовах вони охоплюють дефекти програмного коду, помилки під час оновлення програмного забезпечення, порушення в роботі цифрових каналів або експлуатацію вразливостей промислових протоколів керування. Наприклад, такі протоколи як IEC 60870-5-104 чи DNP3 не створювалися з урахуванням сучасних сценаріїв кіберзагроз, тому залишаються чутливими до маніпуляцій трафіком або перехоплення команд.

Зі збільшенням кількості цифрових компонентів стрімко розширюється і кількість точок доступу до інфраструктури. Хмарні середовища, мобільні інтерфейси, платформи ринкової взаємодії, сервіси аналітики та віддалені робочі місця створюють нові вектори можливих атак. Будь-який збій оновлення, нестабільність серверного обладнання або порушення роботи одного модуля може спричинити ланцюгові ефекти, які поширюються на весь технологічний контур.

Велика кількість сучасних цифрових рішень базуються на алгоритмах машинного навчання, які використовують у прогнозуванні аварійності, оптимізації режимів навантаження, оцінюванні технічного стану обладнання та виявленні аномалій. Однак ці алгоритми створюють новий клас ризиків — алгоритмічних. Вони нерідко мають латентний характер, тобто похибки поступово накопичуються й стають помітними лише в критичний момент. Якщо модель навчена на викривленій або неповній вибірці, її прогнози можуть систематично відхилятися від реальності, формуючи приховану загрозу для стабільності енергетичної системи.

Цифровізація також трансформує роль персоналу. Працівники мають одночасно володіти інженерними компетенціями та розуміти принципи функціонування цифрових платформ, кіберзахисних механізмів і алгоритмічних моделей. Невірна інтерпретація інформації, неправильне реагування на автоматичні сигнали або недостатній рівень цифрової грамотності можуть спричинити ризики, яких не існувало в традиційних технологічних системах.

В умовах цифрової залежності кіберзагрози стають одним із ключових елементів ризикового середовища. На відміну від корпоративних IT-систем, атаки на енергетичну інфраструктуру можуть мати фізичні наслідки: порушення режимів роботи мережі, виведення з ладу підстанцій, некоректну роботу релейного захисту або примусові перемикання технологічних ліній. Через це сучасні підходи до захисту охоплюють сегментацію мереж, розмежування IT/OT-доменів, використання багаторівневих механізмів автентифікації та постійний аудит аномальних подій.

Таким чином, можна зробити висновок, що цифровізація створює нову, складну й багатовимірну архітектуру ризиків, у якій технологічні, інформаційні, алгоритмічні та організаційні аспекти взаємодіють у тісному зв’язку. Ефективна система керування ризиками в такому середовищі вимагає поєднання інженерних методів, інструментів кіберзахисту, технологій великих даних, систем аналітичного моніторингу та прогнозних моделей. Лише інтеграція цих елементів забезпечить цифрову стійкість енергетичної інфраструктури та здатність реагувати на динамічні виклики сучасної енергетичної сфери.

РОЗДІЛ 2 АНАЛІЗ СУЧАСНИХ ІТ-СИСТЕМ ТА ЦИФРОВИХ ПІДХОДІВ ДО УПРАВЛІННЯ РИЗИКАМИ В ЕНЕРГЕТИЦІ

2.1 Інформаційні системи та ІТ-рішення в енергетичних компаніях

Інформаційні системи стали ключовим елементом функціонування сучасних енергетичних підприємств, оскільки саме вони забезпечують цілісний цикл управління технологічними, операційними, бізнесовими та аналітичними процесами. Цифровізація енергетики перетворила традиційно технічну сферу на високоінформаційну сферу, де якість даних, швидкість обробки інформації та стійкість цифрової інфраструктури організовують стабільність усієї енергетичної системи. ІТ-рішення перестали займати роль допоміжних інструментів вони стали невід'ємним фундаментом операційної моделі компаній та платформою для впровадження інновацій.

На даний час системи в енергетиці мають багаторівневу архітектуру. На технологічному рівні працюють системи керування обладнанням, телеметричні вузли, сенсори й контролери, які організовують збір параметрів у реальному часі. Операційний рівень включає диспетчерські платформи SCADA та системи оперативно-технологічного управління, що відповідають за контроль режимів роботи мережі. На корпоративному рівні функціонують системи планування ресурсів, управління персоналом, технічного обслуговування та документообігу. Аналітичний рівень формує модулі прогнозування, обробки великих даних і машинного навчання. Об’єднані в єдине інформаційне середовище, ці рівні створюють цифрову екосистему, яка координує роботу всіх підрозділів підприємства.

Інтеграція цифрових платформ забезпечує значне скорочення інформаційних розривів між службами. Завдяки об’єднанню даних у єдиному середовищі компанія отримує можливість синхронно контролювати технічний стан обладнання, оперативні процеси, фінансову діяльність та стратегічні показники у реальному часі. Це підвищує якість та правильність управлінських рішень, дозволяє

оптимізувати виробничі процеси та створює умови для впровадження передових практик прогнозного управління.

Поширення інтелектуальних сенсорів та IoT-пристроїв значно збільшило об’єм інформації, яку отримує підприємство. На відміну від традиційних систем, що мали обмежений набір параметрів, сучасні пристрої передають сотні показників для кожного вузла мережі. Це створює можливості для глибшої аналітики, але водночас посилює залежність від якості цифрових даних.

Кіберфізичний характер енергетичної інфраструктури означає, що інформаційні системи та фізичні компоненти працюють як єдине ціле. Алгоритми, що керують роботою обладнання, ґрунтуються на даних, які надходять із цифрових каналів. Тому збій у програмному забезпеченні, затримка сигналу або порушення кібербезпеки можуть спричинити матеріальні наслідки починаючи від несправності обладнання до аварійних ситуацій у мережі. Це робить цифрову безпеку ключовим напрямом управління ризиками.

Зростання складності IT-інфраструктури створює потребу в розвитку механізмів її контролю. Сучасні компанії в сфері енергетики впроваджують централізовані системи моніторингу обладнання, серверів, мережевих каналів і програмних модулів. Такі системи дають можливість оперативно виявляти помилки, реагувати на відхилення, оцінювати статус усіх компонентів у режимі реального часу та запобігати каскадним збоям.

Великого значення набуває інтеграція машинного навчання в управлінські та технологічні процеси. Алгоритми здатні аналізувати історичні й поточні дані, виявляти закономірності, розпізнавати нетипові ситуації, прогнозувати поведінку обладнання та формувати рекомендації. Це сприяє переходу від реактивного управління до проактивного, де підприємство не лише реагує, а й передбачає їх виникнення інцидентів.

Важливим введенням є використання цифрових двійників, що відтворюють технічні процеси, обладнання та мережі віртуально. Завдяки цьому енергетичні компанії можуть тестувати режими роботи, оцінювати вплив можливих відхилень, прогнозувати поведінку системи та приймати рішення на основі симуляцій.

Цифрові двійники дозволяють виконати аналіз без ризику для реальної інфраструктури та мінімізують витрати на експериментальні дослідження.

Керування інформаційними системами вимагає також узгодженої взаємодії між різними підрозділами підприємства. Дані, що надходять з технологічних систем, активно використовуються фінансовими, аналітичними та управлінськими підрозділами. Це забезпечує комплексний підхід до планування операцій, виявлення ризиків, формування ремонтних програм та оптимізації витрат.

Сучасна цифрова інфраструктура повинна залишатися стійкою за будь-яких умов. Стійкі до відмов архітектури, кластеризація сервісів, резервування каналів, дублювання критичних модулів це необхідні елементи, що забезпечують безперервність роботи підприємств. В енергетиці, де навіть короткочасний збій може мати значні наслідки, такі заходи є невід'ємними.

Таким чином, можна сформувати висновок, що розвиток інформаційних систем є центральним чинником цифровізації енергетичного сектору. Вони дозволяють відтворити умови для максимально точної аналітики, підвищеної автоматизації, мінімізації людського фактору та впровадження інтелектуальних механізмів управління. Сучасні IT-рішення формують модель функціонування енергетичних компаній це модель, у якій ефективність, безпека та стійкість залежать від рівню цифровізації та здатністю систем до адаптації в режимі реального часу.

2.2 SCADA/EMS як ядро цифрового управління технологічними процесами

Системи SCADA (Supervisory Control and Data Acquisition) та EMS (Energy Management System) являють собою ядро цифрової інфраструктури сучасних енергетичних компаній. У сукупності вони здійснюють безперервний моніторинг стану енергосистеми, оперативне керування технологічними процесами, оптимізацію режимів роботи мережі та підтримку процесів прийняття рішень у штатних і аварійних ситуаціях. Саме SCADA/EMS забезпечують перехід від стандартних підходів до управління, що ґрунтувалися переважно на досвіді персоналу та обмеженій кількості даних, до високотехнологічної моделі керування,

побудованої на багаторівневій цифровій аналітиці, використанні математичних моделей і прогнозуванні.

У структурі цифрового керування енергосистемою SCADA займає роль системи оперативного контролю та збору даних. Вона приймає телеметричну інформацію від тисяч польових пристроїв, серед яких трансформаторні підстанції, вимикачі, лінії електропередачі, генератори, релейний захист, інтелектуальні датчики напруги й струму. Ці дані надходять у режимі, наближеному до реального часу, і відображають фактичний стан енергетичної системи. Опираючись на інформацію SCADA диспетчери бачать поточні режими, напруги, струми, конфігурацію мережі, стан комутаційної апаратури та інші параметри, від яких залежить стабільність роботи системи.

Над SCADA функціонує EMS як аналітична та оптимізаційна надбудова, що оперує комплексними даними, моделями режимів і сценаріями розвитку подій. Якщо SCADA забезпечує «сенсорне сприйняття» стану енергосистеми, то EMS перетворює потоки даних на управлінські рішення:

— здійснює розрахунки потокорозподілу,

— аналізує стійкість системи,

— моделює аварійні ситуації,

— прогнозує навантаження,

— визначає оптимальні режими генерації та розподілу потужності.

У сучасних енергетичних компаніях EMS фактично виступає «мозковим центром» цифрового управління, тоді як SCADA забезпечує надійний «сенсорний контур» та оперативний зворотний зв’язок.

На рисунку 2.1 відображено, як дані послідовно піднімаються від первинних вимірювань до диспетчерського рівня, тоді як керуючі впливи рухаються у зворотному напрямку. Така архітектура організовує цикл спостереження й керування, у межах якого SCADA виступає інтеграційною ланкою між фізичною інфраструктурою та цифровими алгоритмами EMS.

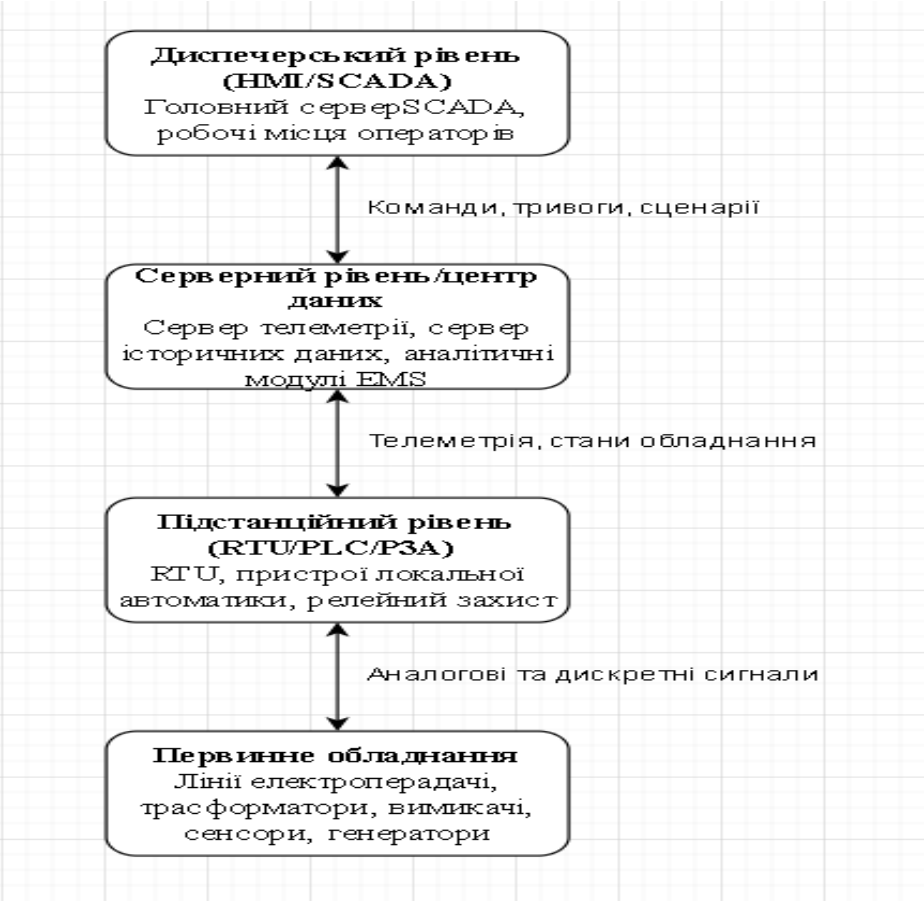


Рисунок 2.1. Структурна схема SCADA-системи

Тісний зв'язок між SCADA та EMS особливо помітний у задачах підтримання енергетичного балансу. Основним принципом є забезпечення відповідності сумарної генерації сумі навантаження та втрат у мережі. У загальному вигляді це можна записати у вигляді формули:

$$\sum P_{\text{ген}} = \sum P_{\text{навантаження}} + \sum P_{\text{втрати}}.$$

Порушення даної формули призводить до зміни частоти в енергосистемі. Зв'язок між зміною потужності та відхиленням частоти в спрощеній формі описується співвідношенням:

$$\Delta f = \frac{\Delta P}{2H},$$

де Δf– відхилення частоти, ΔP– зміна потужності, а H– узагальнений коефіцієнт інерції енергосистеми. EMS використовує ці співвідношення під час аналізу динамічної стійкості та розрахунку режимів реагування на аварійні ситуації.

Вагомою складовою функціонування EMS є розв'язання задач оптимального розподілу навантаження між джерелами генерації. Типова постановка передбачає мінімізацію сумарних витрат на генерацію за умови забезпечення балансу потужності та дотримання технічних обмежень. Загальний вигляд такої задачі можна подати формулами:

$$\min \sum_{i=1}^{n} C_i(P_i),$$

за умов

$$\sum_{i=1}^{n} P_i = P_{\text{попит}} + P_{\text{втрати}},$$

$$P_i^{\min} \le P_i \le P_i^{\max},$$

де $C_i(P_i)$– функція вартості генерації для і-го джерела, P_i– потужність і-го генератора, $P_{\text{попит}}$– сумарне навантаження в системі, $P_{\text{втрати}}$– втрати потужності в мережі, а $P_i^{\min}$та $P_i^{\max}$– технічні обмеження для кожного джерела.

Використовуючи ці моделі, EMS формує рекомендації щодо оптимальних рівнів генерації, які потім реалізуються через команди, що передаються в SCADA.

На стороні мережевих режимів EMS застосовує математичні моделі потокорозподілу. У спрощеному вигляді потік активної потужності між двома вузлами системи можна описати рівнянням:

$$P_{ij} = \frac{U_i U_j}{X_{ij}} \sin(\delta_i - \delta_j),$$

де U_iта U_j– напруги у відповідних вузлах, X_{ij}– реактивний опір лінії між ними, а $\delta_i - \delta_j$– різниця фазових кутів. Застосовуючи цю формулу в масштабі всієї мережі, EMS оцінює завантаження ліній, виявляє потенційно перевантажені ділянки та визначає умови, через які порушення режиму може призвести до системних аварій.

Таблиця 2.1 – Порівняльна характеристика систем SCADA та EMS

Характеристика	**SCADA**	**EMS**
Основне призначення	Оперативний контроль і керування	Оптимізація режимів та аналітика
Тип даних	Поточні виміряні параметри	Моделі, прогнози, агреговані показники
Часова роздільна здатність	Мілісекунди – секунди	Секунди – хвилини
Рівень впливу	Локальні й оперативні рішення	Системні, стратегічні рішення
Зв’язок із ризиками	Виявлення відхилень та аварійних подій	Оцінка стійкості, сценарний аналіз, прогнозування

Виходячи з таблиці 2.1, SCADA та EMS виконують взаємодоповнюючі функції: перша відповідає за точне й оперативне відображення стану системи, друга – за глибоку аналітику та стратегічне керування, включно з управлінням ризиками.

Подальший розвиток SCADA/EMS відбувається в напрямку інтеграції з широкомасштабними системами моніторингу WAMS, що використовують синхронізовані вимірювальні пристрої PMU. Вони здійснюють високоточні вимірювання фазових кутів і частоти, синхронізовані в часі, що значно розширює можливості для аналізу динамічних процесів.

У логічному вигляді взаємодію SCADA, EMS та WAMS можна подати так:

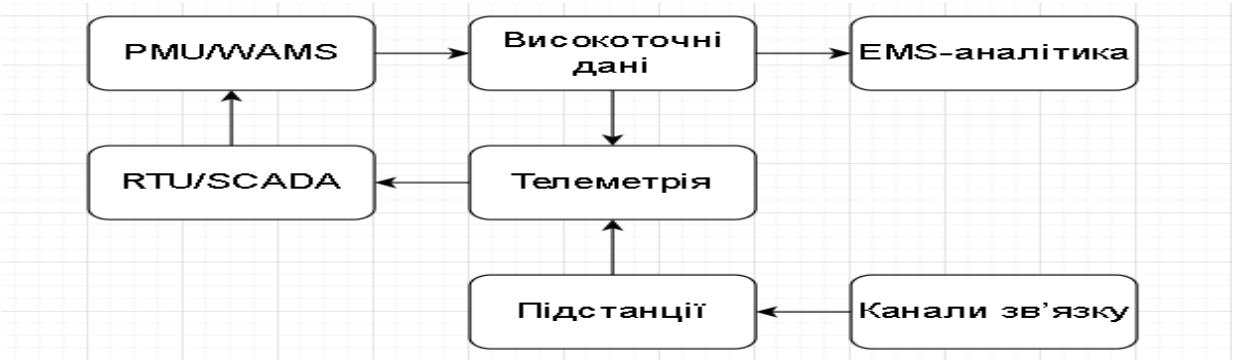


Рисунок 2.2 – Логічна взаємодія SCADA, EMS та WAMS

На рисунку 2.2 відображено, що WAMS доповнює традиційну SCADA високоточною інформацією, а EMS, об’єднуючи обидва джерела даних, здатна сформувати більш адекватні моделі поведінки системи, що важливо для управління ризиками в умовах динамічних змін.

Складність цифрової архітектури SCADA/EMS безпосередньо пов’язана з ризиками, які виникають на рівнях технічних компонентів, даних і алгоритмів.

Таблиця 2.2 – Основні джерела ризиків у середовищі SCADA/EMS

Джерело ризику	**Характеристика**	**Потенційні наслідки**
Телеметрія	Затримка, втрата, спотворення вимірювань	Хибні рішення, некоректні режими
Канали зв’язку	Збої, нестабільність, кібератаки	Втрата керованості, відсутність даних
Програмне забезпечення	Вразливості, помилки в алгоритмах	Несанкціонований доступ, помилкові команди
Людський фактор	Помилки операторів, некоректне втручання	Неправильні перемикання, посилення аварій
Моделі EMS	Невідповідність реальним умовам, спрощення	Некоректний аналіз стійкості та оптимізації

Таблиця 2.2 відображає, що ризики у SCADA/EMS мають комплексний характер і включають в себе технічні, інформаційні, алгоритмічні та організаційні аспекти. Це акцентує необхідність інтегрованого підходу до створення цифрових платформ управління ризиками, у центрі яких мають бути дані та функціонал SCADA/EMS.

Поступове ускладнення енергосистем, поява розподіленої генерації, активних мереж та відновлюваних джерел енергії додатково посилюють навантаження на SCADA/EMS, оскільки зростає обсяг даних та кількість сценаріїв, що потребують аналізу. У таких умовах роль SCADA/EMS виходить далеко за межі класичного диспетчерського управління мережою. Вони стають ключовою ланкою цифрової екосистеми енергетичного сектору, забезпечуючи не лише безперервний

контроль і керування, але й формуючи інформаційну основу для моделей ризиків, систем підтримки прийняття рішень, цифрових двійників і комплексної кібербезпеки.

2.3 Системи кіберзахисту (SOC/SIEM) та цифрова безпека енергетичної інфраструктури

Цифровізація енергетичного сектору, що включає впровадження SCADA/EMS, інтенсивне застосування телеметрії, IoT-пристроїв, інтелектуальних сенсорів та систем дистанційного керування, кардинально змінила спосіб функціонування енергетичної інфраструктури. Сфера перетворилася на складну багаторівневу кіберфізичну систему, у якій інформаційні технології безпосередньо впливають на поведінку та режими роботи обладнання. Саме це спричинило появу нового типу загроз, що мають як цифрові, так і матеріальні наслідки, а питання кіберзахисту стало одним з ключових для забезпечення стабільної роботи енергосистем.

Ключову роль у сучасній моделі цифрової безпеки займають системи SOC (Security Operations Center) та SIEM (Security Information and Event Management). SOC забезпечує цілодобовий моніторинг, аналіз та реагування на події безпеки в IT- та OT-середовищах, а також контролює аномалії, підозрілі операції та потенційні атаки. SIEM, у свою чергу, виконує функцію агрегації та кореляції подій, що надходять з різних компонентів інфраструктури — серверів, комунікаційного обладнання, автоматизованих систем керування, підстанцій та користувацьких станцій. Разом вони формують єдиний цикл роботи з інцидентами: від виявлення та оцінювання загрози до реагування та документування.

Особливість забезпечення кібербезпеки в енергетиці полягає в тому, що цифровий вплив може безпосередньо змінювати фізичний режим роботи обладнання. Некоректні дані у SCADA, спотворення сигналів телеметрії, маніпуляції з параметрами в EMS або втручання в логіку роботи контролерів можуть спричинити дисбаланс потужності, перевантаження мережі, відключення елементів системи або розвиток аварійних ситуацій. Тому SOC/SIEM орієнтовані

не лише на класичні IT-загрози, а й на сигнали, які свідчать про ненормальну поведінку процесів.

Умовно логіку взаємодії цих інструментів можна представити як послідовність. Первинні події надходять до SIEM, де вони фільтруються та зіставляються; підготовлені дані передаються до SOC, який визначає рівень критичності, контекст інциденту та необхідні дії.

Така модель забезпечує своєчасне виявлення цифрових та технологічних ризиків навіть у ситуаціях, коли загроза виникає одночасно в різних сегментах енергетичної інфраструктури, що значно підвищує її загальну стійкість.

Рисунок 2.3. Логічна структура SOC/SIEM у енергетичній компанії

З погляду математичного моделювання система SIEM використовує кореляційні механізми для визначення зв’язків між подіями. Це дозволяє виявляти складні атаки, у яких окремі події не виглядають підозрілими, але в сукупності утворюють чітку траєкторію зловмисної активності. Узагальнено такий зв’язок можна подати у вигляді коефіцієнта кореляції:

$$R_{xy} = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})^2}}.$$

На практиці SIEM застосовує складніші методи, у яких поєднуються статистичні моделі, евристичні правила, поведінкова аналітика та машинне навчання.

SOC аналізує контекст подій, визначає, чи є аномалія результатом кібератаки, технічної помилки або звичайного відхилення режиму. При необхідності SOC може застосувати автоматичне реагування, блокуючи доступ, ізолюючи сегмент мережі або обмежуючи виконання команд у SCADA.

Для комплексного уявлення про роль SOC та SIEM у забезпеченні цифрової безпеки енергетичної інфраструктури можна представити їхню функціональну взаємодію в узагальненій таблиці:

Таблиця 2.3. Функціональна роль SOC та SIEM в енергетичних компаніях

Параметр	SOC	SIEM
Характер взаємодії	Оперативна система безпеки	Центр збору та аналізу подій
Тип даних	Трафік, поведінкові патерни, OT-події	Логи, системні події, журнали доступу
Час реакції	Миттєве або швидке	Аналітичне, з затримкою кілька секунд
Основний результат	Виявлення інцидентів і реакція	Формування сигналів про події
Роль у SCADA/EMS	Захист каналів, команд та доступу	Виявлення підозрілих дій і аномалій

У сучасних енергетичних системах SOC і SIEM займають ключові позиції в протидії цифровим загрозам, зокрема атакам типу MITM, спробам перехоплення телеметрії, втручанню в параметри SCADA/EMS або спробам отримати несанкціонований контроль над підстанціями. Ефективність цих систем полягає у здатності фіксувати зміни у поведінці технологічного обладнання, відстежувати підозрілі команди та визначати нетипові дії навіть легітимних користувачів.

Завдяки використанню алгоритмів машинного навчання SOC може завчасно виявляти ознаки можливого інциденту, ще до того як він набуде небезпечної форми.

Таким чином, SOC та SIEM формують критично важливий елемент багаторівневого захисту цифрової енергетичної інфраструктури. Їх робота забезпечує своєчасне виявлення загроз, мінімізацію наслідків інцидентів, захист даних, що циркулюють у SCADA/EMS, а також підтримання стабільної роботи технологічних процесів навіть за умов цілеспрямованих атак.

З урахуванням того, що енергетичні системи постійно ускладнюються і стають більш залежними від цифрових елементів, значення SOC/SIEM неухильно зростає. У більшості компаній ці системи розглядаються не як допоміжні інструменти кіберзахисту, а як обов'язковий елемент технологічної безпеки. Складні, багаторівневі атаки, які поєднують кібернетичний вплив із маніпуляціями технологічними процесами, вимагають здатності оперативного аналізу контексту подій та блокувати небезпечні дії на різних рівнях всієї системи.

SOC і SIEM все частіше інтегруються зі спеціалізованими платформами аналізу телеметрії, що дає можливість поєднати інформаційні та технологічні показники. Такий підхід дає можливість виявляти складні взаємозв'язки між подіями, які відбуваються у різних частинах всієї енергетичної системи. Наприклад, SIEM може зафіксувати аномалію у корпоративній мережі, а SCADA — одночасно виявити нетипові зміни на підстанції. Разом ці сигнали вказують на скоординовану атаку, яка залишилася б прихованою при аналізі окремих сегментів.

Особливо важливим є контроль команд, що надходять до обладнання. Навіть одна команда, яка відповідає протоколу, але має нестандартне джерело або надходить у нетиповий момент, може спричинити критичний збій. У такому випадку SIEM ідентифікує аномалію, а SOC аналізує контекст інциденту, порівнюючи його з історією дій оператора, режимами та змінами роботи мережі за останні години.

За потреби система може автоматично обмежити доступ або заблокувати виконання небезпечної команди у SCADA.

У зв’язку з розширенням розподілених енергетичних ресурсів: СЕС, ВЕС, накопичувачів енергії, мікромереж, кількість вузлів і каналів взаємодії постійно зростає. SOC/SIEM дозволяють централізувати моніторинг, створюючи спільний інформаційний простір для всіх елементів системи, незалежно від їх місця розташування або типу технологічного обладнання.

Важливе місце займає поведінковий аналіз персоналу. Системи будують профіль типової активності для інженерів, диспетчерів та адміністраторів, після чого фіксують будь-які відхилення, а саме входи з незвичних локацій, невластиві послідовності команд, спроби зміни критичних параметрів. Це дозволяє виявляти як компрометацію облікових даних, так і свідомі порушення регламентів.

Ефективність SOC/SIEM залежить від повноти даних, які надходять у систему:

— логи доступу,

— журнали SCADA,

— телеметричні потоки,

— інформація про стан обладнання,

— мережевий трафік,

— історія оновлень програмно-технічних засобів.

Інтеграція цих джерел дозволяє не лише швидко реагувати на загрози, але й створити довгострокову аналітику, виявляти приховані патерни та формувати прогнозні моделі.

Сучасні атаки наразі є складними, малопомітними та довготривалими, тому SOC/SIEM все частіше доповнюються модулями машинного навчання. Моделі прогнозування та аномалій дозволяють виявляти «повільні» атаки, зміну структури трафіку, нетипові операції в рідко використовуваних сегментах, а також загрози без явних сигнатур.

2.4 Інтелектуальні датчики, IoT, телеметрія та цифрові двійники в енергетиці

Цифровізація сектору енергетики значною мірою пов’язана з розвитком інтелектуальних сенсорів, систем Інтернету речей (IoT), телеметричних платформ та технологій цифрових двійників. Ці інструменти забезпечують підвищену прозорість стану енергетичної інфраструктури, дозволяють змоделювати її поведінку та створюють нову якість керованості. Сучасні компанії все менше покладаються на періодичні ручні вимірювання або лише на класичні комплекси SCADA, адже цифрові сенсори та IoT-пристрої забезпечують безперервний потік даних у реальному часі, формуючи багаторівневий інформаційний простір для точного контролю й аналізу.

Інтелектуальні датчики відіграють ключову роль у контролі технічного стану обладнання. Вони здатні вимірювати критично важливі параметри — напругу, струм, температуру, вібрацію, навантаження, частоту, фазові кути, тиск тощо. Завдяки вбудованим модулям попередньої аналітики сенсори можуть відсіювати шум, виявляти аномалії та передавати до центральних систем лише релевантні значення. Це зменшує навантаження на канали зв’язку, підвищує точність оцінки й дозволяє оперативно реагувати на відхилення, що особливо важливо у системах, де зміни відбуваються в межах мілісекунд.

IoT-пристрої також займають особливе місце, оскільки поєднують сенсорні можливості з локальною обчислювальною логікою та можливість взаємодії між елементами системи. Вони використовуються для контролю стану підстанцій, моніторингу трансформаторів, управління мікромережами, координації роботи відновлюваних джерел енергії. На відміну від класичних телеметричних рішень, IoT забезпечує гнучку, адаптивну архітектуру, у якій кожний пристрій може автономно приймати рішення, підтримувати роботу в умовах часткових відмов і передавати інформацію безпосередньо іншим вузлам або центральним системам.

Одним із ключових напрямів застосування сенсорів та IoT у енергетиці є впровадження систем прогнозного обслуговування. Математична модель може бути описана у спрощеному вигляді як рівняння:

$$Y_t = \beta_0 + \beta_1 X_t + \beta_2 X_{t-1} + \ldots + \varepsilon_t,$$

де Y_tє показником імовірності відмови, X_t– набір параметрів обладнання, β– коефіцієнти впливу, а ε_t– випадкова складова.

Такі моделі використовуються для оцінювання стану трансформаторів, виявлення прискореної деградації ізоляції, контролю роботи ліній електропередачі та аналізу поведінки релейних пристроїв.

У сучасних комплексах дані від сенсорів та IoT-пристроїв передаються телеметричними каналами до локальних серверів або хмарних платформ обробки. Інформація надходить із високою частотою, іноді з мілісекундною роздільністю, що дає змогу системам SCADA та EMS працювати в quasi-реальному часі та оперативно реагувати на зміни режимів роботи. Така інтенсивність потоків даних потребує процедур попередньої обробки: фільтрації шумів, нормалізації значень, усунення пропусків, контролю аномалій та точного вирівнювання часових міток. Завдяки цьому телеметрія стає фундаментом для подальших аналітичних моделей і єдина основа, що гарантує коректність прогнозів та рішень.

Сучасні телеметричні рішення орієнтовані не лише на швидку передачу інформації, але й на безпеку каналів зв’язку. Критичні об’єкти використовують дубльовані маршрути та протоколи з низькою затримкою та захистом від зміни даних, оскільки маніпуляція телеметрією здатна призвести до некоректних дій EMS та створити ризики технологічних інцидентів.

Для узагальнення взаємодії сенсорів, IoT-пристроїв і телеметричних каналів у межах енергетичної системи доцільно відобразити їх у вигляді логічної структурної схеми:

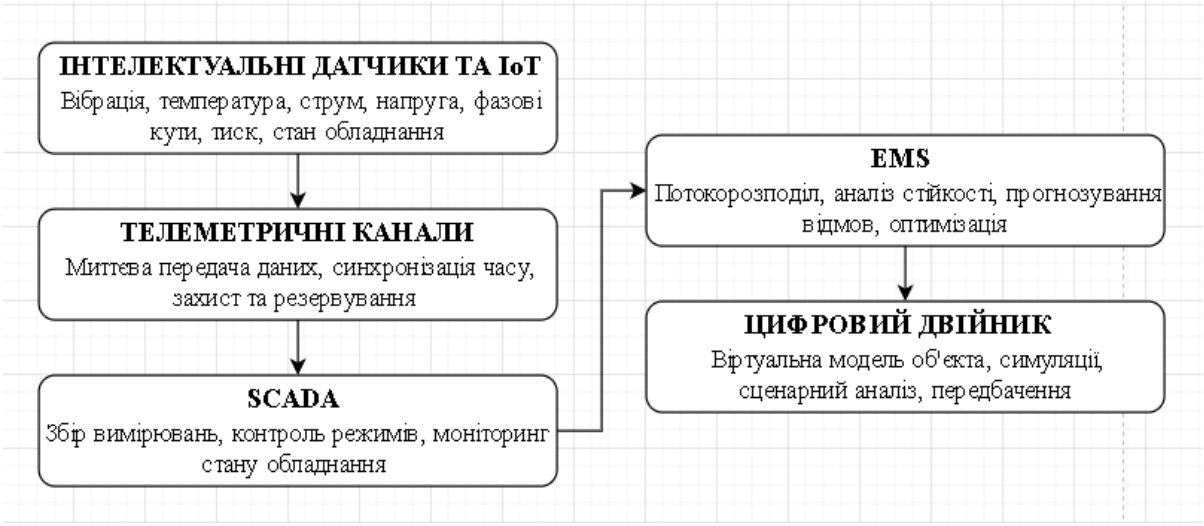


Рисунок 2.4. Логічна взаємодія сенсорів, IoT, телеметрії та SCADA/EMS

Рисунок 2.4. показує повну траєкторію руху інформації в цифровій енергосистемі починаючи від показників, які знімають сенсори та IoT-пристрої, до телеметричних каналів, систем SCADA й EMS, і далі до цифрового двійника, що створює динамічну віртуальну модель обладнання або енергетичного об’єкта.

Серед усіх елементів цифрової інфраструктури особливо важливими є цифрові двійники. Це детальні математичні моделі, які працюють синхронно з даними з реальної системи. Такий інструмент дозволяє безпечно проаналізувати поведінку обладнання, дослідити варіанти його роботи, оцінити наслідки можливих відмов та тестувати зміну режимів або конфігурації без будь-якого втручання в реальну інфраструктуру.

Завдяки доступу до великих обсягів телеметрії цифрові двійники здатні завчасно спрогнозувати зношення вузлів, виявляти аномальні стани та оцінювати, як змінюватимуться ключові параметри в різних експлуатаційних умовах. Це дає змогу підприємствам точніше планувати ремонті роботи, оптимізувати витрати та підвищувати надійність роботи технологічних об’єктів. У сфері управління ризиками цифровий двійник є одним із найрезультативніших інструментів, адже дозволяє перевіряти сценарії, які неможливо протестувати на реальному обладнанні.

Розвиток цифрових двійників тісно пов’язаний із методами машинного навчання. Алгоритми дозволяють моделювати поведінку системи в нетипових умовах, створювати тестові ситуації та шукати критичні точки, у яких обладнання

може працювати нестабільно. Інтеграція цифрових двійників із системами SCADA/EMS формує цілісну інтелектуальну екосистему, що поєднує прогнозування, аналіз та оперативне управління.

Для наочності ролі сенсорів і IoT-пристроїв у цифровій енергетиці наведено порівняльну таблицю їхніх функцій, можливостей та обмежень.

Таблиця 2.4. Порівняння класичних і інтелектуальних сенсорів

Параметр	Класичні сенсори	Інтелектуальні сенсори та IoT
Обробка даних	Лише вимірювання	Первинна аналітика, фільтрація
Частота оновлення	Низька	Висока (до мс)
Тип взаємодії	Одностороння	Двостороння з SCADA/EMS
Роль у моделюванні	Обмежена	Повна інтеграція у цифрові двійники
Захищеність	Стандартна	Криптографічний захист, резервування

У результаті інтелектуальні датчики, IoT-платформи, телеметричні канали та цифрові двійники формують основний технологічний фундамент цифрової енергетики. Їхнє поєднання забезпечує безперервне спостереження за роботою обладнання, дає змогу завчасно виявляти ознаки можливих відмов і точніше керувати режимами енергосистеми. Завдяки цим технологіям створюються детальні цифрові моделі, що підтримують сценарний аналіз та прогнозування. Сукупно ці інструменти зменшують рівень технічних і операційних ризиків, підвищують стійкість інфраструктури та сприяють переходу енергетики до адаптивних, високотехнологічних систем керування.

2.5 Технології збору, обробки та візуалізації даних (Big Data, BI, ML) в енергетиці

Активна цифровізація сфери енергетики та впровадження сенсорів, телеметричних пристроїв і розподілених джерел даних сформували нову ключову складову сучасного управління — Big Data. Здатність накопичувати й аналізувати великі обсяги інформації в реальному часі стала критично важливою для ефективності роботи енергетичних компаній. На відміну від традиційних систем з обмеженим набором параметрів, цифрова енергетика генерує безперервні

високошвидкісні потоки даних великої варіативності та обсягу. Це зумовлює необхідність застосування технологій Big Data, платформ бізнес-аналітики та алгоритмів машинного навчання.

Великі масиви даних формуються практично на всіх рівнях інфраструктури: від інтелектуальних сенсорів, IoT-пристроїв і "розумних" лічильників до SCADA, EMS, PMU, систем моніторингу, релейного захисту та кібербезпеки. Обсяг та різнорідність цих даних унеможливлюють їх обробку класичними підходами, тому компанії впроваджують системи потокової аналітики, здатні синхронізувати, очищати та інтерпретувати дані, а також визначати аномалії й будувати прогнозні моделі.

Робота з великими даними в енергетиці охоплює кілька ключових етапів. Першим є збір даних із різних телеметричних джерел починаючи від високочастотних вимірювань PMU до повільніших параметрів SCADA та історичних логів. На цьому етапі важливо забезпечити уніфікацію форматів, коректне узгодження часових міток та контроль якості, що створює основу для подальшої аналітики.

Наступним етапом є обробка даних, яка включає фільтрацію шуму, виявлення пропусків, валідацію, приведення до єдиного масштабу та очищення. Енергетичні підприємства часто використовують моделі згладжування, наприклад експоненціальне згладжування, яке можна описати формулою:

$$S_t = \alpha X_t + (1 - \alpha) S_{t-1},$$

де S_t— згладжене значення, X_t— фактичний параметр у момент часу t, а α— коефіцієнт згладжування.

Такі методи дають можливість уникати різких коливань у даних, які можуть бути спричинені шумами, перешкодами або інтерференцією.

Після очищення дані переходять до аналітичного шару, де використовуються моделі машинного навчання. В енергетиці машинне навчання застосовується для прогнозування навантаження, аналізу ймовірності відмов, визначення залишкового ресурсу обладнання, класифікації аварійних режимів, виявлення аномалій у поведінці мережі, побудови прогнозів виробітку відновлюваних джерел та оцінки

ризиків. Однією з найпоширеніших моделей є алгоритм регресії, який описується рівнянням:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_n X_n,$$

де Y— прогнозований параметр, $X_1 \ldots X_n$— змінні, що впливають на результат, а β— вагові коефіцієнти.

Використання таких моделей дозволяє виявляти залежності між параметрами, які неможливо визначити за допомогою класичних методів.

Важливим елементом роботи з великими даними є їхня візуалізація. Платформи бізнес-аналітики (BI) дають можливість перетворювати великі масиви числової інформації на зрозумілі графічні форми. Це значно полегшує аналіз даних і пришвидшує ухвалення рішень, особливо у середовищі, де параметри енергосистеми змінюються динамічно.

BI-рішення інтегруються з журналами подій, SCADA, EMS, телеметрією та цифровими двійниками, створюючи цілісну інформаційну панель для диспетчерів та інженерів. Така інтеграція дозволяє оперативно оцінювати стан мережі, контролювати навантаження, виявляти нестандартні режими та швидко визначати потенційні відхилення.

Узагальнена аналітична екосистема енергетичної компанії поєднує Big Data, BI та ML-алгоритми, утворюючи цілісний ланцюг від збору даних до їх інтелектуальної інтерпретації. Її структуру можна подати у вигляді умовної схеми.

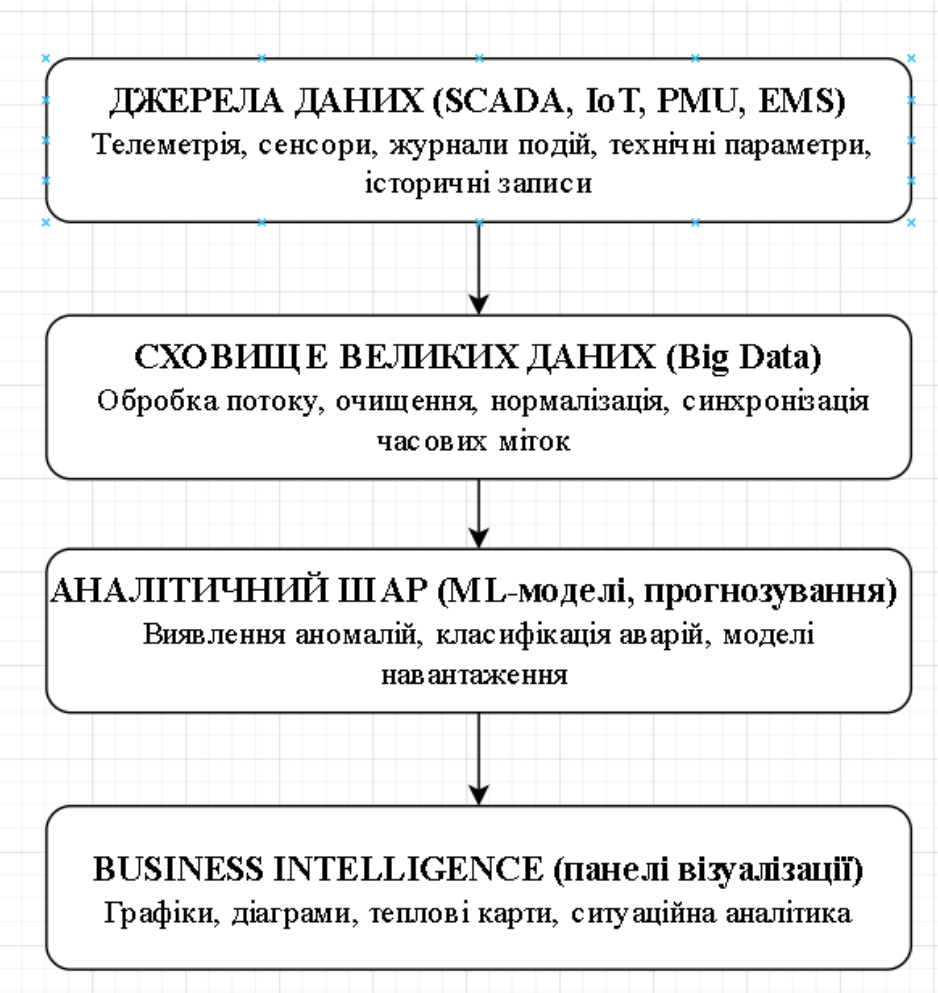


Рисунок 2.5. Узагальнена аналітична екосистема енергетичної компанії

Однією з основних переваг використання Big Data та алгоритмів машинного навчання є можливість виявляти приховані закономірності, непомітні за традиційного аналізу. Наприклад, телеметричні дані з ліній електропередач можуть містити неочевидні коливання напруги, які здаються випадковими. Але застосування методів кластеризації дає змогу відокремити повторювані події, пов’язані з певними режимами роботи або часовими інтервалами. Такі патерни часто сповіщають про зародження технічної проблеми або початок деградації обладнання, що дозволяє завчасно спрогнозувати можливі відмови.

Додаткову цінність має використання технологій потокового аналізу, які працюють з даними у режимі реального часу. Системи потокової обробки дозволяють фіксувати аномалії миттєво, ще до того, як вони виявляться в SCADA чи EMS. Завдяки цьому інженери можуть реагувати на критичні зміни практично

негайно, що підвищує стійкість енергосистеми й дозволяє уникнути масштабних інцидентів.

Нижче наведено узагальнене порівняння можливостей класичних методів обробки даних та сучасних технологій Big Data.

Таблиця 2.5. Порівняння традиційної аналітики та Big Data в енергетиці

Параметр	Традиційна аналітика	Big Data / ML
Обсяг даних	Обмежений	Масштабований, необмежений
Швидкість	Низька	Потокова обробка
Тип даних	Структуровані	Структуровані та неструктуровані
Можливість прогнозування	Обмежена	Висока
Адаптивність	Низька	Автоматичне навчання моделей

Технології Big Data, аналітичні платформи та алгоритми машинного навчання поступово стали основою для цифрової енергетики. Їх використання дозволяє не лише відстежувати поточний стан мережі з високою точністю, але й прогнозувати зміни режимів, аналізувати причини відхилень та формувати моделі, що описують поведінку обладнання у різних умовах. Такі підходи підсилюють можливості управління ризиками та підвищують стійкість енергетичної інфраструктури до технологічних і цифрових впливів.

Інтеграція потокової аналітики, інтелектуальних алгоритмів та сучасних засобів візуалізації забезпечує персонал якісним інформаційним базисом для ухвалення рішень. Завдяки цьому енергетичні компанії можуть швидко реагувати на відхилення, що виникають у кіберфізичних системах, ефективніше запобігати аваріям та забезпечувати стабільність роботи навіть у складних режимах експлуатації.

2.6 Недоліки існуючих систем і обґрунтування необхідності цифрової платформи управління ризиками

Незважаючи на суттєвий прогрес у цифровізації енергетичних підприємств, наявні SCADA, EMS, телеметричні комплекси, засоби кіберзахисту та аналітичні модулі залишаються роз’єднаними й не формують цілісної системи управління ризиками. Більшість цих рішень створювалася для виконання окремих виробничих

або інформаційних функцій, тому дані залишаються фрагментованими в межах технологічних сегментів. У результаті чого відсутній єдиний інформаційний простір, який міг би поєднати телеметрію, режими роботи обладнання, результати математичних моделей, журнали безпеки та історію подій у загальну ризико-орієнтовану архітектуру.

Сучасні системи працюють переважно у вертикальній логіці: SCADA керує локальними процесами, EMS аналізує режими, SOC/SIEM забезпечують кіберзахист, IoT збирає розподілені дані, а Big Data-платформи відповідають за аналітичну частину. За відсутності глибокої інтеграції між цими рівнями формується ефект «інформаційних островів», що ускладнює оперативну оцінку ризиків. Кожен елемент бачить лише власну частину системи, тому загальна картина стану інфраструктури залишається неповною.

Ще однією критичною проблемою є слабкий горизонтальний зв’язок між інформаційними потоками. Різна частота оновлення, неузгоджені часові мітки або розбіжності у форматах даних часто призводять до того, що телеметрія, моделі EMS та результати моніторингу обладнання не синхронізуються. Такі невідповідності суттєво ускладнюють аналіз ризиків, оскільки навіть мінімальні затримки здатні вплинути на роботу кіберфізичних систем.

Хоча SCADA та EMS добре справляються з виробничими функціями, вони не мають інструментів для повноцінного аналізу ризиків. Їхня аналітика обмежена технологічними параметрами, а фактори поведінки персоналу, кіберзагрози, організаційні процеси чи зовнішні умови, переважно залишаються поза межами їхнього функціоналу. Через це ризик-менеджмент розділений між різними підрозділами підприємства й працює без єдиного координувального центру.

У фрагментованій архітектурі виникають «інформаційні розриви», коли окремі події не пов’язуються між собою. Наприклад, аномалія у потоці телеметрії може збігатися з підозрілою активністю у каналі керування, але через відсутність комплексної аналітики така комбінація залишається непоміченою. Це знижує можливість підприємства прогнозувати інциденти та швидко реагувати на загрози.

Зі збільшенням кількості IoT-пристроїв, мікрогенерації та розподілених мереж зростають вимоги до масштабованості систем. Традиційні інформаційні рішення не завжди здатні обробляти високочастотні потоки даних у реальному часі, що створює ризики втрати інформації, формування некоректних висновків або затримок при прийнятті управлінських рішень.

Для фіксації основних недоліків існуючих систем управління доцільним є використання порівняльної таблиці.

Таблиця 2.6. Недоліки традиційних систем управління в енергетиці

Аспект роботи	**Недолік**	**Потенційний ризик**
SCADA	Відсутність прогнозування	Несвоєчасне реагування на аварію
EMS	Обмежена горизонтальна інтеграція	Помилкові режимні рішення
SOC/SIEM	Нерозвинена взаємодія з OT	Невидимість атак на обладнання
IoT	Розрізненість архітектур	Втрата даних, несинхронність
Big Data	Відсутність єдиного профілю ризику	Неповна оцінка стану системи

Сукупність виявлених недоліків чинних інформаційних рішень у енергетичних компаніях свідчить про нагальну потребу створення єдиної інтегрованої цифрової платформи управління ризиками, яка поєднувала б технологічні, інформаційні, аналітичні, організаційні та кіберзахисні компоненти в узгоджену систему. Така платформа має забезпечувати приймання великих потоків даних з різних джерел, їх синхронізацію, оперативну аналітику, формування профілів ризиків та побудову прогнозних моделей, що дає можливість керівникам і інженерам отримувати повну й актуальну картину стану енергетичної інфраструктури.

Інтегрована система повинна відповідати вимогам масштабованості, високої доступності та відмовостійкості, мати модульну архітектуру та підтримувати підключення нових підсистем без зупинки основних процесів. Такий підхід дозволяє об’єднати роботу SCADA, EMS, SOC/SIEM, IoT-сенсорів, телеметрії, Big Data-платформ та цифрових двійників у єдине середовище, орієнтоване на безперервний моніторинг, аналіз і прогнозування ризиків у реальному часі.

Перехід від фрагментованих рішень до цілісної платформи управління ризиками доцільно подати у вигляді узагальненої структурної схеми.

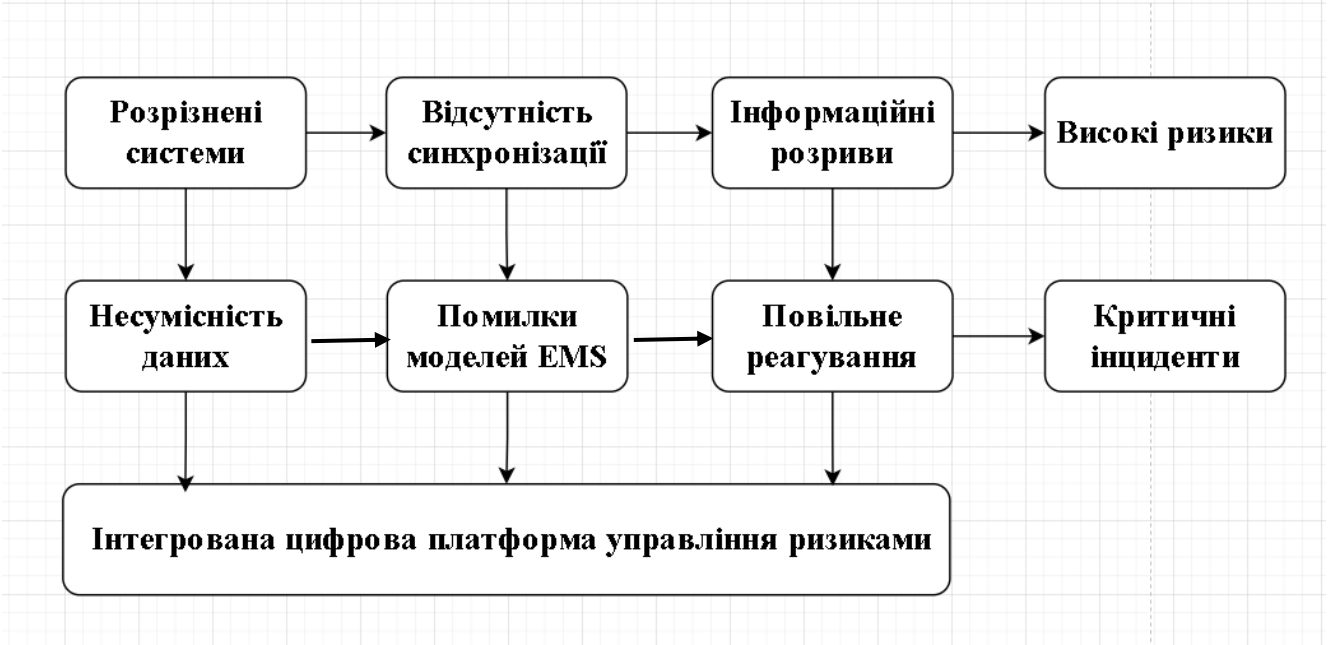


Рисунок 2.6. Необхідність переходу до інтегрованої цифрової платформи ризик-менеджменту

Головним ефектом впровадження інтегрованої цифрової платформи є можливість створення єдиного ризикового профілю для кожного елемента енергетичної інфраструктури. Завдяки цьому підприємство переходить від реактивної моделі роботи, яка передбачає усунення наслідків подій, до проактивного підходу, що зосереджується на їх попередженні. Синхронізована інформація з різних джерел об’єднується в одному середовищі, що дозволяє оперативно виявляти відхилення, оцінювати їх контекст і визначати потенційні загрози на ранніх стадіях.

Інтегрована платформа також формує єдине робоче середовище для персоналу. Узгоджені дані, спільні інструменти аналізу та систематизована інформаційна взаємодія підвищують якість координації між підрозділами та скорочують час прийняття рішень. Завдяки цьому підприємство отримує можливість швидше реагувати на зміни в роботі мережі, технологічні відхилення або прояви кіберзагроз.

Таким чином, виявлені недоліки традиційних SCADA, EMS, SOC, IoT- та аналітичних систем підтверджують потребу переходу до комплексної цифрової

платформи управління ризиками. Така платформа відповідає сучасним викликам цифрової енергетики й забезпечує підвищення стійкості, надійності та ефективності роботи енергетичних підприємств у умовах постійного зростання технологічної складності.

РОЗДІЛ 3. ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ ПРОТОТИПУ ЦИФРОВОЇ ПЛАТФОРМИ УПРАВЛІННЯ РИЗИКАМИ

3.1 Концепція та архітектура цифрової платформи управління ризиками

Розроблена в межах даної магістерської роботи цифрова платформа управління ризиками є інтегрованим веб-рішенням, яке підтримує процеси ідентифікації, оцінювання та моніторингу ризиків в енергетичній галузі. Її концепція базується на принципах гнучкості, масштабованості та модульності, що дає можливість легко адаптувати систему до особливостей підприємства та інтегрувати її з існуючими цифровими ресурсами. Обрана архітектура орієнтована на швидке опрацювання даних, зручність роботи користувача та можливість подальшого функціонального розширення.

Прототип реалізовано з використанням веб-технологій, що забезпечує доступ до системи без встановлення додаткового ПЗ. Застосування Python і Streamlit дозволяє створити інтуїтивний інтерфейс із динамічним оновленням інформації, інтерактивними таблицями та візуалізацією результатів оцінювання ризику. Такий підхід робить платформу доступною для широкого кола користувачів починаючи від інженерів до управлінського персоналу.

Функціональна модель платформи охоплює всі ключові етапи ризик-менеджменту: від ідентифікації та аналізу параметрів ризику до побудови реєстру та подальшого моніторингу. Логіка роботи системи узгоджена зі стандартами ISO 31000 та IEC 31010, що забезпечує відповідність сучасним вимогам корпоративного управління та дозволяє інтегрувати платформу в існуючі бізнес-процеси енергетичного підприємства.

Архітектура прототипу складається з кількох взаємопов’язаних рівнів. Перший рівень — інтерфейс користувача, який забезпечує введення даних, відображення результатів і формування реєстру ризиків. Другий рівень містить аналітичну логіку, де виконуються обчислення з використанням параметрів

ймовірності та впливу. Саме тут реалізовано математичну модель оцінювання ризику, подану у вигляді узагальненої формули:

$$R = P \cdot I,$$

де R— інтегральний рівень ризику, P— імовірність настання події, а I— величина її впливу на енергетичну систему.

Обрана логіка оцінювання ризиків спирається на стандартну для енергетичної галузі двопараметричну модель, у якій кожен ризик визначається через поєднання ймовірності та ступеня впливу. Такий підхід робить систему зрозумілою, дозволяє легко порівнювати різні ризики між собою та застосовувати шкалу прийнятності без додаткових ускладнень.

Третій рівень архітектури відповідає за обробку та тимчасове збереження даних. У поточній реалізації прототип працює на основі внутрішнього середовища збереження Streamlit, що дає змогу створювати інтерактивний реєстр ризиків без використання окремої бази даних. Такий підхід спрощує структуру коду, зберігає гнучкість і демонструє можливості системи в навчальному та експериментальному форматі. При необхідності рішення може бути масштабоване до повноцінної бази даних — SQLite, PostgreSQL або іншої корпоративної системи, що забезпечить інтеграцію з виробничими даними підприємства.

Важливою частиною архітектури є правильно організована структура запису ризику. Базова модель включає сім ключових полів: унікальний код, назву ризику, його категорію, змістовний опис, значення ймовірності, показник впливу та підсумковий рівень ризику. Такі параметри забезпечують баланс між деталізацією та компактністю, а також дозволяє швидко формувати повноцінний реєстр ризиків без зайвого інформаційного навантаження.

Узагальнену структуру даних представлено у таблиці:

Таблиця 3.1. Базова структура даних для моделі ризику

Поле	Опис
id	Унікальний ідентифікатор ризику
назва	Стисла назва ризику
категорія	Технічна, організаційна, кібернетична тощо
опис	Характеристика джерела ризику
ймовірність	Значення від 1 до 5
вплив	Значення від 1 до 5
рівень ризику	Результат обчислення $R = P \cdot I$

Для того щоб продемонструвати логіку архітектури та взаємодію її складових, доцільно представити систему у вигляді схеми, яка відображає рух даних між компонентами.

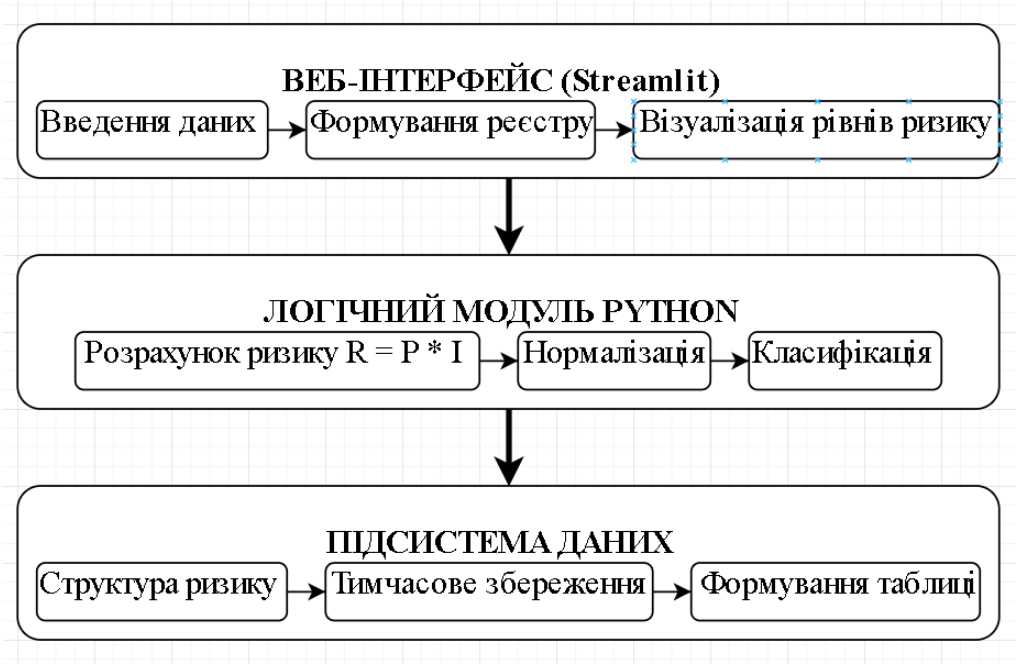


Рисунок 3.1. Узагальнена архітектура веб-прототипу платформи управління ризиками

Концепція створюваної платформи спрямована на формування простого, зручного та технологічно гнучкого інструмента, який може використовуватись енергетичними компаніями як базовий засіб управління ризиками та водночас слугувати основою для розвитку у повноцінну корпоративну систему. У межах даної роботи прототип демонструє ключові функціональні можливості: введення

параметрів ризику, автоматичне обчислення його рівня, побудову інтерактивного реєстру та відтворення результатів у веб-інтерфейсі. Завдяки інтерактивності користувач може змінювати характеристики ризику та одразу бачити, як це впливає на підсумкові розрахунки, що підсилює аналітичну цінність платформи.

Архітектура прототипу виконана таким чином, щоб відтворювати реальні процеси ризик-менеджменту в секторі енергетики, але водночас залишатися компактною й придатною для реалізації в навчальних умовах.

3.2 Модель даних, структура реєстру ризиків та логіка інформаційних потоків

Фундаментом роботи цифрової платформи управління ризиками є модель даних, яка структурує відомості про ризики, їх характеристики, взаємозв'язки та результати оцінювання. Саме коректно побудована модель визначає якість обчислень, формування реєстру ризиків, створення візуальних елементів та функціонування аналітичних модулів. Вона має бути достатньо компактною для реалізації у прототипі, але водночас містити всі необхідні елементи для охоплення повного циклу ризик-менеджменту.

У роботі застосовано базову модель із семи параметрів, яка забезпечує баланс між простотою та інформативністю і відповідає поширеним підходам у галузі та міжнародним стандартам.

Модель передбачає автоматичне створення унікального ідентифікатора для кожного ризику, що усуває дублювання та забезпечує правильну роботу реєстру. Назва визначає загальний зміст ризику, а категорія відносить його до технічного, організаційного, кібернетичного або іншого типу, що спрощує систематизацію й підготовку звітів.

Опис слугує якісною характеристикою та дозволяє деталізувати джерела виникнення, чинники впливу й потенційні наслідки. У сфері енергетики це особливо важливо, оскільки числові показники не завжди повністю відображають складність технологічних взаємозв'язків.

Параметри «ймовірність» та «вплив» формують основу кількісної оцінки ризику. Обидва значення задаються у шкалі від 1 до 5, де 1 означає мінімальний

рівень, а 5 — критичний. Підсумковий рівень ризику розраховується відповідно до методики, описаної у попередньому розділі:

$$R = P \cdot I.$$

Запропонована модель оцінювання ризику є лінійною, що забезпечує зрозуміле й однозначне трактування результатів. Такий підхід дозволяє легко порівнювати ризики між собою та швидко визначати їхню пріоритетність. Незважаючи на те, що у великих корпоративних системах деколи застосовують багатофакторні або нелінійні моделі, у даному прототипі свідомо обрано прозору та інтерпретовану методику..

Модель даних є основою для формування реєстру ризиків — центрального елементу платформи, який представляє весь перелік актуальних загроз у вигляді динамічної таблиці. Реєстр автоматично оновлюється після додавання нового запису, що забезпечує актуальність інформації та можливість оперативного аналізу. Він виконує роль ключового інформаційного ресурсу системи, надаючи інструменти для сортування, фільтрації, пошуку та перегляду характеристик кожного ризику. У майбутньому саме на основі цього реєстру можуть формуватися графічні звіти, аналітичні панелі або інші складні візуальні компоненти.

Таблиця 3.2. Структура моделі даних цифрової платформи

Поле	Тип	Призначення
id	Цілочисельний	Унікальний індекс запису
назва	Текст	Стисла ідентифікація ризику
категорія	Текст	Приналежність до типу ризику
опис	Текст	Детальна характеристика ризику
ймовірність (P)	Число 1–5	Оцінка частоти виникнення
вплив (I)	Число 1–5	Ступінь наслідків
рівень ризику (R)	Число	Обчислений показник $R = P \cdot I$

Важливою складовою моделі є логіка руху даних, яка визначає, як інформація проходить між усіма компонентами системи починаючи від моменту введення користувачем параметрів до формування підсумкової таблиці ризиків. Процес починається в інтерфейсі веб-додатка, де користувач задає числові та текстові значення. Після підтвердження ці дані передаються до логічного модуля на Python,

який перевіряє їх коректність, виконує необхідні обчислення та формує структурований запис ризику.

Сформовані дані надходять до підсистеми збереження. У прототипі використовується механізм тимчасового зберігання у сесії Streamlit, що дозволяє підтримувати актуальний стан реєстру протягом роботи програми. Такий підхід демонструє принципи побудови системи без потреби у використанні повноцінної бази даних, але при цьому зберігає логіку реального цифрового рішення.

Завершальним етапом є створення реєстру ризиків, який автоматично оновлюється після кожного внесення нового запису. Streamlit забезпечує інтерактивне відображення таблиці, що дозволяє користувачеві переглядати, сортувати та фільтрувати інформацію, формуючи зручний інструмент для подальшого аналізу.

Для узагальнення послідовності цих процесів використовується схема, яка демонструє взаємодію між основними елементами моделі.

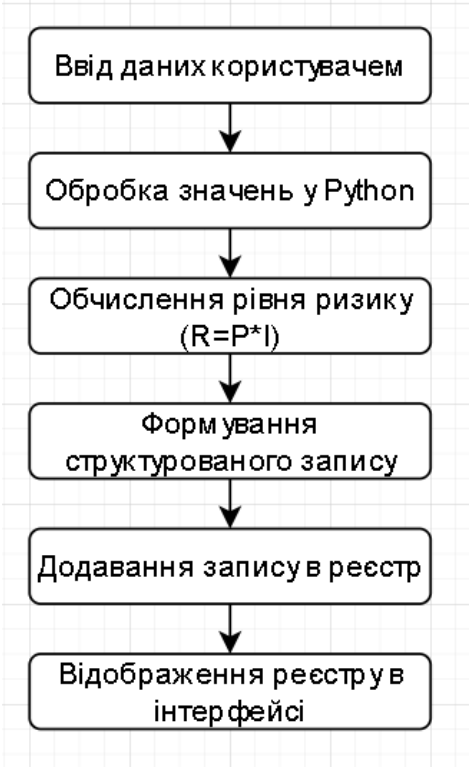


Рисунок 3.2.– Логіка руху даних у прототипі платформи управління ризиками

Логіка інформаційних потоків визначає фундамент для майбутнього масштабування платформи та її інтеграції з іншими цифровими системами. Саме

вона забезпечує можливість подальшого підключення зовнішніх баз даних, модулів кіберзахисту, аналітичних сервісів, а також інтеграцію з SCADA/EMS та іншими виробничими системами. У результаті реєстр ризиків може стати частиною комплексного корпоративного рішення, яке охоплюватиме як технологічні процеси, так і аналітичні механізми управління.

Сформована модель даних, структура реєстру і побудована логіка руху інформації створюють основу для наступного етапу — розробки функціональних модулів. Саме ці модулі виконуватимуть ключові операції платформи, забезпечуючи взаємодію користувача з системою, розрахунки та обробку даних.

3.3 Функціональні модулі системи (ідентифікація, оцінювання, аналіз, звітність)

Проектування цифрової платформи управління ризиками передбачає створення модульної системи, де кожен компонент виконує свою функцію в рамках загального процесу ризик-менеджменту. Такий підхід дає можливість розділити логіку роботи на окремі частини, забезпечити прозорість алгоритмів, спростити реалізацію та створити умови для подальшого масштабування. У рамках прототипу виділено чотири основні модулі: ідентифікаційний, оцінювальний, аналітичний та модуль звітності. Разом вони формують послідовний цикл цифрового управління ризиками та підтримують прийняття обґрунтованих рішень. Ідентифікаційний модуль є вихідною точкою платформи та відповідає за створення нового запису в системі. У веб-інтерфейсі він поданий у вигляді набору форм, де користувач вводить ключові характеристики ризику: найменування, категорію, опис та показники ймовірності й впливу. Модуль перевіряє правильність введених даних, після чого створює упорядкований запис, який додається до реєстру ризиків. На цьому етапі визначається первинна структура профілю ризику.

Наступним у ланцюзі є модуль оцінювання. Його завдання розрахувати інтегральний рівень ризику на основі введених показників.

Обчислення виконуються відповідно до простої математичної моделі:

$$R = P \cdot I,$$

де P— імовірність виникнення ризику, а I— ступінь його впливу.

Оцінювальний модуль, окрім базового обчислення інтегрального показника, може виконувати додаткові операції — нормалізацію введених величин або перетворення числового значення ризику у якісні категорії, такі як «низький», «середній» чи «високий». Подібна класифікація широко використовується в енергетичних компаніях та спрощує інтерпретацію результатів. У межах створеного прототипу використано лінійну модель оцінювання, що забезпечує простоту реалізації та повну зрозумілість алгоритму для користувача.

Аналітичний модуль відповідає за узагальнення даних та їх подальше подання у зручному форматі. На рівні демонстраційного прототипу він формує інтерактивну таблицю реєстру ризиків, яка автоматично оновлюється після кожного нового запису. У перспективі цей модуль може бути доповнений розширеною аналітикою — графіками, тепловими картами, діаграмами зв’язків, дашбордами та інструментами сценарного моделювання. Саме аналітичний модуль визначає потенціал розвитку системи до повноцінної корпоративної платформи, інтегрованої з іншими цифровими сервісами підприємства.

Заключним елементом структури є модуль звітності. Його головне завдання це формувати структуровані представлення даних, які можуть бути використані у процесах оперативного, тактичного та стратегічного управління. У межах прототипу звітність реалізована у вигляді інтерактивного виведення реєстру ризиків, проте архітектура передбачає можливість подальшого додавання формування PDF-звітів, експорту в CSV та організації обміну даними з іншими системами. Завдяки цьому модуль звітності виконує роль комунікаційного інтерфейсу між різними групами користувачів — інженерами, аналітиками та керівництвом.

Для наочного представлення логіки взаємодії між модульними компонентами доцільним є формування схеми, що демонструє послідовність і взаємозв’язки етапів обробки даних у платформі.

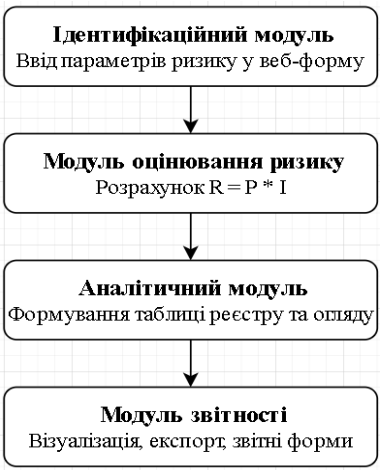


Рисунок 3.3 – Логічна взаємодія функціональних модулів системи

Спільна модель даних забезпечує узгодженість інформації між усіма елементами платформи та підтримує безперервність процесів її обробки. Завдяки єдиній структурі даних система охоплює повний цикл управління ризиками починаючи від моменту їх ідентифікації до формування підсумкового звіту. Така організація дозволяє забезпечити логічну цілісність процесів та відповідність вимогам ризик-менеджменту, які застосовуються в енергетичних компаніях.

Для відображення ролі кожного модуля у загальній архітектурі доцільно подати узагальнену таблицю, що демонструє їхні ключові функції та взаємозв’язки у контексті роботи платформи.

Таблиця 3.3. Функціональні характеристики модулів прототипу

Модуль	Основне призначення	Результат функціонування
Ідентифікаційний	Ввід параметрів ризику та формування запису	Структурований набір вхідних даних
Модуль оцінювання	Обчислення рівня ризику	Значення інтегрального показника ризику
Аналітичний	Формування та відображення реєстру	Оновлювана таблиця ризиків
Модуль звітності	Формування підсумкових представлень	Візуальна аналітика та експорт

Узагальнюючи, можна стверджувати, що розроблені функціональні модулі формують цілісний фундамент цифрової платформи управління ризиками, яка відповідає сучасним вимогам до інформаційних систем енергетичного сектору. Їхня структурована взаємодія демонструє потенціал для подальшого розвитку та інтеграції з більш складними інфраструктурними рішеннями, включно з системами SCADA, EMS, SOC, телеметричними платформами та засобами бізнес-аналітики. Завдяки такій архітектурі система здатна підтримувати розширений аналіз ризиків, забезпечувати узгодженість даних та адаптуватися до специфічних умов роботи енергетичних підприємств.

3.4. Програмна реалізація цифрової платформи (опис алгоритмів, структури та принципів роботи)

Програмна реалізація цифрової платформи управління ризиками виконана за допомогою Python та Streamlit, що дало змогу створити інтерактивний веб-застосунок без розроблення окремих клієнтських і серверних модулів. Такий підхід значно спрощує роботу користувача та водночас забезпечує необхідний рівень гнучкості й функціональності для підтримки основних процесів управління ризиками у сфері енергетики.

Логіка програмної частини побудована за модульним принципом і охоплює кілька ключових етапів: введення параметрів ризику, виконання обчислень, автоматичне оновлення реєстру та інтерактивне відображення результатів. Основою роботи системи є модель оцінювання ризику, що передбачає множення показників імовірності та впливу, тобто використання формули виду:

$$R = P \cdot I,$$

де P— імовірність виникнення ризику, а I— ступінь впливу на технологічні чи бізнес-процеси.

Ця модель забезпечує простий і зрозумілий механізм розрахунку, який повністю відповідає концепції прототипу та дозволяє користувачу одразу отримувати результати оцінювання у зручному форматі.

Основою роботи веб-платформи є механізм тимчасового збереження даних у сесії користувача. У Streamlit для цього використовується внутрішній контейнер

st.session_state, у якому зберігається список ризиків у структурованому форматі. Кожен запис формується як словник із ключовими параметрами: назва, категорія, опис, значення ймовірності та впливу, а також підрахований інтегральний показник ризику. Використання сесійного сховища дозволяє автоматично оновлювати реєстр у момент додавання кожного нового ризику, що забезпечує наочність роботи прототипу.

Важливим елементом програмної логіки є модуль класифікації, який визначає належність ризику до однієї з категорій — «низький», «середній» або «високий». Це спрощує оцінку критичності та дає змогу пріоритезувати реагування. Реєстр ризиків у прототипі впорядковується автоматично: найвищі значення R відображаються першими, що дозволяє одразу бачити найбільш вагомі записи.

Система також виконує базові аналітичні операції. Після формування таблиці визначається ризик із максимальним значенням R та розраховується середній інтегральний показник по всіх записах. Ця інформація відображається текстово та демонструє можливість первинного узагальнення даних. У перспективі аналітичний блок може бути розширений графічними інструментами, модулями машинного навчання або функціями прогнозування.

Фінальний веб-інтерфейс включає форму для введення параметрів ризику, інтерактивну таблицю реєстру та елемент відображення підсумкової аналітики. Введення даних реалізоване через input-поля та повзунки, що мінімізує ймовірність помилок користувача. Логіка обробки є структурованою та ізольованою, що забезпечує стабільність роботи всієї системи.

З технічної точки зору прототип повністю функціонує у PyCharm або будь-якому іншому середовищі з встановленим Python і необхідними бібліотеками. Запуск здійснюється командою:

streamlit run risk_app.py

Після цього відкривається браузер із користувацьким інтерфейсом платформи. Повний вихідний код із коментарями та описом модулів наведений у Додатку А.

3.5 Тестування прототипу та приклади його використання

Тестування прототипу платформи управління ризиками проводилося для підтвердження коректності роботи алгоритмів, перевірки стабільності веб-інтерфейсу та оцінки того, як система обробляє й оновлює реєстр ризиків у режимі реального часу. Оскільки платформа реалізована як інтерактивний веб-додаток на Streamlit, перевірка здійснювалася у середовищі PyCharm з подальшим відображенням інтерфейсу у браузері, що відтворило типові умови користувацької роботи.

Першим кроком був запуск додатка через команду streamlit run risk_app.py, після чого автоматично відкрився веб-інтерфейс. На початковому етапі тестування оцінювалася правильність відображення всіх елементів: полів введення назви, категорії, текстового опису, а також повзунків для встановлення значень ймовірності та впливу. Перевірка засвідчила, що інтерфейс працює стабільно, елементи реагують без затримок, а взаємодія не потребує перезавантаження сторінки.

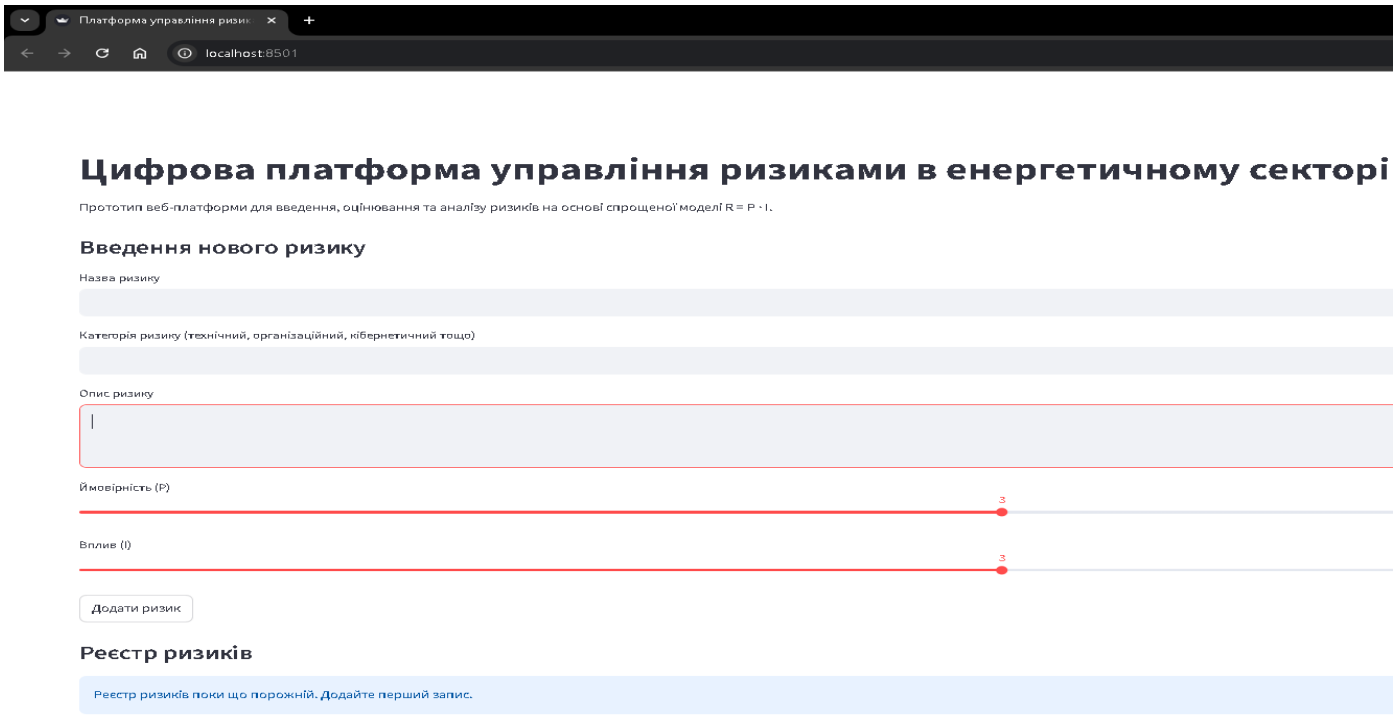


Рисунок 3.4. Початковий екран прототипу в веб-браузері

Після перевірки коректності роботи інтерфейсу було розпочато функціональне тестування логіки обробки та збереження інформації. На цьому етапі до платформи вводилися тестові дані характерні для енергетичної галузі. Основна увага приділялася тому, як система опрацьовує введені значення, чи коректно вони зберігаються в межах поточного сеансу та чи вірно формується таблиця реєстру. У ході тестування встановлено, що всі записи успішно додаються, миттєво відображаються в таблиці та залишаються доступними протягом усього сеансу роботи програми.

Приклади використаних тестових даних:

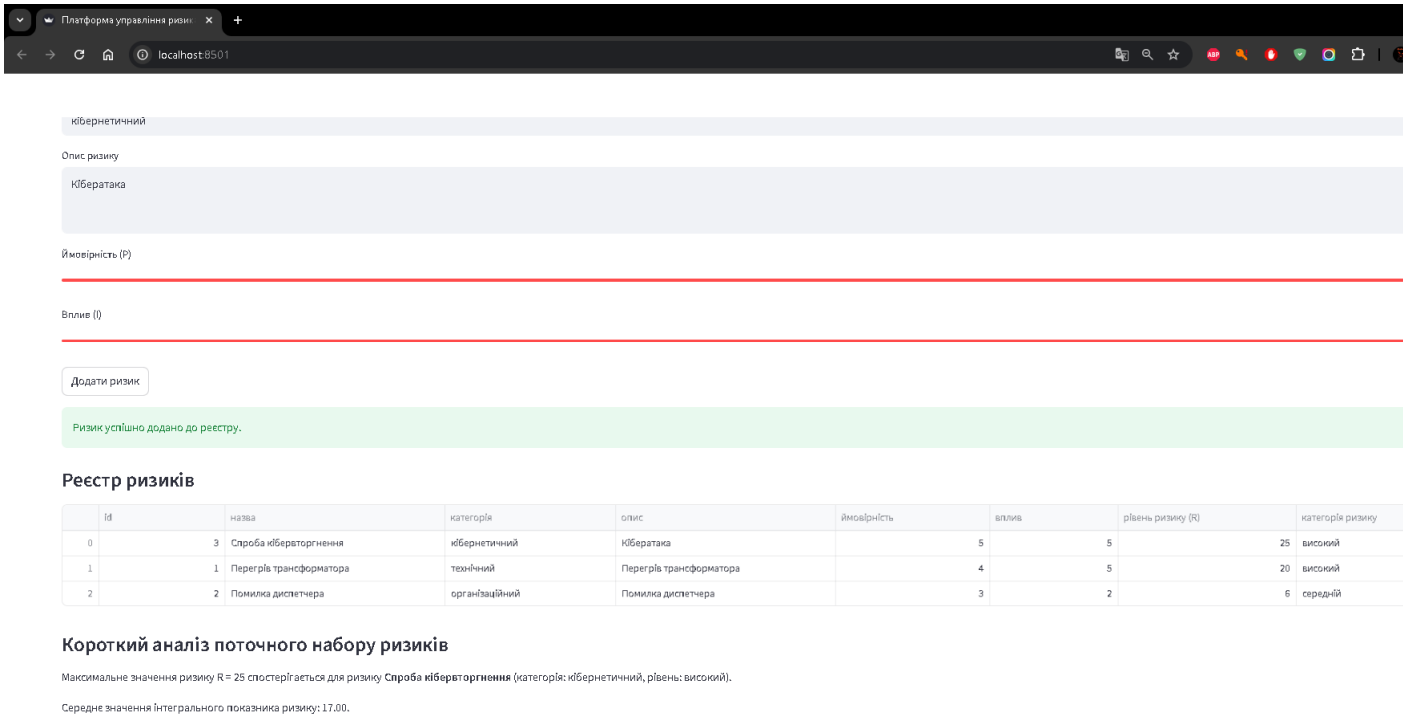
— **Тестовий ризик 1:**
Назва: «Перегрів трансформатора».
Категорія: технічний.
Ймовірність: 4.
Вплив: 5.
Очікуване значення $R = 20$(високий рівень ризику).

— **Тестовий ризик 2:**
Назва: «Помилка диспетчера».
Категорія: організаційний.
Ймовірність: 3.
Вплив: 2.
Очікуване значення $R = 6$(середній рівень ризику).

— **Тестовий ризик 3:**
Назва: «Спроба кібервторгнення».
Категорія: кібернетичний.
Ймовірність: 5.
Вплив: 5.
Очікуване значення $R = 25$(високий рівень ризику).

Після внесення кожного нового запису система автоматично розраховувала інтегральний рівень ризику, створювала відповідну структурну модель даних та зберігала її у внутрішньому сховищі st.session_state. Результати тестування показали, що розрахунок за формулою R = P·I виконується правильно в усіх перевірених сценаріях. Окремо було підтверджено коректність роботи механізму класифікації: значення R≤5 відносилися до низького рівня, 6–12 — до середнього, а R>12 — до високого.

На наступному етапі оцінювалося автоматичне формування реєстру ризиків. Після введення трьох тестових прикладів система побудувала таблицю DataFrame, упорядковану за спаданням інтегрального показника. Це відповідає логіці пріоритезації, коли першочергово аналізуються найкритичніші ризики. Відповідний результат продемонстровано на Рисунку 3.5, де наведено сформований реєстр після додавання тестових даних.



	id	назва	категорія	опис	ймовірність	вплив	рівень ризику (R)	категорія ризику
0	3	Спроба кібервторгнення	кібернетичний	Кібератака	5	5	25	високий
1	1	Перегрів трансформатора	технічний	Перегрів трансформатора	4	5	20	високий
2	2	Помилка диспетчера	організаційний	Помилка диспетчера	3	2	6	середній

Рисунок 3.5. Сформований реєстр після додавання тестових даних

Під час тестування окремо оцінювалася робота аналітичного модуля. Після побудови реєстру система коректно визначала ризик із максимальним значенням R та розраховувала середній інтегральний показник. У тестовому прикладі найвищим став ризик «Спроба кібервторгнення» зі значенням R=25, а середнє значення становило 17.0. Це підтвердило стабільність алгоритмів і коректність роботи розрахункових механізмів у середовищі pandas, що було додатково перевірено візуально.

Також протестовано поведінку системи за відсутності обов’язкових значень. Перевірка на заповнення полів назви та категорії працює належним чином: у разі

спроби додати неповний запис система відразу виводить повідомлення про помилку. Відповідний приклад показано на Рисунку 3.6.

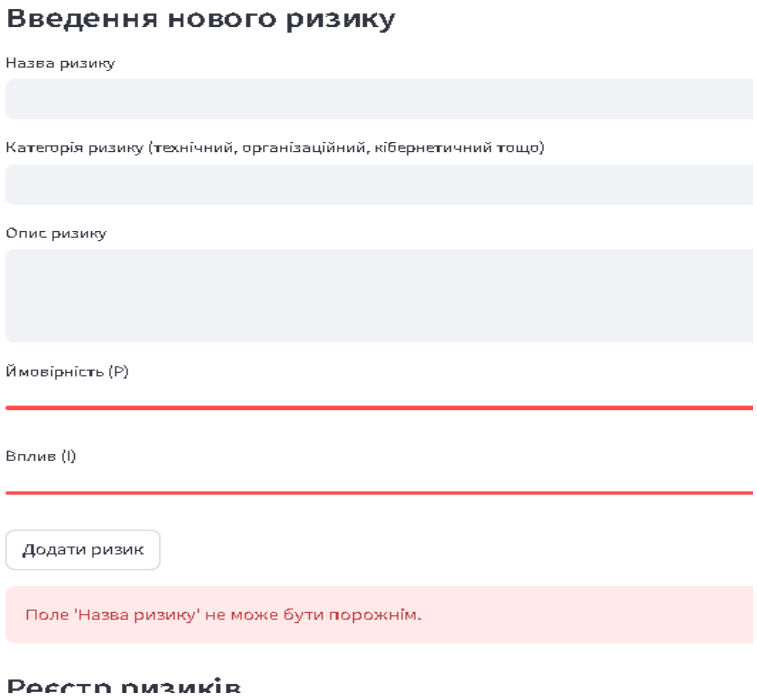


Рисунок 3.6. Відображення помилки при некоректному введені даних

Таке реагування системи підтверджує коректну роботу механізмів валідації введених даних. Загальні результати тестування засвідчили, що прототип працює стабільно: правильно приймає та опрацьовує інформацію, коректно розраховує інтегральний рівень ризику, формує та оновлює реєстр у режимі реального часу, а також забезпечує наочне відображення результатів. Функціональність прототипу повністю відповідає вимогам, поставленим для базової цифрової платформи управління ризиками, і може слугувати фундаментом для створення розширеної системи, адаптованої до потреб енергетичних підприємств.

Проведене тестування підтвердило відповідність програмного рішення встановленим вимогам та довело його практичну придатність для підтримки процесів ризик-менеджменту. Скріншоти, що демонструють роботу системи, додатково згруповані у Додатку А.

3.6 Перспективи розвитку та можливості масштабування цифрової платформи

Розроблена цифрова платформа управління ризиками є початковим прикладом реалізації концепції, що демонструє можливість структурованого збору та обробки ризикової інформації в енергетичній галузі. Попри свою базовість, система відображає ключові етапи процесу ризик-менеджменту та може слугувати основою для подальшого розширення. Водночас динамічний розвиток цифрових технологій, зростання кількості телеметричних пристроїв і підвищення кіберзагроз створюють потребу у масштабуванні функціоналу прототипу в різних напрямках — як технічних, так і організаційних.

Одним із наступних логічних кроків розвитку є інтеграція платформи з промисловими цифровими системами (SCADA, EMS, WAMS, АСУ ТП). Це дозволить отримувати дані в режимі реального часу та формувати ризикові події автоматично, без ручного введення. Автоматизація процесу значно скоротить час реагування й зменшить залежність від людського фактору.

Перспективним також є впровадження алгоритмів машинного навчання, які дадуть змогу прогнозувати ризикові ситуації, визначати приховані тенденції та покращувати точність оцінювання. Перехід до прогнозних моделей забезпечить вищий рівень аналітики та дозволить системі підтримувати прийняття рішень у складних режимних умовах.

Удосконалення архітектури даних є ще одним напрямом розвитку. Наявне сесійне збереження даних слід замінити на повноцінне сховище, яке дозволить накопичувати історичні записи, проводити аудит та відстежувати зміни в ризикових профілях. Це важливий крок для застосування платформи в реальних умовах енергетичного підприємства.

Подальший розвиток інтерфейсу може включати створення інтерактивних панелей моніторингу, графіків, теплових карт та інструментів сценарного аналізу. Розширена візуалізація дасть змогу користувачам швидше оцінювати ситуацію та приймати обґрунтовані рішення.

Платформа може бути інтегрована з корпоративними системами (SOC/SIEM, CMMS/ERP, Power BI, Tableau) через API, що створить єдиний інформаційний контур управління ризиками. Така інтеграція дозволить об'єднати технічні, інформаційні та адміністративні дані в одну екосистему.

Посилення безпеки є обов’язковим елементом розвитку платформи. Розширена версія має відповідати вимогам міжнародних та галузевих стандартів (ISO/IEC 27001, NERC CIP, ДСТУ), передбачати автентифікацію, контроль доступу, шифрування та ведення журналу подій.

Отже, створений прототип має значний потенціал розвитку. Система може бути трансформована у масштабну цифрову платформу управління ризиками, здатну працювати з великими потоками даних, взаємодіяти з технологічними комплексами та підтримувати стратегічні рішення на основі сучасних інформаційних технологій. Гнучка архітектура дозволяє адаптувати платформу до потреб енергетичних підприємств та вимог цифрової інфраструктури.

ВИСНОВКИ

У магістерській роботі проведено комплексне дослідження теоретичних, практичних та аналітичних аспектів управління ризиками в енергетичній сфері. Аналіз показав, що цифрова трансформація енергетичного сектору, зростання залежності від інформаційних технологій та поява нових типів загроз формують сучасне середовище ризиків, де традиційні підходи вже не забезпечують необхідної точності та оперативності. На цьому тлі потреба у створенні цифрової платформи для управління ризиками є цілком обґрунтованою.

У першому розділі встановлено, що енергетичні системи характеризуються високою взаємопов’язаністю, великою кількістю інформаційних потоків та різноманітністю потенційних загроз технічного, кібернетичного, організаційного й зовнішнього характеру. Це вимагає переходу від статичних методів оцінювання до інтегрованих цифрових рішень, здатних працювати з великими масивами даних і підтримувати аналітику в реальному часі.

Другий розділ був присвячений огляду актуальних цифрових систем, що використовуються енергетичними підприємствами (SCADA, EMS, цифрові двійники, IoT, інструменти кіберзахисту). Виявлено, що попри значний розвиток цих технологій, вони функціонують відокремлено, що не дозволяє формувати єдиний комплексний погляд на ризики. Саме ця фрагментованість стала основою для визначення вимог до цифрової платформи: інтегративності, адаптивності, автоматизованості та здатності до масштабування.

На основі проведеного аналізу у третьому розділі запропоновано концепцію архітектури цифрової платформи управління ризиками та створено її прототип. Реалізація на Python із застосуванням Streamlit дала змогу сформувати зручний веб-інтерфейс, забезпечити введення ризиків, їх обробку, ранжування за інтегральним показником та динамічне оновлення реєстру. Модель оцінювання ризику, продемонструвала свою практичність і зрозумілість для користувача.

Тестування підтвердило коректність роботи прототипу, правильність алгоритмів розрахунку та стабільність веб-інтерфейсу. Система успішно

опрацювала тестові сценарії, коректно визначила найкритичніші ризики та сформувала структурований реєстр, що засвідчує її придатність як демонстраційного інструменту та основу для подальшої модернізації.

Перспективи розвитку платформи включають інтеграцію з технологічними системами енергетики, розширення аналітичного блоку, впровадження механізмів машинного навчання, перехід до промислових баз даних, покращення інформаційної безпеки та масштабування інфраструктури. Такі напрями дадуть змогу перетворити прототип на повноцінну корпоративну платформу підтримки управлінських рішень.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Коваленко А. О., Костенко В. В. Управління ризиками на підприємствах енергетичного сектору: сучасні підходи та виклики цифровізації. *Економіка та держава*. 2021. № 6. С. 48–52.

2. Пахомов Ю. О., Риженко К. О. Інформаційні технології в енергетиці: сучасний стан та перспективи. Київ: Наук. думка, 2020.

3. Шевченко І. В. Кіберстійкість енергетичних систем у контексті цифрової трансформації. *Вісник НТУУ «КПІ». Інформатика*. 2022. № 3. С. 17–25.

4. Маляренко А. Системи SCADA в електроенергетиці: архітектура та захист. Запоріжжя: ЗНУ, 2021.

5. Гриб О. Г., Данилюк А. Ф. Основи ризик-менеджменту. Київ: КНЕУ, 2019.

6. Міністерство енергетики України. Енергетична стратегія України до 2035 року. Київ, 2017.

7. Міненерго України. Звіт про стан ОЕС України за 2022 рік. Київ, 2023.

8. ДТЕК. Звіт зі сталого розвитку 2022–2023.

9. Войтович О. М., Павлюк П. М. Інтелектуальні енергетичні системи та цифрові двійники: сучасні тенденції. *Енергетика та електрифікація*. 2021. № 4. С. 22–31.

10. Кучеренко О. Г., Матвієнко В. Д. Інформаційна безпека критичної інфраструктури. Київ: НАУ, 2021.

11. ДСТУ 3973:2000. Надійність техніки. Терміни та визначення.

12. Закон України «Про ринок електричної енергії». Київ, 2019.

13. Закон України «Про основи національної безпеки України». Київ, 2020.

14. Постанова НКРЕКП № 1431 «Про забезпечення кіберзахисту об’єктів енергетики». Київ, 2021.

15. Гнатюк В. О. Кібербезпека та захист критичної інфраструктури. Київ: КРОК, 2020.

16. Олійник А. В. Математичні методи оцінювання ризиків в інженерних системах. Львів: ЛНУ, 2018.

17. Пеліховський О. М., Нікітін Є. В. Цифровізація енергетики: виклики та можливості. Харків: ХНУРЕ, 2021.

18.Міненерго України. Концепція кіберзахисту енергетики. Київ, 2022.

19.НАН України. Цифрова трансформація енергетичних систем: науковий звіт. Київ, 2022.

20.Кравчук О. В. Аналітика великих даних в енергетиці. Київ: ІЕП НАНУ, 2021.

21.Мороз Н. Л. Інформаційні системи підтримки прийняття рішень. Київ: КНЕУ, 2020.

22.Бровко О. П., Калюжний С. В. Управління технологічними ризиками. Запоріжжя: ЗДІА, 2019.

23.Держенергонагляд України. Звіт щодо технічних інцидентів у мережах за 2022 рік. Київ, 2023.

24.Укренерго. Звіт про надійність магістральних мереж. Київ, 2022.

25.Укренерго. Концепція цифрової трансформації 2021–2025. Київ, 2021.

26.Офіс цифрової трансформації України. Стратегія цифрової інфраструктури. Київ, 2022.

27.НАНУ. Енергетична безпека України: проблеми і рішення. Київ, 2021.

28.Станкевич С. Системний аналіз у сфері енергетики. Харків: ХАІ, 2020.

29.Таргонський Ю. В. IoT-рішення в енергетиці. Київ: ДУТ, 2022.

30.Слободянюк М. В. Алгоритми обробки даних в енергосистемах. Одеса: ОНУ, 2021.

31.Національний центр кібербезпеки України. Аналітичний огляд інцидентів у критичній інфраструктурі. Київ, 2023.

32.ДПС України. Методичні рекомендації з аналізу ризиків. Київ, 2020.

33.ISO 31000:2018 Risk management — Guidelines. International Organization for Standardization, 2018.

34.ISO/IEC 27001:2022 Information security management systems — Requirements. ISO, 2022.

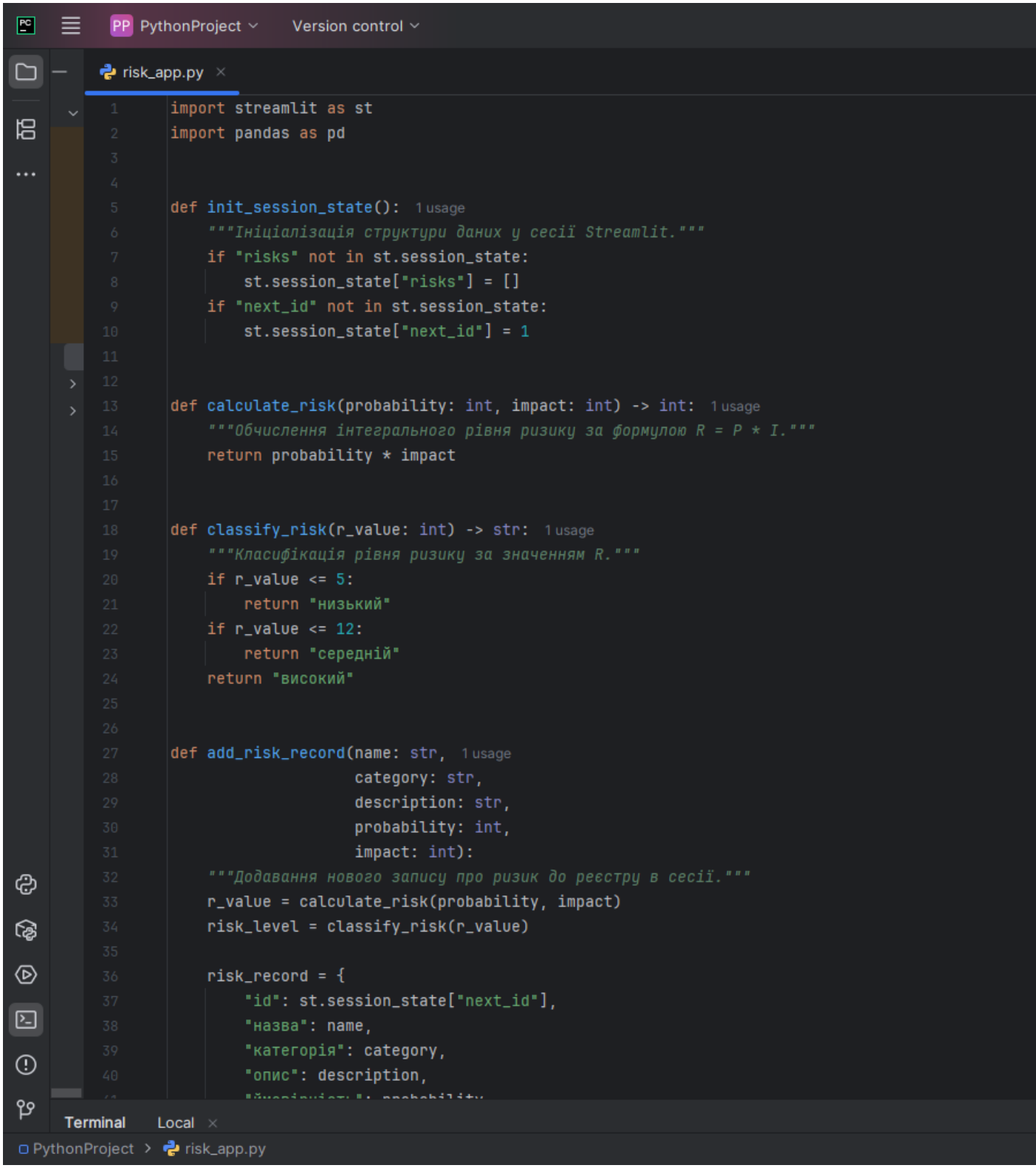
35.IEC 62351. Data and communication security for power systems. IEC, 2018.

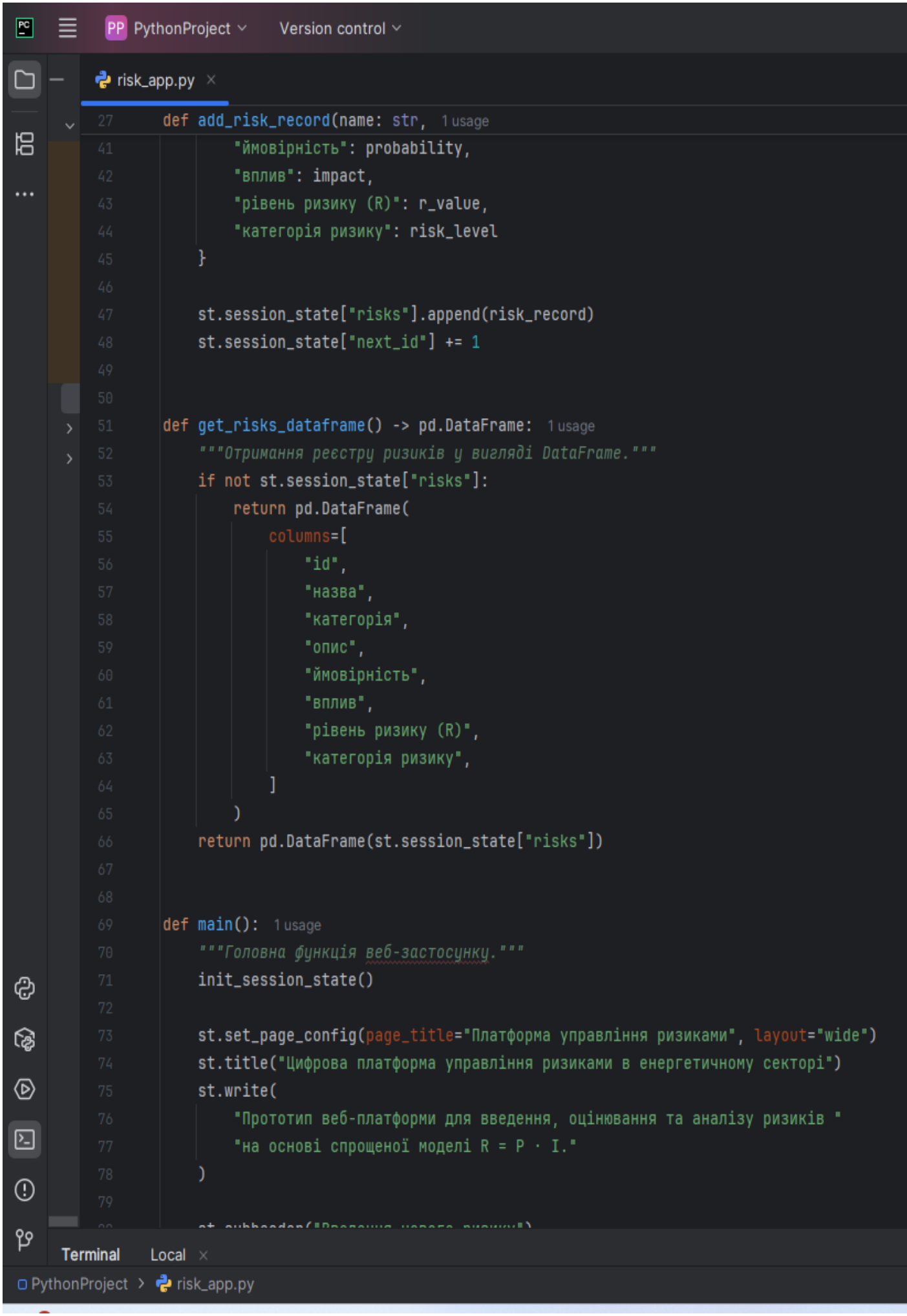
36.ENTSO-E Cybersecurity Framework. European Network of Transmission System Operators for Electricity, 2021.

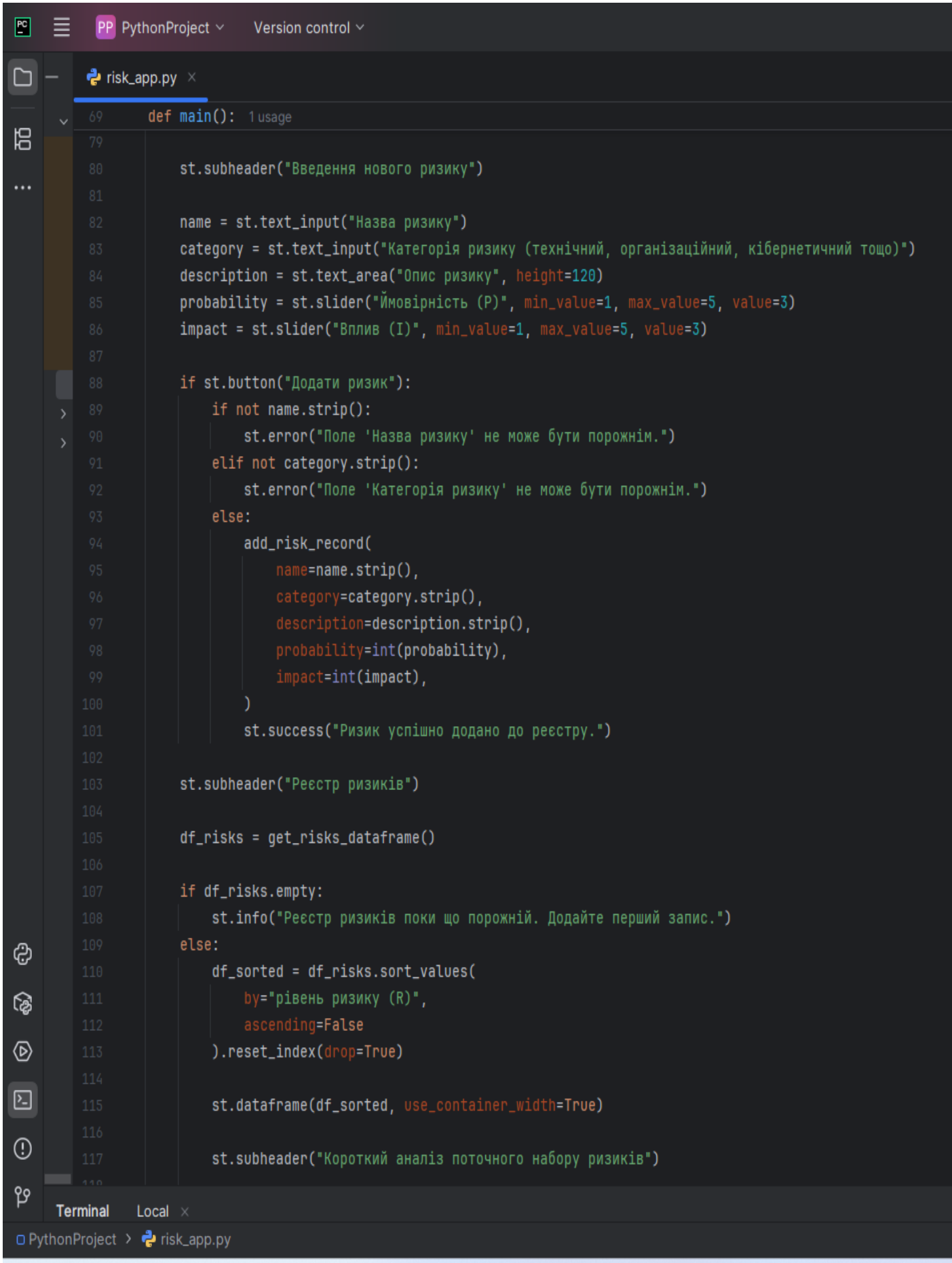
37.NERC CIP Standards. North American Electric Reliability Corporation.

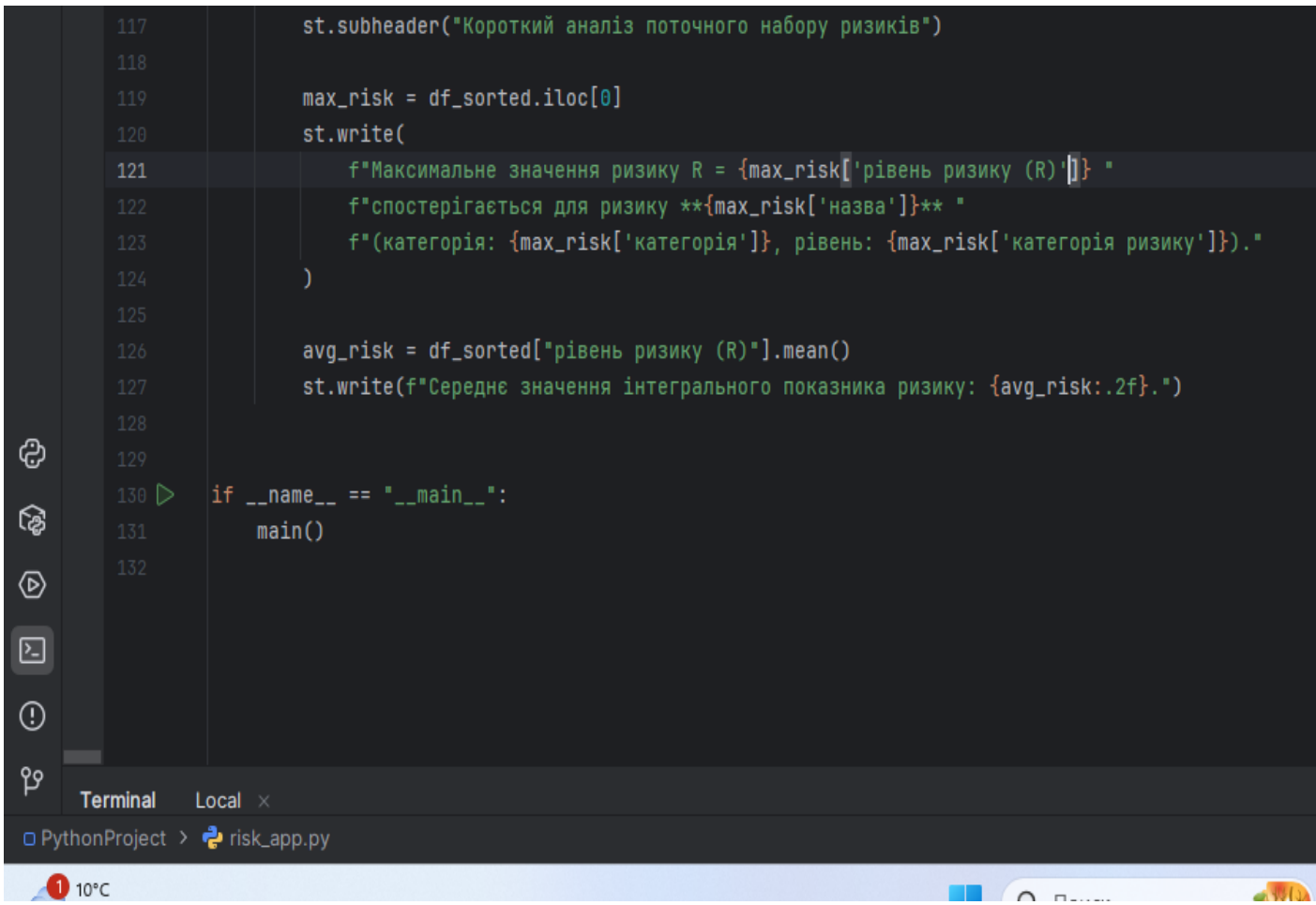
38.Big Data Analytics in Smart Grids / S. Maier, M. Liserre (Eds.). Springer, 2020.
39.Zhang Y., Wang L. Cyber-Physical Attacks and Defence in Power Systems. Springer, 2020.
40.IBM Energy & Utilities. Artificial Intelligence in Grid Operations. Whitepaper, 2021.
41.Kosek A. Real-Time Anomaly Detection in Smart Grids. *Journal of Modern Power Systems and Clean Energy*. 2020.
42.Siano P. Demand Response and Smart Grids: A Survey. *Renewable and Sustainable Energy Reviews*. 2020.
43.Bessis N., Dobre C. Big Data and Internet of Things: Roadmap for Smart Environments. Springer, 2019.
44.Oracle Utilities. Risk-Based Asset Management in Power Systems. Technical Report, 2020.
45.International Energy Agency (IEA). Digital Demand-Driven Electricity Systems Report. Paris, 2022.

ДОДАТОК А
ВИХІДНИЙ КОД ПРОГРАМНОГО ПРОТОТИПУ ЦИФРОВОЇ ПЛАТФОРМИ УПРАВЛІННЯ РИЗИКАМИ

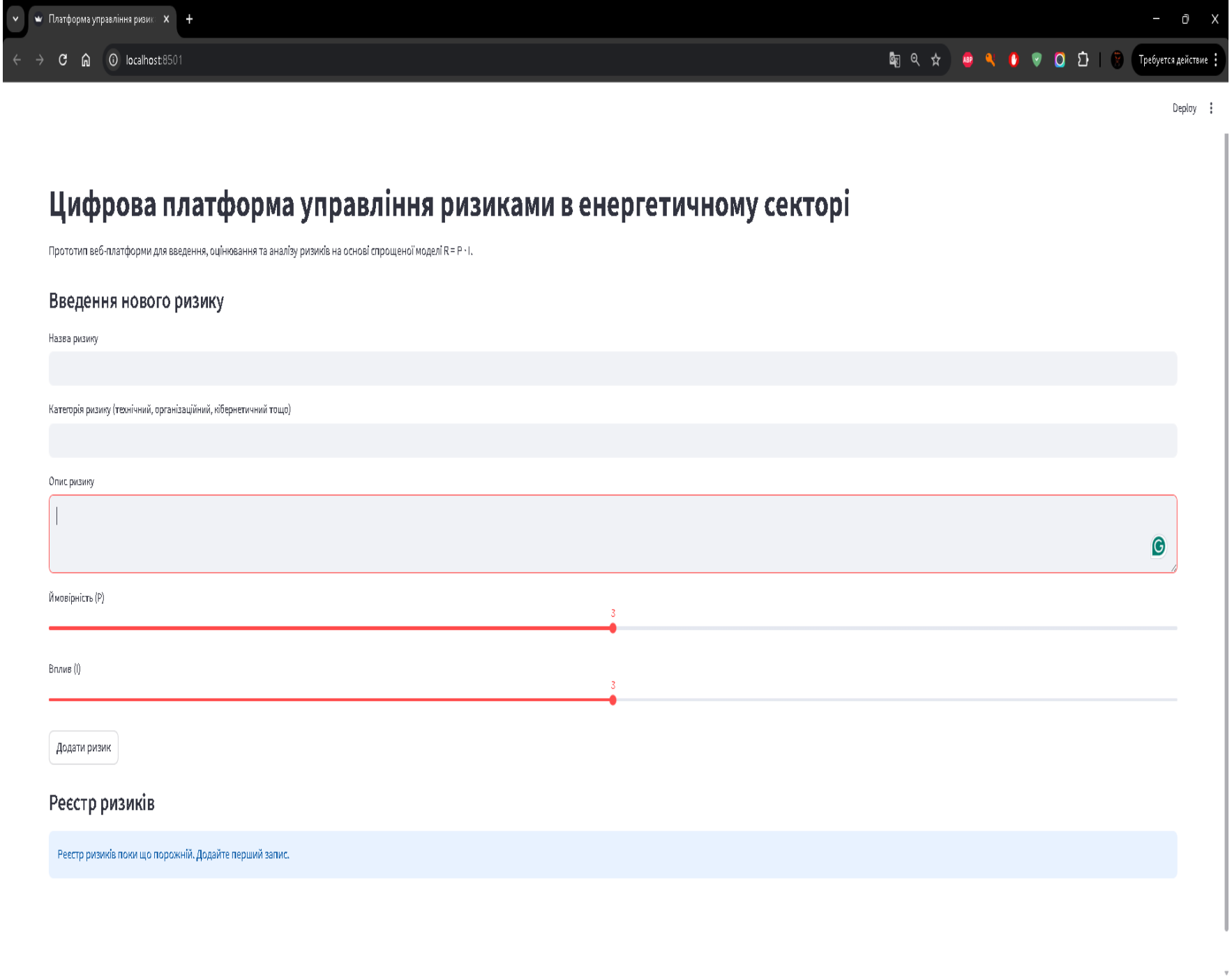


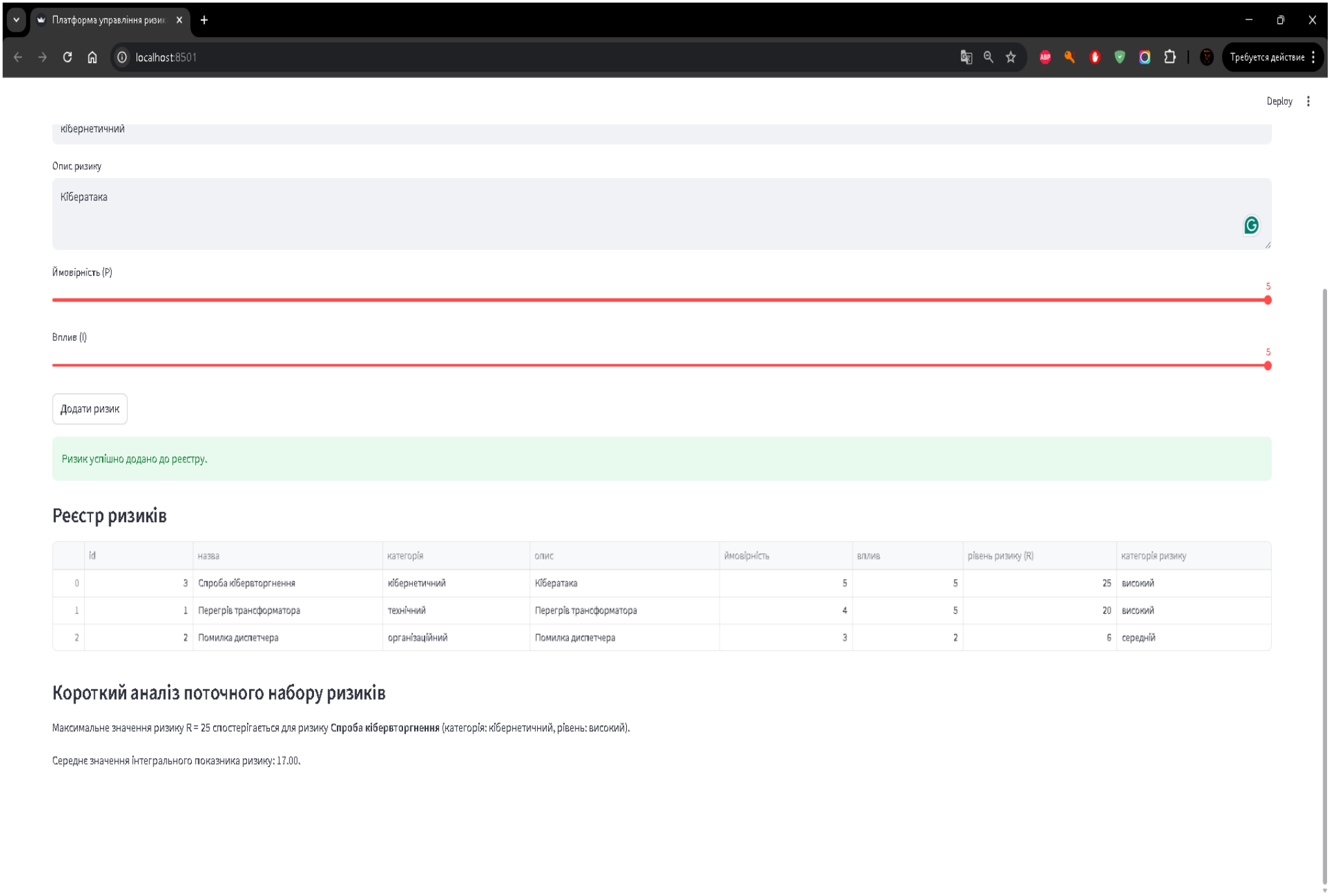

PythonProject
Version control
risk_app.py
27 def add_risk_record(name: str, 1 usage
41 "ймовірність": probability,
42 "вплив": impact,
43 "рівень ризику (R)": r_value,
44 "категорія ризику": risk_level
45 }
46
47 st.session_state["risks"].append(risk_record)
48 st.session_state["next_id"] += 1
49
50
51 def get_risks_dataframe() -> pd.DataFrame: 1 usage
52 """Отримання реєстру ризиків у вигляді DataFrame."""
53 if not st.session_state["risks"]:
54 return pd.DataFrame(
55 columns=[
56 "id",
57 "назва",
58 "категорія",
59 "опис",
60 "ймовірність",
61 "вплив",
62 "рівень ризику (R)",
63 "категорія ризику",
64]
65)
66 return pd.DataFrame(st.session_state["risks"])
67
68
69 def main(): 1 usage
70 """Головна функція веб-застосунку."""
71 init_session_state()
72
73 st.set_page_config(page_title="Платформа управління ризиками", layout="wide")
74 st.title("Цифрова платформа управління ризиками в енергетичному секторі")
75 st.write(
76 "Прототип веб-платформи для введення, оцінювання та аналізу ризиків "
77 "на основі спрощеної моделі R = P · I."
78)
79
Terminal
Local
PythonProject
risk_app.py

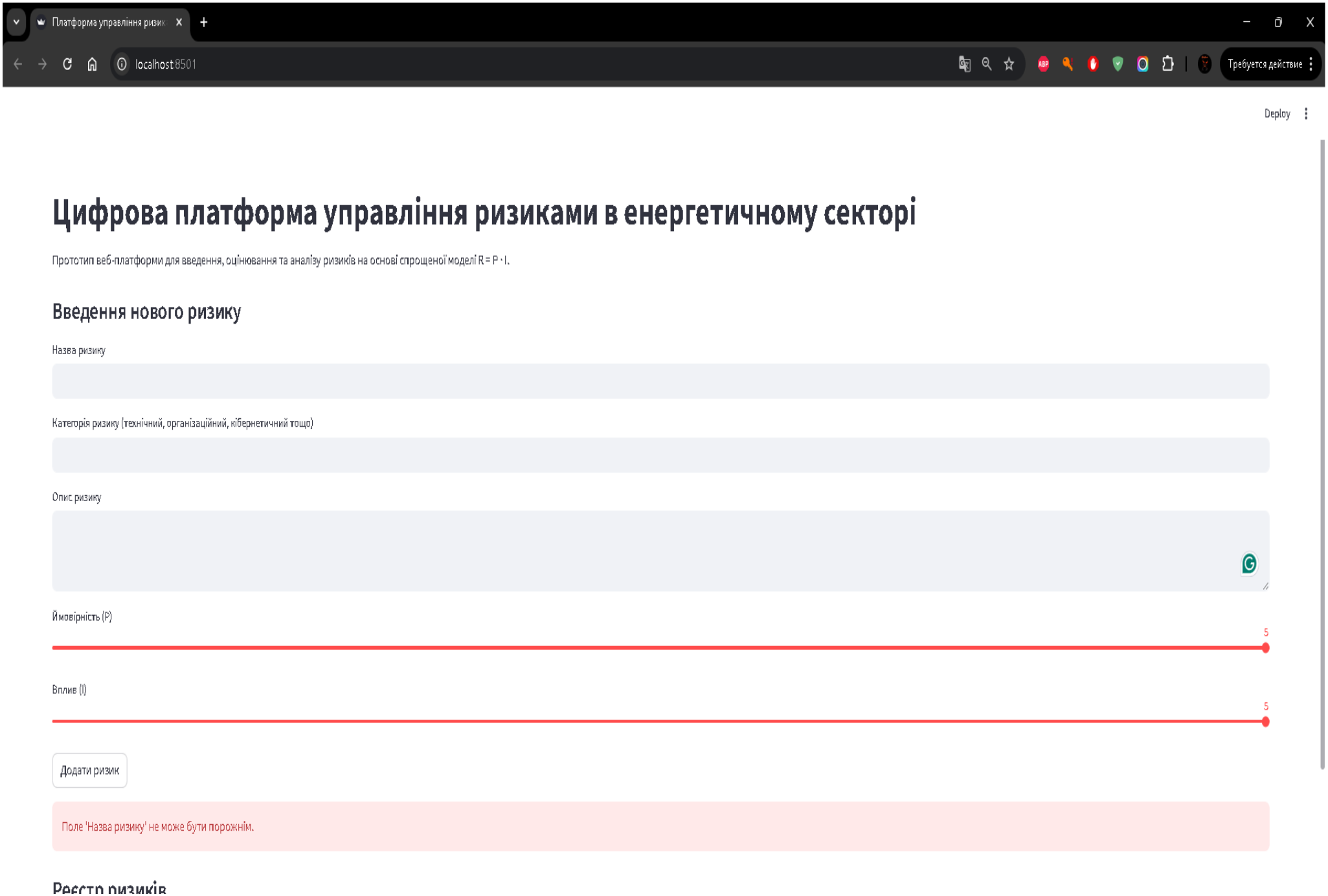

PythonProject
Version control
risk_app.py
def main(): 1 usage
st.subheader("Введення нового ризику")
name = st.text_input("Назва ризику")
category = st.text_input("Категорія ризику (технічний, організаційний, кібернетичний тощо)")
description = st.text_area("Опис ризику", height=120)
probability = st.slider("Ймовірність (P)", min_value=1, max_value=5, value=3)
impact = st.slider("Вплив (I)", min_value=1, max_value=5, value=3)
if st.button("Додати ризик"):
if not name.strip():
st.error("Поле 'Назва ризику' не може бути порожнім.")
elif not category.strip():
st.error("Поле 'Категорія ризику' не може бути порожнім.")
else:
add_risk_record(
name=name.strip(),
category=category.strip(),
description=description.strip(),
probability=int(probability),
impact=int(impact),
)
st.success("Ризик успішно додано до реєстру.")
st.subheader("Реєстр ризиків")
df_risks = get_risks_dataframe()
if df_risks.empty:
st.info("Реєстр ризиків поки що порожній. Додайте перший запис.")
else:
df_sorted = df_risks.sort_values(
by="рівень ризику (R)",
ascending=False
).reset_index(drop=True)
st.dataframe(df_sorted, use_container_width=True)
st.subheader("Короткий аналіз поточного набору ризиків")
Terminal
Local
PythonProject
risk_app.py


st.subheader("Короткий аналіз поточного набору ризиків")
max_risk = df_sorted.iloc[0]
st.write(
f"Максимальне значення ризику R = {max_risk['рівень ризику (R)']} "
f"спостерігається для ризику **{max_risk['назва']}** "
f"(категорія: {max_risk['категорія']}, рівень: {max_risk['категорія ризику']})."
)
avg_risk = df_sorted["рівень ризику (R)"].mean()
st.write(f"Середнє значення інтегрального показника ризику: {avg_risk:.2f}.")
if __name__ == "__main__":
main()
Terminal
Local
PythonProject
risk_app.py
10°C

ПРИКЛАДИ РЕЗУЛЬТАТІВ РОБОТИ ПРОГРАМИ




Платформа управління ризик
localhost:8501
Требуется действие
Deploy
кібернетичний
Опис ризику
Кібератака
Ймовірність (P)
5
Вплив (I)
5
Додати ризик
Ризик успішно додано до реєстру.
Реєстр ризиків
id
назва
категорія
опис
ймовірність
вплив
рівень ризику (R)
категорія ризику
0 3 Спроба кібервторгнення кібернетичний Кібератака 5 5 25 високий
1 1 Перегрів трансформатора технічний Перегрів трансформатора 4 5 20 високий
2 2 Помилка диспетчера організаційний Помилка диспетчера 3 2 6 середній
Короткий аналіз поточного набору ризиків
Максимальне значення ризику R = 25 спостерігається для ризику Спроба кібервторгнення (категорія: кібернетичний, рівень: високий).
Середнє значення інтегрального показника ризику: 17.00.


Платформа управління ризик
localhost:8501
Требуется действие
Deploy
Цифрова платформа управління ризиками в енергетичному секторі
Прототип веб-платформи для введення, оцінювання та аналізу ризиків на основі спрощеної моделі R = P · I.
Введення нового ризику
Назва ризику
Категорія ризику (технічний, організаційний, кібернетичний тощо)
Опис ризику
Ймовірність (P)
5
Вплив (I)
5
Додати ризик
Поле 'Назва ризику' не може бути порожнім.
Реєстр ризиків

ДОДАТОК Б

ПРЕЗЕНТАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-
КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

на тему: «Платформа управління ризиками в енергетичних компаніях»

Виконав студент групи САДМ-61
Яременко Юрій Вікторович
Керівник кваліфікаційної роботи:
Патракеєв Ігор Михайлович
к.т.н, доцент кафедри ІСТ

Київ 2026

1

Мета та завдання проекту

Мета магістерської роботи:
дослідження та розробка концепції цифрової платформи управління ризиками в енергетичних компаніях з використанням сучасних інформаційних технологій для підвищення стійкості, безпеки та ефективності управління.
Об'єкт дослідження:
процеси управління ризиками в енергетичному секторі в умовах цифрової трансформації та кіберфізичних систем.
Предмет дослідження:
методи, моделі та програмні засоби цифрової підтримки ідентифікації, оцінювання та аналізу ризиків в енергетичних компаніях.
Завдання проекту:
1. Дослідити теоретичні основи управління ризиками в енергетичних компаніях.
2. Проаналізувати існуючі інформаційні системи та підходи до автоматизації ризик-менеджменту.
3. Розробити прототипу платформи управління ризиками

2

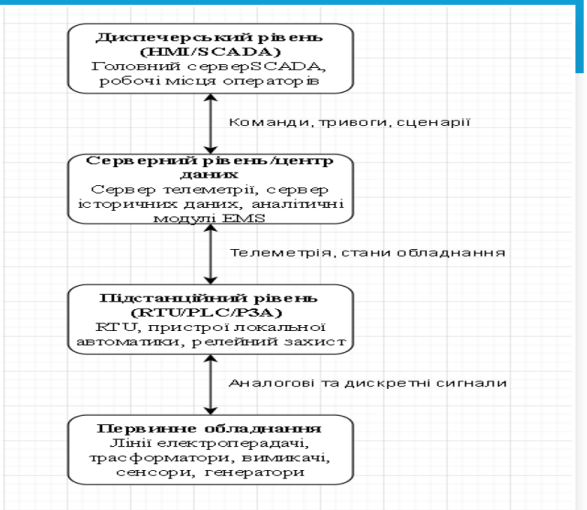
Актуальність:

Енергетичний сектор є однією з ключових складових критичної інфраструктури держави та відіграє вирішальну роль у забезпеченні економічної стабільності й національної безпеки. Умови цифрової трансформації енергетики супроводжуються зростанням обсягів технологічних, телеметричних та інформаційних даних, а також підвищенням рівня кібернетичних і техногенних загроз.Наявні підходи до управління ризиками в енергетичних компаніях часто є фрагментованими та не забезпечують комплексного аналізу взаємопов'язаних подій у реальному часі. Використання цифрових платформ дозволяє інтегрувати різнорідні джерела даних, автоматизувати процеси ідентифікації та оцінювання ризиків, а також підвищити оперативність прийняття управлінських рішень.Застосування сучасних інформаційних технологій у сфері ризик-менеджменту створює передумови для підвищення стійкості енергетичної інфраструктури, зниження ймовірності аварійних ситуацій та мінімізації їхніх наслідків, що визначає актуальність даної магістерської роботи.

3

Структура сучасної енергетичної інфраструктури та рівні управління

- Багаторівнева структура управління енергетичною інфраструктурою, що включає рівні виробництва, передачі, розподілу та диспетчерського управління, а також взаємодію технологічних і інформаційних компонентів.



4

Взаємодія ключових інформаційних систем енергетичної компанії (SCADA, EMS, SOC/SIEM)

- Взаємодія інформаційних систем SCADA, EMS та SOC/SIEM, що забезпечують моніторинг технологічних процесів, оперативне управління енергосистемою та підтримку кібербезпеки.

5

Основні обмеження та недоліки існуючих підходів до управління ризиками

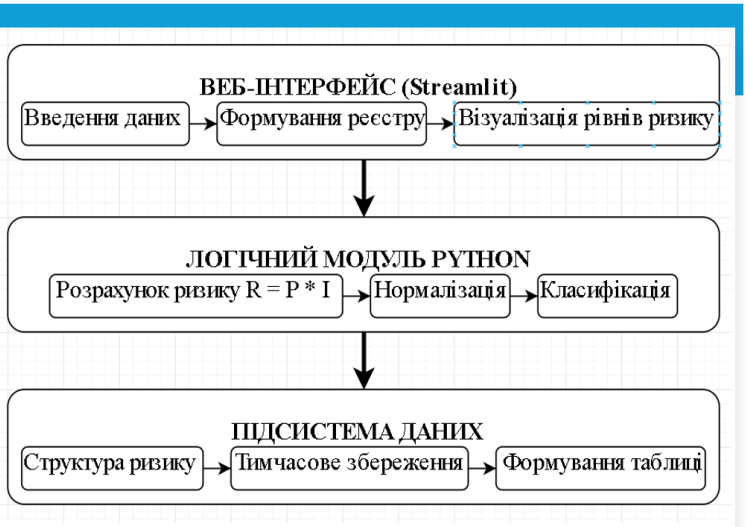
- Ключові недоліки традиційних підходів до управління ризиками, зокрема фрагментованість даних, низький рівень автоматизації та обмежені можливості аналізу в реальному часі.

Джерело ризику	Характеристика	Потенційні наслідки
Телеметрія	Затримка, втрата, спотворення вимірювань	Хибні рішення, некоректні режими
Канали зв'язку	Збої, нестабільність, кібератаки	Втрата керованості, відсутність даних
Програмне забезпечення	Вразливості, помилки в алгоритмах	Несанкціонований доступ, помилкові команди
Людський фактор	Помилки операторів, некоректне втручання	Неправильні перемикання, посилення аварій
Моделі EMS	Невідповідність реальним умовам, спрощення	Некоректний аналіз стійкості та оптимізації

6

Архітектура цифрової платформи управління ризиками в енергетичних компаніях

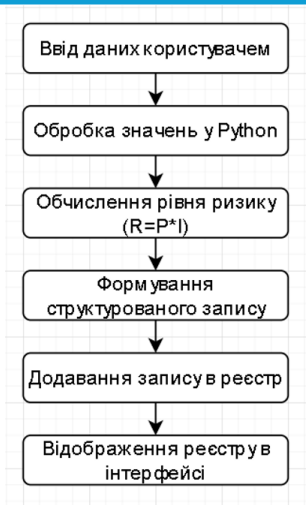
- Модульна архітектура цифрової платформи управління ризиками, що охоплює процеси збору даних, аналітичної обробки, оцінювання ризиків та формування управлінської звітності.



Модель даних та процес оцінювання ризиків

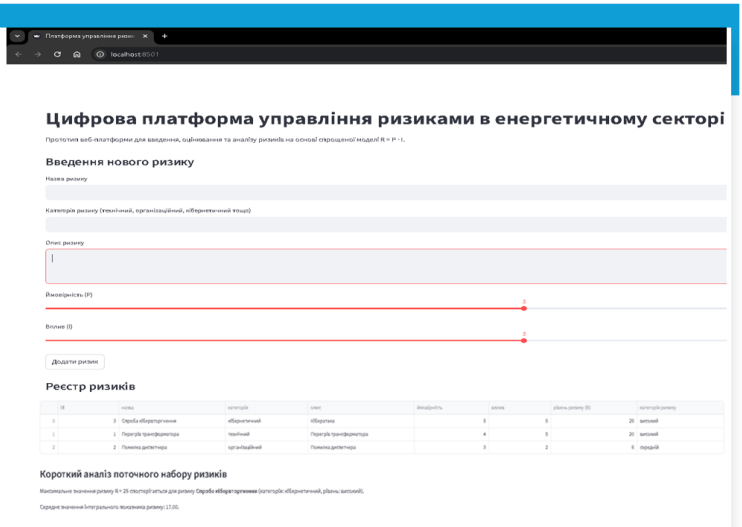
Поле	Опис
id	Унікальний ідентифікатор ризику
назва	Стисла назва ризику
категорія	Технічна, організаційна, кібернетична тощо
опис	Характеристика джерела ризику
ймовірність	Значення від 1 до 5
вплив	Значення від 1 до 5
рівень ризику	Результат обчислення $R = P \cdot I$

- Модель даних платформи та послідовність процесу оцінювання ризиків, що включає ідентифікацію загроз, визначення ймовірності, оцінку впливу та розрахунок інтегрального показника ризику.



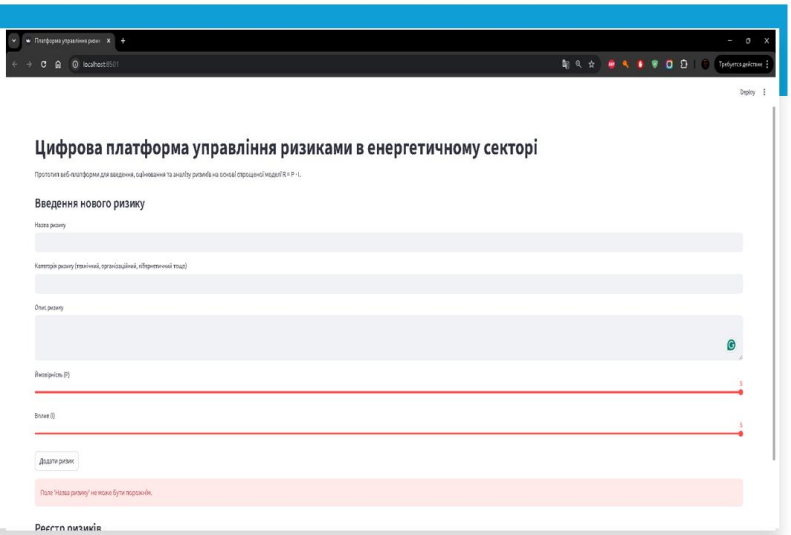
Програмна реалізація прототипу цифрової платформи

- Інтерфейс програмного прототипу цифрової платформи управління ризиками, що забезпечує введення даних, аналіз ризиків та візуалізацію результатів.



Результати тестування програмного прототипу

- Результати тестування програмного прототипу цифрової платформи, що підтверджують коректність роботи алгоритмів та стабільність функціонування системи.



Формування реєстру ризиків та результати аналізу

Реєстр ризиків

	Id	назва	категорія	опис	ймовірність	вплив	рівень ризику (R)	категорія ризику
0	3	Спроба кібервторгнення	кібернетичний	Кібератака	5	5	25	високий
1	1	Перегрів трансформатора	технічний	Перегрів трансформатора	4	5	20	високий
2	2	Помилка диспетчера	організаційний	Помилка диспетчера	3	2	6	середній

Короткий аналіз поточного набору ризиків

Максимальне значення ризику R = 25 спостерігається для ризику **Спроба кібервторгнення** (категорія: кібернетичний, рівень: високий).

Середнє значення інтегрального показника ризику: 17.00.

- Приклад сформованого реєстру ризиків та результати їх аналізу з використанням цифрової платформи управління ризиками.

11

ВИСНОВКИ

- Досліджено особливості управління ризиками в енергетичних компаніях в умовах цифрової трансформації.
- Встановлено, що сучасна енергетична інфраструктура характеризується високою складністю та зростанням технічних і кібернетичних загроз.
- Проаналізовано існуючі підходи до управління ризиками та виявлено їх фрагментованість і обмеженість аналітичних можливостей.
- Запропоновано концепцію цифрової платформи управління ризиками з модульною архітектурою.
- Розроблено програмний прототип платформи, що забезпечує формування реєстру ризиків та автоматичний розрахунок інтегрального показника ризику.
- Проведено тестування прототипу, результати якого підтвердили коректність реалізованих алгоритмів і працездатність системи.
- Отримані результати підтверджують доцільність використання цифрових платформ управління ризиками в енергетичному секторі.

АПРОБАЦІЯ

III всеукраїнська науково-технічна конференція «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу», на теми:

1. «Інтелектуальна платформа аналізу та управління ризиками в енергетичному секторі» ст. 137, 18 листопада 2025 року.
2. «Використання інформаційних технологій для управління ризиками в енергетичних компаніях» ст. 249, 18 листопада 2025 року.

12