

# КЛАСИФІКАЦІЯ РИЗИКІВ В АСПЕКТІ ФОРМУВАННЯ ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ЕНЕРГЕТИЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ

©2024 ПРОХОРОВА В. В., МИХАЛЬЧЕНКО Г. Г., БУДАНОВ М. П.

UDK 620.91(477):005.334

JEL: D81; L94

## Прохорова В. В., Михальченко Г. Г., Буданов М. П. Класифікація ризиків в аспекті формування організаційно-економічного забезпечення управління енергетичною безпекою підприємств

У статті розглянуто класифікацію ризиків у контексті формування організаційно-економічного забезпечення управління енергетичною безпекою промислових підприємств електроенергетичної системи. У ході дослідження показано, що ризики виникають на всіх етапах енергетичного циклу: від генерації до передачі, транспортування, розподілу та споживання енергії. Запропонована класифікація ризиків передбачає їх поділ на виробничі, фінансово-економічні та інформаційні, що сприяє детальному аналізу та оцінці їхнього впливу на енергетичну безпеку підприємств. Основна мета роботи полягає в удосконаленні класифікації ризиків з метою підвищення ефективності організаційно-економічного забезпечення управління енергетичною безпекою. У результаті досліджень було проведено ранжування ризиків за видами, а також конкретних загроз, притаманних кожному етапу енергетичного виробництва. Ризики енергетичної безпеки класифіковано на макро-, мезо- та мікрорівнях, що дозволило детально вивчити їхній вплив на різних рівнях економічної діяльності. Такий підхід забезпечує комплексну оцінку стану енергобезпеки підприємств в умовах як внутрішніх, так і зовнішніх факторів. Досліджено проблеми функціонування підприємств в умовах нестабільного економічного середовища, проведено теоретичний і практичний аналіз ризиків та факторів, що впливають на їхню інтенсивність. Показано, що ефективне управління ризиками є критично важливим для забезпечення стабільної роботи підприємства, оскільки висока динаміка зовнішнього середовища суттєво підвищує ймовірність виникнення загроз, що можуть мати негативний вплив на виробничі процеси. На основі проведеного дослідження запропоновано комплексний підхід до мінімізації впливу потенційних загроз, зокрема шляхом упровадження системи раннього виявлення ризиків та оперативного реагування на них. Зроблено висновок, що одним із найважливіших факторів, який впливає на ефективність підприємства та рівень його енергетичної безпеки, є швидка адаптація до змін у зовнішньому середовищі. Запропоновані підходи можуть бути використані керівниками енергетичних підприємств для оптимізації управлінських рішень у сфері забезпечення енергетичної безпеки.

**Ключові слова:** енергетична безпека, ризики, класифікація ризиків, енергопідприємство, загрози.

Табл.: 3. Бібл.: 11.

**Прохорова Вікторія Володимирівна** – доктор економічних наук, професор, завідувачка кафедри економіки та менеджменту, Навчально-науковий інститут «Українська інженерно-педагогічна академія» Харківського національного університету імені В. Н. Каразіна (вул. Університетська, 16, Харків, 61003, Україна)

E-mail: [vkprohkorova@gmail.com](mailto:vkprohkorova@gmail.com)

ORCID: <https://orcid.org/0000-0003-2552-2131>

Researcher ID: <https://www.webofscience.com/wos/author/record/2000787>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57203623016>

**Михальченко Ганна Григорівна** – доктор економічних наук, професор, завідувачка кафедри економіки підприємств та менеджменту, Бахмутський навчально-науковий професійно-педагогічний інститут Харківського національного університету імені В. Н. Каразіна (майдан Свободи, 4, Харків, 61022, Україна)

E-mail: [mikhalchenko@i.ua](mailto:mikhalchenko@i.ua)

ORCID: <https://orcid.org/0000-0003-2616-9499>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57220197412>

**Буданов Микола Павлович** – здобувач ступеня доктора філософії, Навчально-науковий інститут «Українська інженерно-педагогічна академія» Харківського національного університету імені В. Н. Каразіна (вул. Університетська, 16, Харків, 61003, Україна)

E-mail: [pavelfeofanovich@ukr.net](mailto:pavelfeofanovich@ukr.net)

ORCID: <https://orcid.org/0000-0001-8032-0562>

UDC 620.91(477):005.334

JEL: D81; L94

## Prokhorova V. V., Mykhalchenko H. H., Budanov M. P. Classification of Risks in the Aspect of Formation of Organizational and Economic Support for Energy Security Management of Enterprises

The article considers the classification of risks in the context of the formation of organizational and economic support for energy security management of industrial enterprises of the electric power system. The study shows that risks arise at all stages of the energy cycle: from generation to transmission, transportation, distribution, and consumption of energy. The proposed classification of risks provides for their division into production, financial, economic, and informational risks, thus contributing to a detailed analysis and assessment of their impacts on the energy security of enterprises. The main aim of the article is to improve the classification of risks in order to increase the efficiency of organizational and economic support for energy security management. As result of researches, a ranking of risks by types, as well as specific threats inherent in each stage of energy production, was carried out. Energy security risks are classified at macro-, meso- and micro-levels, which made it possible to study in detail their impact at different levels of economic activity. This approach provides a comprehensive

assessment of the state of energy security of enterprises in the face of both internal and external factors. Problematic issues of functioning of enterprises in an unstable economic environment are studied, a theoretical and practical analysis of risks and factors influencing their intensity is carried out. It is shown that efficient risk management is critically important for ensuring the stable operation of the enterprise, since the high dynamics of the external environment significantly increases the likelihood of threats that can have a negative impact on production processes. On the basis of the carried out study, an integrated approach to minimizing the impact of potential threats is proposed, in particular through the introduction of a system for early detection of risks and prompt response to them. It is concluded that one of the most important factors influencing the efficiency of enterprise and the level of its energy security is rapid adaptation to changes in the external environment. The proposed approaches can be used by managers of energy enterprises to optimize management decisions in the field of energy security.

**Keywords:** energy security, risks, classification of risks, energy enterprise, threats.

**Tabl.:** 3. **Bibl.:** 11.

**Prokhorova Viktoriia V.** – D. Sc. (Economics), Professor, Head of the Department of Economics and Management, Educational and Scientific Institute "Ukrainian Engineering and Pedagogical Academy" of V. N. Karazin Kharkov National University (16 Universytetska Str., Kharkiv, 61003, Ukraine)

**E-mail:** vkprokhorova@gmail.com

**ORCID:** <https://orcid.org/0000-0003-2552-2131>

**Researcher ID:** <https://www.webofscience.com/wos/author/record/2000787>

**Scopus Author ID:** <https://www.scopus.com/authid/detail.uri?authorId=57203623016>

**Mykhalchenko Hanna H.** – D. Sc. (Economics), Professor, Head of the Department of Business Economics and Management, Bakhmut Education Research and Professional Pedagogical Institute of V. N. Karazin Kharkiv National University (4 Svobody Square, Kharkiv, 61022, Ukraine)

**E-mail:** mikhcalchenko@i.ua

**ORCID:** <https://orcid.org/0000-0003-2616-9499>

**Scopus Author ID:** <https://www.scopus.com/authid/detail.uri?authorId=57220197412>

**Budanov Mykola P.** – Graduate of the degree of Doctor of Philosophy, Educational and Scientific Institute "Ukrainian Engineering and Pedagogical Academy" of V. N. Karazin Kharkov National University (16 Universytetska Str., Kharkiv, 61003, Ukraine)

**E-mail:** pavelfeofanovich@ukr.net

**ORCID:** <https://orcid.org/0000-0001-8032-0562>

Підприємство електроенергетичної системи є основною структуротворною ланкою економіки, оскільки саме на ньому зосереджені трудові, матеріальні та фінансові ресурси для виробництва продукції. Енергопідприємство є основним джерелом задоволення потреб суспільства в товарах і послугах, місцем застосування сил більшості працездатного населення країни. Проте ситуація ускладнюється тим, що періодично повторюються фінансово-економічні кризи, які обумовлені як внутрішніми, так і зовнішніми негативними факторами у вигляді загроз і ризиків енергобезпеці.

Це визначає актуальність розробки методичних питань до виходу енергопідприємств із кризових ситуацій, обумовлених як внутрішніми, так і зовнішніми ризиками, із якими стикаються підприємства електроенергетичної системи на макро-, мезо- і мікрорівнях економіки.

Виходячи з аналізу практики функціонування енергопідприємств за умов невизначеності необхідно розробити практичні рекомендації щодо прийняття управлінських рішень при виборі стратегічних напрямів діяльності підприємства з урахуванням усіх особливостей господарського, адміністративного та нормативно-правового середовища, в якому діє енергопідприємство. Актуальність зазначеної проблематики підтверджується і тим, що навіть найуспішніші підприємства знаходяться у своєрідній «зоні ризику», що стримує вихід економіки з кризового стану.

Отже, функціонування енергопідприємства в умовах впливу зовнішніх факторів постійно нара-

жається на небезпеку зриву або погіршення ситуації через можливе порушення фінансових або матеріально-сировинних потоків, а також ринків збуту. Така ситуація не може не впливати на стан рівня енергобезпеки підприємств електроенергетичної системи на макро-, мезо- та мікрорівнях економіки.

У рамках даного дослідження проведено класифікацію наявних ризиків енергетичної безпеки підприємств електроенергетичної системи на макро-, мезо- та мікрорівнях на основі таких критеріїв: стадії технологічного процесу енергетичного виробництва (генерація, передача, розподіл та споживання енергії), які залежно від джерел ризику об'єднані у групи виробничих, фінансово-економічних та інформаційних ризиків. Основою класифікації послужили систематизовані за вищезазначеними критеріями результати, одержані під час аналізу літературних джерел [1–9].

Цілий ряд сучасних досліджень науковців присвячується різним проблемам впливу ризиків на стан енергетичної безпеки підприємств.

У роботах [1–3] аналізуються нові підходи до управління попитом на енергію як способу підвищення енергетичної безпеки і стійкості, що включає методи зменшення споживання енергії та інтеграцію відновлювальних джерел в енергетичну мережу для зниження ризиків перебоїв з постачанням. Крім того, розглядаються кібернетичні ризики, які загрожують енергетичному сектору, зокрема атаки на критичну інфраструктуру та дані. При цьому оцінюється вплив таких за-

гроз на безпеку підприємств і пропонуються стратегії для посилення кіберзахисту.

У роботі [4] пропонується методологічний підхід до інтеграції ризиків кліматичних змін в управлінні енергетичною безпекою, що включає приклади з реального життя, які демонструють, як зміни клімату можуть вплинути на енергетичні системи і які стратегії можна застосувати для адаптації.

У роботі [5] проводиться оцінка ризиків енергетичної безпеки в умовах переходу до відновлюваних джерел енергії, а також розглядаються виклики та можливості, пов'язані з переходом на нові технології, та пропонуються напрямки для подальших досліджень у цій сфері.

У роботі [6] досліджується вплив геополітичних ризиків на енергетичну безпеку у країнах, що розвиваються, а також аналізуються політичні й економічні факторів, які можуть вплинути на стабільність постачання енергії та стратегії адаптації для країн з ринками, що розвиваються.

Огляд теоретичних і практичних аспектів стійкості в контексті енергетичної безпеки, зокрема на промислових підприємствах, зроблено в роботі [7], що включає методи та стратегії для поліпшення стійкості енергетичних систем до різних видів ризиків.

У роботах [8] аналізуються сучасні методи оцінки ризиків енергетичної безпеки і тенденції розвитку в цій сфері та взаємодія між ринковими структурами та ризиками постачання енергії, а також розглядаються новітні підходи до моделювання і прогнозування ризиків та їх вплив на енергетичні системи для оцінки того, як різні типи ринкових структур можуть впливати на безпеку енергетичних постачань.

У роботі [9] проводиться оцінка ролі технологічних інновацій у зменшенні ризиків енергетичної безпеки, а також розглядається новітні технології, такі як розумні мережі та системи збереження енергії, які можуть поліпшити стійкість енергетичних систем.

У рамках аналізу останніх досліджень [1–9] можна відзначити, що наявні роботи охоплюють різні аспекти енергетичної безпеки: від управління попитом на енергію та інтеграції відновлювальних джерел до кібернетичних ризиків і впливу кліматичних змін. Однак недостатньо досліджено питання інтеграції цих аспектів у єдину систему управління ризиками, що ускладнює практичне застосування теоретичних напрацювань.

З метою вдосконалення управління енергобезпекою підприємств дане дослідження має на меті уточнити класифікацію ризиків та запропонувати потенційні рішення для їх уникнення. Це до-

зволить не лише підвищити стійкість енергетичних систем до різноманітних ризиків, але й сприятиме стабільному функціонуванню енергетичних підприємств в умовах зовнішніх і внутрішніх викликів.

Незважаючи на наявні дослідження, існують кілька невирішених аспектів проблеми. По-перше, недостатньо уваги приділено розробці практичних рекомендацій для управління енергетичними підприємствами в умовах невизначеності, що включає формування стратегічних напрямів діяльності з урахуванням особливостей господарського, адміністративного та нормативно-правового середовища. По-друге, існує потреба в удосконаленні класифікації ризиків, що дозволить краще адаптувати управлінські рішення до специфічних умов енергетичних підприємств.

Для вдосконалення управління енергобезпекою підприємств дане дослідження спрямоване на уточнення класифікації ризиків і розробку потенційних рішень для їх уникнення. Це сприятиме не тільки підвищенню стійкості енергетичних систем до різних загроз, але й забезпечить стабільну роботу енергетичних підприємств в умовах зовнішніх та внутрішніх викликів.

Тому метою статті є вдосконалення класифікації ризиків в аспекті формування організаційно-економічного забезпечення управління енергобезпекою підприємства та визначення потенційних можливостей їх уникнення.

Виходячи з поставленої мети дослідження можна виділити кілька ключових завдань, які слід вирішити:

1. *Аналіз сучасних підходів до управління ризиками в енергетичній безпеці:* провести комплексний огляд наявних методів та стратегій управління ризиками, які застосовуються в енергетичному секторі. Це включає аналіз практик, які вже використовуються, та виявлення їхніх слабких місць і недоліків.
2. *Розробка вдосконаленої класифікації ризиків для енергетичних підприємств:* уточнити класифікацію ризиків з урахуванням специфіки діяльності енергетичних підприємств. Це дозволить краще розподілити ризики за категоріями та визначити їхній вплив на різні рівні економіки (макро-, мезо- і мікрорівень).

Ці завдання спрямовані на розв'язання проблем у сфері енергетичної безпеки, поліпшення управління ризиками та забезпечення стійкості енергетичних систем в умовах сучасних викликів.

Методика проведення дослідження включає:

- ♦ огляд наявних досліджень (вивчити сучасні підходи до управління ризиками в енерге-

тичній безпеці, виявити вже наявні методи та їхні недоліки, зібрати та проаналізувати наукові роботи, статті, звіти та інші джерела інформації, що стосуються теми дослідження);

- ✦ аналіз наявних підходів та виявлення проблем (оцінити ефективність наявних методик управління ризиками та виявити їхні слабкі місця, провести порівняльний аналіз методів управління ризиками, виявити їхні недоліки та обмеження, а також визначити, які аспекти енергетичної безпеки не отримали достатньої уваги);
- ✦ розробка вдосконаленої класифікації ризиків (уточнити класифікацію ризиків, що стосуються енергетичних підприємств, і розробити нову або вдосконалену класифікацію ризиків, яка відображає специфіку діяльності енергетичних підприємств, визначити критерії класифікації та розподілити ризики за категоріями (фінансові, технологічні, геополітичні, тощо);
- ✦ розробка практичних рекомендацій (сформулювати практичні рекомендації для управлінських рішень у контексті управління ризиками та розробити рекомендації щодо стратегічного планування, управління фінансовими та матеріально-сировинними потоками, урахувавши специфіку господарського, адміністративного та нормативно-правового середовища);
- ✦ оцінка впливу ризиків на енергетичну безпеку (визначити, як різні типи ризиків впливають на енергетичну безпеку підприємств і провести аналіз впливу внутрішніх і зовнішніх ризиків на енергетичну безпеку, а також оцінити потенційні сценарії кризових ситуацій і їх наслідки).

Ця методика дозволяє системно підходити до розв'язання проблем енергетичної безпеки, забезпечуючи детальний аналіз наявних підходів, розробку нових класифікацій ризиків, а також перевірку їх практичної ефективності.

**З**абезпечення енергетичної безпеки промислового підприємства є важливим фактором розвитку електроенергетичної системи та особливо значуще як складова її економічної безпеки на макро-, мезо- та мікрорівнях економіки України [10].

Процес дослідження проблеми управління енергетичною безпекою тісно пов'язаний з попереднім визначенням і класифікацією загроз енергобезпеці та їх оцінкою за допомогою окремих показників та інтегральних індексів, де загрози

згруповані в блоки енергетичної самостійності, диверсифікації видів та надійності постачання енергоресурсів, а також енергетичної ефективності їх кінцевого споживання [11].

Слід зазначити, що різні загрози є основою ризиків енергетичної безпеки, та з урахуванням особливостей виявлених основних ризиків пропонується класифікувати їх на ризики виробничого, фінансово-економічного та інформаційного характеру на всіх етапах енергетичного виробництва: генерації, передачі (транспортування), розподілу та споживання енергії.

**Р**озглянемо підхід до класифікації ризиків енергобезпеки підприємства електроенергетичної системи на макро-, мезо- та мікрорівнях економіки.

З метою ефективної розробки напрямів щодо формування стратегії енергетичної безпеки підприємства пропонується розглянути загрози та ризики енергобезпеки з урахуванням їхньої значущості на всіх етапах енергетичного виробництва з оцінкою їх впливу на стійкий економічний розвиток електроенергетичної системи на макро-, мезо- та мікрорівнях економіки.

Для реалізації цієї мети була виконана класифікація наявних ризиків енергетичної безпеки підприємства електроенергетичної системи на макро-, мезо- та мікрорівнях економіки України за двома критеріями: стадії енергетичного виробництва та джерела ризиків, де джерела ризиків на кожній стадії енергетичного виробництва (генерація, передача, розподіл, споживання енергії) були об'єднані в групи (види): виробничі ризики; фінансово-економічні ризики; ризики використання інформаційних технологій (інформаційні ризики).

Слід зазначити, що різні джерела ризиків (технологічний процес, фінансово-економічна діяльність, застосування інформаційних технологій) кожної стадії енерговиробництва приводять до різних ризиків.

Аналіз наукових праць [1–9] дозволив усі ризики систематизувати з урахуванням таких основних критеріїв:

1. *Ризики енергетичної безпеки підприємства електроенергетичної системи на стадії технологічного процесу «Генерація енергії».* Основним етапом енергетичного виробництва є виробництво електричної та теплової енергії шляхом перетворення її з інших видів енергії як традиційними, так і альтернативними генерувальними технічними пристроями.

У зв'язку з цим доцільно запропонувати класифікацію ризиків енергетичної безпеки підприємства за джерелами їх походження на стадії технологічного процесу «Генерація енергії» (табл. 1).

**Класифікація ризиків енергетичної безпеки підприємства електроенергетичної системи  
за джерелами ризиків на стадії процесу «Генерація енергії»**

Вид ризику	Зміст ризику на стадії процесу «Генерація енергії»
1	2
1. Виробничі ризики	1.1. Знос основних засобів
	1.2. Зниження завантаження власних потужностей, що генерують (наприклад, у зв'язку з виведенням з експлуатації ЗАЕС)
	1.3. Необхідність підтримки резервів потужності (наприклад, у зв'язку з виведенням з експлуатації ЗАЕС)
	1.4. Несвоєчасне введення об'єктів резервування потужностей (наприклад, у зв'язку з позаплановим режимом зупинки ЗАЕС)
	1.5. Створення споживачами власної генерації та залучення їх до регулювання навантажень (наприклад, створення сонячних фотоелектричних установок (СФЕУ) та сонячної електростанції (СЕС))
	1.6. Зниження надійності роботи обладнання (наприклад, збільшення відмов технологічного обладнання енергоблоку електростанції)
	1.7. Аварії та відмови в роботі технологічного обладнання у зв'язку з помилковими діями оперативного персоналу (наприклад, оператор автоматизованого робочого місця (АРМ) автоматизованої системи управління технологічними процесами (АСУТП) енергоблоку прийняв помилкове управлінське рішення на відхилення від норми параметрів технологічного процесу генерації енергії)
	1.8. Низький коефіцієнт використання встановленої потужності технологічного обладнання енергоблоку електростанції
	1.9. Диверсії та терористичні акти (наприклад, захоплення російськими військами території ЗАЕС)
	1.10. Негативна дія на навколишнє середовище (наприклад, викид відпрацьованого ядерного палива за межі ядерного реактора)
2. Фінансово-економічні ризики	2.1. Зростання вартості основних паливно-енергетичних ресурсів
	2.2. Зниження прибутковості «Обленерго» через зменшення завантаження власних генерувальних потужностей
	2.3. Дефіцит оборотних засобів та інвестицій
	2.4. Різна рентабельність регіональних (обласних) енергосистем
	2.5. Зростання вартості ремонтних робіт підрядних організацій
	2.6. Зростання собівартості валової відпустки (наприклад, через зниження обсягів вироблення електроенергії від власних джерел регіональних (обласних) енергосистем у зв'язку з виведенням з експлуатації ЗАЕС)
	2.7. Високі витрати на утримання допоміжних ремонтних цехів та об'єктів
	2.8. Високі витрати на утримання технічних систем, а також іншого допоміжного обладнання та спецмеханізмів
	3.1. Низький рівень інформатизації (цифровізації) управління генерувальним технологічним обладнанням
	3.2. Відмови та збої в роботі об'єктів інформатизації, що безпосередньо управляють генерувальним обладнанням
	3.3. Відмови або збої в роботі об'єктів інформатизації, які безпосередньо керують обладнанням розподільчих пристроїв електростанцій
	3.4. Відмови або збої в роботі об'єктів інформатизації, які безпосередньо управляють енергооб'єктами центральної диспетчерської служби
	3.5. Відмови або збої в роботі об'єктів інформатизації, які безпосередньо управляють обладнанням контролю шкідливих викидів в атмосферу
	3.6. Різномірність використання програмних та апаратних засобів у новозбудованих автоматизованих системах управління технологічними процесами (АСУ ТП)
	3.7. Цифрова залежність від технологій та від постачальників цих технологій
	3.8. Несумісність терміну експлуатації технічних засобів АСУ ТП та основного технологічного обладнання

1	2
	3.9. Невідповідність засобів інформаційної безпеки впровадженим інформаційним рішенням
	3.10. Неякісне виконання проєкту з первинної розробки алгоритму управління техпроцесом
	3.11. Несанкціоновані дії та хакерські кібератаки
	3.12. Недостатній рівень кваліфікації персоналу
	3.13. Відсутність на підприємствах спеціальних систем контролю, які відповідають за інформаційну безпеку

**Джерело:** складено авторами на основі [1–11].

Дані табл. 1 дозволяють зробити висновок, що найважливішими на стадії «Генерація енергії» для енергопідприємств більшості регіональних (обласних) енергосистем є виробничі ризики енергобезпеки підприємства. Особливо значущими є ризик підвищеного зносу основних виробничих засобів і зниження завантаження власних генерувальних потужностей (наприклад, у зв'язку з виведенням з експлуатації ЗАЕС), де в першому випадку при збільшенні зносу вище 45% даний ризик негативно впливає на надійність поставок електричної та теплової енергії споживачам енергії, а в другому випадку можуть збільшитися питомі витрати палива на виробництво теплової та електричної енергії через неоптимальний режим роботи генерувального обладнання. До найменш важливих виробничих ризиків можна віднести низький коефіцієнт використання встановленої потужності з енергооб'єктів на мезорівні, зважаючи на скорочення промислових споживачів електричної та теплової енергії, та створення децентралізованих джерел електро- та тепlopостачання, обумовлених трансформацією української енергосистеми.

Результат аналізу значущості фінансових ризиків на даній стадії енерговиробництва показав, що цьому виду ризиків особливе значення надають підприємства електроенергетичної системи на макро- та мезорівнях, а найбільш важливими ризиками для всіх енергетичних об'єктів енергосистем є зростання вартості основних паливно-енергетичних ресурсів, які становлять 70–80% у витратах на пальне, що може призвести до підвищення тарифів для реального сектора економіки та неконкурентоспроможності енергоємних підприємств ЕЕС, а також провокувати появу виробничого ризику щодо створення споживачами власної генерації. Також до найважливіших ризиків необхідно віднести зниження прибутковості об'єктів ЕЕС, зважаючи на зменшення завантаження власних генерувальних потужностей (наприклад, у зв'язку з виведенням з експлуатації ЗАЕС). Незначними

фінансовими ризиками визнано високі витрати на утримання допоміжних ремонтних цехів та різних об'єктів спецобладнання та механізмів.

До групи ризиків, пов'язаних із використанням інформаційних технологій, належать відмови та збої в роботі систем, які управляють технологічним обладнанням. Особливу значущість мають проблеми з обладнанням електростанцій, які відповідають за генерацію та розподіл електричної енергії. Такі збої можуть призвести до недостатнього постачання енергії споживачам. До незначних інформаційних ризиків віднесено відмови або збої в роботі об'єктів інформатизації, які безпосередньо керують технологічним обладнанням контролю шкідливих викидів в атмосферу.

2. *Ризики енергетичної безпеки підприємств електроенергетичної системи на стадії технологічного процесу «Передача енергії».* Важливою стадією енергетичного виробництва є передача (транспортування) енергії через лінії електропередачі високої напруги.

У табл. 2 наведено класифікацію передбачуваних ризиків енергетичної безпеки підприємства електроенергетичної системи на стадії технологічного процесу «Передача енергії».

Дані табл. 2 дозволяють зробити висновок, що найбільш важливими ризиками енергобезпеки підприємства на стадії «Передача енергії» для електроенергетичної системи на макро- та мезорівнях є виробничі ризики, з яких найважливіший ризик – знос основних засобів технологічного обладнання. Для цього особливо важливим необхідно вважати додаткове електромережеве будівництво міжсистемних зв'язків на макро- та мезорівнях електроенергетичної системи.

Інформаційними ризиками високого рівня на стадії «Передача енергії» можуть бути визначені відмови або збої в роботі об'єктів інформатизації, які безпосередньо керують технологічним обладнанням підстанцій, а також у системах управління енергооб'єктами центральної диспетчерської служби. До найменш важливих інформаційних

**Класифікація ризиків енергетичної безпеки підприємства електроенергетичної системи за джерелами ризиків на стадії процесу «Передача енергії»**

Вид ризику	Зміст ризику на стадії процесу «Передача енергії»
1. Виробничі ризики	1.1. Зношування основних засобів
	1.2. Збільшення необхідних резервів установленої потужності (наприклад, через виведення з експлуатації ЗАЕС)
	1.3. Необхідність додаткового електромережевого будівництва міжсистемних зв'язків (наприклад, з причин збільшення необхідних резервів установленої потужності пп. 2.1.2)
	1.4. Низький рівень автоматизації (цифровізації) електромереж
	1.5. Аварії та відмови в роботі технологічного обладнання енергоблоку електростанції у зв'язку з помилковими діями оперативного персоналу
	1.6. Збільшення частки втрат у разі зниження обсягів промислового виробництва
	1.7. Зниження надійності роботи електромережі через погодні та сезонні умови
	1.8. Недостатній рівень резервування найбільших джерел генерації в електроенергетичній системі на макро- і мезорівнях
	1.9. Зростання навантажувальних втрат при транспортуванні електричної та теплової енергії
	1.10. Диверсії та терористичні акти (наприклад, захоплення російськими військами території ЗАЕС)
2. Фінансово-економічні ризики	2.1. Різна рентабельність підприємств електроенергетичної системи на макро- та мезорівнях економіки
	2.2. Дефіцит обігових засобів та інвестицій
	2.3. Відсутність джерел фінансування на реконструкцію мереж
	2.4. Зростання вартості ремонтних робіт підрядних організацій
	2.5. Високі витрати на утримання допоміжних ремонтних цехів та об'єктів
	2.6. Високі витрати на утримання автотранспорту та спецмеханізмів
3. Інформаційні ризики	3.1. Низький рівень цифровізації управління електро- та тепломережами
	3.2. Відмови чи збої в роботі об'єктів інформатизації, які безпосередньо керують обладнанням електричних підстанцій
	3.3. Відмови чи збої в роботі об'єктів інформатизації, які безпосередньо керують енергооб'єктами центральної диспетчерської служби
	3.4. Різномірність використання програмних та апаратних засобів при побудові автоматизованих систем управління технологічною інформацією (АСУ ТП)
	3.5. Цифрова залежність від технологій та від постачальників цих інформаційних технологій
	3.6. Несумісність терміну експлуатації технічних засобів АСУ ТІ та основного технологічного обладнання енергоблоку електростанції
	3.7. Невідповідність засобів інформаційної безпеки впровадженим інформаційним управлінським рішенням
	3.8. Неякісне виконання проєкту з первинної розробки алгоритму управління технологічним процесом
	3.9. Несакціоновані дії та хакерські кібератаки
	3.10. Недостатній рівень кваліфікації оперативного персоналу
	3.11. Відсутність на енергопідприємствах спеціалізованих підрозділів, які безпосередньо відповідають за інформаційну безпеку

**Джерело:** складено авторами на основі [1–11].

ризиків належать різномірність використання програмних та апаратних засобів в автоматизованих системах управління технологічними процесами (АСУ ТП) енергопідприємств та автоматизованих систем контролю та обліку енергії (АСКОЕ), а та-

кож невідповідність засобів інформаційної безпеки впровадженим інформаційним управлінським рішенням.

*3. Ризики енергетичної безпеки підприємства електроенергетичної системи на стадії техноло-*

гічного процесу «Розподіл та споживання енергії». Значною стадією енергетичного виробництва є доведення електричної та теплової енергії до кінцевого споживача через розподільні електричні та теплові мережі із забезпеченням достовірного обліку споживаної енергії та встановлення самоокупних тарифів на електричну та теплову енергію.

У табл. 3 наведено класифікацію виявлених ризиків енергетичної безпеки підприємства електроенергетичної системи на стадії технологічного процесу «Розподіл та споживання енергії».

Як видно з табл. 3, на стадії технологічного процесу «Розподіл та споживання енергії» макро- та мезорівнів, найбільш важливими виробничими ри-

Таблиця 3

**Класифікація ризиків енергетичної безпеки підприємства електроенергетичної системи за джерелами ризиків на стадії процесу «Розподіл та споживання енергії»**

Вид ризику	Зміст ризику на стадії процесу «Розподіл та споживання енергії»
1	2
1. Виробничі ризики	1.1. Відключення, що призводять до порушення функціонування об'єктів забезпечення безперебійного постачання об'єктів промисловості та життєдіяльності населення
	1.2. Знос основних засобів
	1.3. Недостатність потужностей електромережі 0,4...10 кВ
	1.4. Необхідність масштабної реконструкції та будівництва електромережі 0,4...10 кВ
	1.5. Високий рівень витрат на обслуговування розподільчої мережі
	1.6. Аварії та відмови в роботі обладнання у зв'язку з помилковими діями оперативного персоналу автоматизованих систем контролю та обліку електроенергії (АСКОЕ)
	1.7. Зниження надійності роботи розподільної мережі через погодні та сезонні умови
	1.8. Прийом на баланс за «фактичним станом» зношених мереж від інших суб'єктів господарювання
	1.9. Високий рівень технічних і комерційних втрат у мережі 6 кВ
	1.10. Збільшення технологічної витрати електроенергії на транспорт з урахуванням роботи електродвигунів
	1.11. Відсутність 100% покриття електронними приладами обліку споживачів електричною та тепловою енергією
	1.12. Диверсії та терористичні акти
2. Фінансово-економічні ризики	2.1. Дефіцит обігових засобів та інвестицій
	2.2. Недостатність джерел фінансування для модернізації приладового парку обліку електричної та теплової енергії
	2.3. Надання значній кількості суб'єктів господарювання знижок із тарифів
	2.4. Зниження платоспроможності споживачів на макро- та мезорівнях економіки
	2.5. Зростання тарифів на купівлю енергії від блок-станцій (електростанцій та інших енергооб'єктів)
	2.6. Зростання цін на комплектні трансформаторні підстанції та щоголові трансформаторні підстанції, електронні прилади обліку, спліт-системи
	2.7. Відсутність впливу ЕЕС макро- та мезорівнів на встановлені тарифи
	2.8. Зростання вартості ремонтних робіт підрядних організацій
	2.9. Високі витрати на утримання допоміжних ремонтних цехів та об'єктів
3. Інформаційні ризики	3.1. Низький рівень автоматизації (цифровізації) розподільчої мережі
	3.2. Відмови або збої в роботі об'єктів інформатизації (наприклад, системи АСКОЕ), які безпосередньо керують технологічним обладнанням електричних підстанцій
	3.3. Відмови чи збої в роботі об'єктів інформатизації, які безпосередньо керують енергооб'єктами центральної диспетчерської служби (ЦДС)
	3.4. Різномірність використання програмних та апаратних засобів в автоматизованих системах управління (наприклад, у системах АСУ ТП та АСКОЕ)
	3.5. Цифрова залежність від технологій (особливо іноземних) і від постачальників цих інформаційних технологій
	3.6. Несумісність терміну експлуатації технічних засобів АСУ ТП (АСКОЕ) та основного технологічного обладнання



1	2
3. Інформаційні ризики	3.7. Невідповідність засобів інформаційної безпеки запровадженим інформаційним рішенням
	3.8. Неякісне виконання проєкту з первинної розробки алгоритму управління технологічним процесом розподілу енергії
	3.9. Несанкціоновані дії та хакерські кібератаки
	3.10. Недостатній рівень кваліфікації оперативного персоналу
	3.11. Відсутність на енергопідприємствах спеціалізованих автоматизованих робочих місць операторів (АРМо), які безпосередньо мають відповідати за інформаційну складову енергобезпеки підприємства ЕЕС

Джерело: складено авторами на основі [1–11].

зиками енергобезпеки підприємства є відключення, які призводять до порушення функціонування об'єктів забезпечення життєдіяльності населення (водо-, газо-, тепло-, електропостачання, водовідведення) – соціальний аспект ризику, а також ризик зносу основних засобів, який визнаний значним ризиком на попередніх етапах енерговиробництва. Відключення, що призводять до порушення функціонування об'єктів забезпечення життєдіяльності населення, можуть призвести до порушення електропостачання промислових споживачів, до значних економічних, соціальних і виробничих збитків, відсутності в населення основних житлово-комунальних послуг і, відповідно, соціальних благ.

У сучасних умовах дуже важливим необхідно вважати ризик диверсій та терористичних актів (наприклад, захоплення російськими військами території ЗАЕС). Ризик «диверсії та терористичні акти» проявляється досить серйозно в разі його реалізації, оскільки об'єкти енергетичної галузі як базові інфраструктурні об'єкти життєдіяльності держави є пріоритетними цілями для виведення з ладу. Зниження (нівелювання) даного ризику може бути здійснено тільки за рахунок додаткового захисту даних об'єктів. До найменш важливих виробничих ризиків необхідно віднести ризики, до яких належать: відсутність 100% покриття електронними приладами обліку споживачів; високий рівень витрат за обслуговування розподільчої мережі.

Згідно з наведеними в табл. 3 даними, щодо фінансово-економічних ризиків, експертів енергосистеми найбільше може турбувати дефіцит оборотних засобів та інвестицій (у тому числі зовнішніх) на модернізацію об'єктів розподільної електромережевої інфраструктури, зниження платоспроможності споживачів у регіоні, надання значній кількості суб'єктів господарювання знижок тарифів. Щоправда, відсутність впливу регіональних (обласних) енергосистем на рівень встановлених тарифів надає цьому ризику міні-

мального значення. До найменш важливих фінансово-економічних ризиків також віднесено високі витрати на утримання об'єктів транспорту та спецмеханізмів з відносно низькими коефіцієнтами випуску та сезонності використання деяких груп рухомого складу, а також високі витрати на утримання допоміжних ремонтних цехів при моральному та фізичному старінні їх виробничих потужностей і застосовуваних технологій.

Відповідно до табл. 3 до найбільш важливих ризиків, пов'язаних із застосуванням інформаційних технологій, на стадії процесу «Розподіл та споживання енергії» в електроенергосистемі на макро- та мезорівнях віднесено відмови або збої в роботі об'єктів інформатизації, які безпосередньо керують обладнанням підстанцій. Важливими інформаційними ризиками є несанкціоновані дії та хакерські кібератаки (злом, впровадження шкідливих програм-шифрувальників і блокувань, шантаж), неякісне виконання проєкту з первинної розробки алгоритму управління технологічним процесом (з подальшою ув'язкою з програмно-технічним комплексом та АСКОЕ). Крім того, важливим інформаційним ризиком є недостатній рівень кваліфікації оперативного персоналу, відсутність його зацікавленості в упровадженні інформаційних технологій, що призводить до відмов, помилок і збоїв у роботі технологічного обладнання з вини оперативного персоналу (наприклад, помилка оператора АСУ ТП чи АСКОЕ у прийнятті управлінського рішення щодо зниження впливу чи повної ліквідації загроз ЕБ підприємства).

Найменш важливим інформаційним ризиком на макро- та мезорівнях ЕЕС є цифрова залежність від технологій (особливо іноземних) та від постачальників цих інформаційних технологій (відмови в роботі технологічного обладнання у зв'язку з ненаданням постачальником програмно-технічного комплексу (ПТК) відповідних паролів для доступу до програмного забезпечення) (ПЗ), можливість віддаленого контролю та впливу на роботу техно-

логічного обладнання, зняття даних постачальником, промислове шпигунство та ін.). Слід звернути увагу на високий рейтинг інформаційного ризику – відсутність на енергопідприємствах автоматизованого робочого місця оператора (АРМо), який має відповідати за інформаційну складову енергобезпеки підприємства.

**Т**аким чином, слід зазначити, що підходи до визначення значущості груп ризиків схожі, а оцінки значущості конкретних ризиків у групах можуть відрізнятися з урахуванням особливостей функціонування підприємств електроенергетичних систем на макро-, мезо- та мікрорівнях економіки України.

Крім цього, необхідно відзначити основну особливість ризику – ризик має властивість зменшуватися зі збільшенням передбачуваності події, від настання чи ненастання якої залежить відповідно успіх або невдача аналізованого підприємства. І оскільки ризик у такому разі виражається відсотковою (або кількісною) можливістю нездійснення сприятливої події, то чим більше можливостей передбачити цю подію, тим менше значення ризику.

Ризик – це ситуація, що пов'язана з наявністю вибору з передбачуваних альтернатив шляхом оцінки ймовірності настання події, яка містить ризик, що тягне як позитивні, так і негативні наслідки.

Отже, ризик не можна визначити як подію. Подія в цьому випадку – це умова виникнення ризикової ситуації.

## ВИСНОВКИ

Запропонована класифікація загроз і ранжування ризиків енергобезпеки з урахуванням їхньої значущості на всіх етапах енергетичного виробництва можуть бути використані для формування системи управління ризиками підприємства електроенергетичної системи на макро-, мезо- та мікрорівнях економіки України. У результаті реалізації розглянутих заходів щодо зниження негативних впливів ризиків має бути досягнута економічна ефективність підприємства як результат провадження діяльності відповідно до цілей, поставлених у стратегії його розвитку, що виражається відношенням ефекту (результату) до витрачених ресурсів на його досягнення за оптимізації вартості.

Пропонований підхід до визначення видів та факторів ризиків підприємств, їх теоретичне та практичне узагальнення, на основі якого сформовано заходи щодо їх компенсації, можуть бути використані при прийнятті управлінських рішень.

Подальший розвиток досліджень у напрямку класифікації ризиків для організаційно-економічного забезпечення управління енергетичною

безпекою підприємств полягає в розробці більш глибоких і комплексних моделей управління ризиками з урахуванням макро-, мезо- та мікрорівнів економіки. У рамках подальших досліджень необхідно уточнити та розширити класифікацію ризиків, адаптуючи її до змін у зовнішньому та внутрішньому середовищі, особливо в умовах підвищеної економічної та політичної нестабільності. ■

## БІБЛІОГРАФІЯ

1. Iorember P. T., Gbaka S., Işık A. et al. New insight into decoupling carbon emissions from economic growth: Do financialization, human capital, and energy security risk matter? *Review of Development Economics*. 2024. Vol. 28. Iss. 3. P. 827–850. DOI: <https://doi.org/10.1111/rode.13077>
2. Axon C. J., Darton R. C. Sustainability and risk – a review of energy security. *Sustainable Production and Consumption*. 2021. Vol. 27. P. 1195–1204. DOI: <https://doi.org/10.1016/j.spc.2021.01.018>
3. Cergibozan R. Renewable energy sources as a solution for energy security risk: Empirical evidence from OECD countries. *Renewable Energy*. 2022. Vol. 183. P. 617–626. DOI: <https://doi.org/10.1016/j.renene.2021.11.056>
4. Iyke B. N. Climate change, energy security risk, and clean energy investment. *Energy Economics*. 2024. Vol. 129. Art. 107225. DOI: <https://doi.org/10.1016/j.eneco.2023.107225>
5. Podbregar I., Šimić G., Radovanović M. et al. International energy security risk index – Analysis of the methodological settings. *Energies*. 2020. Vol. 13. Iss. 12. Art. 3234. DOI: <https://doi.org/10.3390/en13123234>
6. Pang L., Liu L., Zhou X. et al. How does natural resource depletion affect energy security risk? New insights from major energy-consuming countries. *Energy Strategy Reviews*. 2024. Vol. 54. Art. 101460. DOI: <https://doi.org/10.1016/j.esr.2024.101460>
7. Lee C. C., Yuan Z., Wang Q. How does information and communication technology affect energy security? International evidence. *Energy Economics*. 2022. Vol. 109. Art. 105969. DOI: <https://doi.org/10.1016/j.eneco.2022.105969>
8. Axon C. J., Darton R. C. The causes of risk in fuel supply chains and their role in energy security. *Journal of Cleaner Production*. 2021. Vol. 324. Art. 129254. DOI: <https://doi.org/10.1016/j.jclepro.2021.129254>
9. Qiu L., Wang X., Wei J. Energy security and energy management: The role of extreme natural events. *Innovation and Green Development*. 2023. Vol. 2. Iss. 2. Art. 100051. DOI: <https://doi.org/10.1016/j.igd.2023.100051>
10. Prokhorova V., Budanov M., Budanov P. Devising an Integrated Methodology for Energy Safety Assessment at an Industrial Power-Generating Enterprise. *Eastern-European Journal of Enterprise Technologies*. 2024. Vol. 4. No. 13. P. 118–131. DOI: <https://doi.org/10.15587/1729-4061.2024.308056>

11. Буданов М. Загрози енергетичній безпеці підприємств України: методичний аспект. *Адаптивне управління: теорія і практика. Серія «Економіка»*. 2024. Вип. 18.  
DOI: [https://doi.org/10.33296/2707-0654-18\(36\)-08](https://doi.org/10.33296/2707-0654-18(36)-08)

## REFERENCES

- Axon, C. J., and Darton, R. C. "Sustainability and risk – a review of energy security". *Sustainable Production and Consumption*, vol. 27 (2021): 1195-1204.  
DOI: <https://doi.org/10.1016/j.spc.2021.01.018>
- Axon, C. J., and Darton, R. C. "The causes of risk in fuel supply chains and their role in energy security". *Journal of Cleaner Production*, art. 129254, vol. 324 (2021).  
DOI: <https://doi.org/10.1016/j.jclepro.2021.129254>
- Budanov, M. "Zahrozy enerhetychnii bezpetsi pid-priemstv Ukrainy: metodychnyi aspekt" [Threat to Power Safety of Enterprises of Ukraine: Methodical Aspect]. *Adaptyvne upravlinnia: teoriia i praktyka. Ser-riia «Ekononika»*, iss. 18 (2024).  
DOI: [https://doi.org/10.33296/2707-0654-18\(36\)-08](https://doi.org/10.33296/2707-0654-18(36)-08)
- Cergibozan, R. "Renewable energy sources as a solution for energy security risk: Empirical evidence from OECD countries". *Renewable Energy*, vol. 183 (2022): 617-626.  
DOI: <https://doi.org/10.1016/j.renene.2021.11.056>
- lorember, P. T. et al. "New insight into decoupling carbon emissions from economic growth: Do financialization, human capital, and energy security risk matter?" *Review of Development Economics*, vol. 28, no. 3 (2024): 827-850.  
DOI: <https://doi.org/10.1111/rode.13077>
- lyke, B. N. "Climate change, energy security risk, and clean energy investment". *Energy Economics*, art. 107225, vol. 129 (2024).  
DOI: <https://doi.org/10.1016/j.eneco.2023.107225>
- Lee, C. C., Yuan, Z., and Wang, Q. "How does information and communication technology affect energy security? International evidence". *Energy Economics*, art. 105969, vol. 109 (2022).  
DOI: <https://doi.org/10.1016/j.eneco.2022.105969>
- Pang, L. et al. "How does natural resource depletion affect energy security risk? New insights from major energy-consuming countries". *Energy Strategy Reviews*, art. 101460, vol. 54 (2024).  
DOI: <https://doi.org/10.1016/j.esr.2024.101460>
- Podbregar, I. et al. "International energy security risk index - Analysis of the methodological settings". *Energies*, art. 3234, vol. 13, no. 12 (2020).  
DOI: <https://doi.org/10.3390/en13123234>
- Prokhorova, V., Budanov, M., and Budanov, P. "Devising an Integrated Methodology for Energy Safety Assessment at an Industrial Power-Generating Enterprise". *Eastern-European Journal of Enterprise Technologies*, vol. 4, no. 13 (2024): 118-131.  
DOI: <https://doi.org/10.15587/1729-4061.2024.308056>
- Qiu, L., Wang, X., and Wei, J. "Energy security and energy management: The role of extreme natural events". *Innovation and Green Development*, art. 100051, vol. 2, no. 2 (2023).  
DOI: <https://doi.org/10.1016/j.igd.2023.100051>

УДК 005.32:331.101.3]:331.225.3

JEL: M12; M54

DOI: <https://doi.org/10.32983/2222-4459-2024-7-459-465>

# ПРЕМІЮВАННЯ ПЕРСОНАЛУ ЯК ІНСТРУМЕНТ РОЗВИТКУ МОТИВАЦІЙНОГО МЕНЕДЖМЕНТУ

©2024 МАХСМА М. Б., МЕЛЬНИК Т. П.

УДК 005.32:331.101.3]:331.225.3

JEL: M12; M54

## Махсма М. Б., Мельник Т. П. Преміювання персоналу як інструмент розвитку мотиваційного менеджменту

Метою статті є аналіз сучасного стану матеріального стимулювання, зокрема преміювання персоналу на прикладі виробничого підприємства, та окреслення заходів, спрямованих на підвищення його ефективності в сучасних воєнних умовах господарювання. Система мотивації та стимулювання працівників вітчизняних підприємств виробничого сектора протягом останніх п'яти років зазнала великих шоків пандемії та повномасштабного вторгнення. Останнє проявлялося хвилями скорочення обсягів виробництва, погіршенням фінансового стану підприємств і, як наслідок, скороченням темпів зростання заробітної плати та продуктивності праці. Водночас у 2023 р. підприємства здебільшого адаптувалися до викликів і обмежень воєнного стану, що дозволило їм зміцнити фінансові показники та дещо полішити систему мотивації, зокрема підвищити рівень оплати праці. Разом із тим негативною тенденцією на тлі позитивних зрушень у стимулюванні працівників стало скорочення частки додаткової заробітної плати, зокрема виробничих і невиробничих премій, що негативно позначилося на мотивації працівників, спричинило уповільнення темпів зростання продуктивності праці персоналу та відповідне погіршення інших фінансово-економічних показників. За умов воєнного стану, в яких зараз функціонує підприємницький сектор, важливим завданням менеджменту підприємства є вдосконалення мотиваційної політики, яка має спрямовуватися не лише на номінальне підвищення рівня оплати праці, але й на удосконалення структури заробітної плати. У контексті підвищення ефективності мотивації та стимулювання персоналу пропонуються збільшення питомої ваги додаткової заробітної плати, зокрема премій, розширення їх видів, уточнення критеріїв та показників преміювання, поліпшення інформаційної та комунікаційної взаємодії менеджменту і персоналу та інші заходи, спрямовані на побудову дієвої системи преміювання. Застосування запропонованих заходів