УДК 351.86:338.49 DOI 10.18372/2073-4751.87.21677

Азаренко О.В.[1], д.ф.-м.н.,
orcid.org/0000-0003-2927-5545,
e-mail: azarenko_ev@ukr.net**,**

Дівізінюк М.М[2], д.ф.-м.н.,
orcid.org/0000-0002-5657-2302,
e-mail: divizinyuk@ukr.net**,**

Лукашенко В.В.[3], д.т.н.,
orcid.org/0009-0009-0458-2590,
e-mail: viktoriia.lukashenko@kai.edu.ua**,**

Фаррахов О.В.[2], д.т.н.,
orcid.org/0000-0003-4988-126X,
e-mail: farrakhov@ukr.net

УЗАГАЛЬНЕНА СИСТЕМА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕНЕРГЕТИЧНОГО ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

[1]Науково-дослідний лабораторно-експериментальний центр «БРАНД ТРЕЙД»
[2]Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України
[3]Національний університет «Київський авіаційний інститут»

Вступ

Перед Україною як державою, що перебуває в умовах війни, постає низка надзвичайно важливих завдань, серед яких захист суверенітету, територіальної цілісності та незалежного існування держави, забезпечення безпеки життя цивільного населення та інші, що традиційно об'єднуються поняттями енергетичної безпеки, державної безпеки та безпеки критичної інфраструктури. Безперечно, вирішення цих завдань є першочерговим пріоритетом.

У загальному вигляді електроенергетика (або генерація електроенергії) складається з атомних електростанцій (АЕС), які забезпечують базове, масштабне та екологічно чисте (з погляду викидів) виробництво електроенергії. Теплові електростанції (ТЕС) і теплоелектроцентралі (ТЕЦ) працюють на вугіллі, природному газі або мазуті, виробляючи електричну та теплову енергію. Гідроелектростанції (ГЕС) і гідроакумулювальні електростанції (ГАЕС) використовують енергію водних потоків і відіграють важливу роль у покритті пікових навантажень енергосистеми. Вітрові та сонячні електростанції (ВЕС, СЕС) належать до децентралізованої «зеленої» генерації. Забезпечення безпеки цих об'єктів є актуальною науково-прикладною проблемою, над розв'язанням якої працюють науковці, фахівці-практики та військові.

Виходячи з викладеного, метою цієї статті є розгляд узагальненої системи забезпечення безпеки енергетичного об'єкта критичної інфраструктури.

Для досягнення поставленої мети необхідно вирішити такі завдання. Насамперед проаналізувати узагальнену структуру системи безпеки енергетичного

об'єкта. Далі надати характеристику її складових. Після цього запропонувати використання інформаційного принципу Пампуро для вдосконалення існуючих і розроблення принципово нових систем забезпечення безпеки енергетичних об'єктів.

Наукова новизна роботи полягає в удосконаленні структурно-функціонального представлення системи забезпечення безпеки енергетичного об'єкта критичної інфраструктури шляхом її побудови у вигляді замкненого інформаційно-керувального контуру «система моніторингу – система підтримки прийняття рішень – система виконання – зворотний контроль стану об'єкта». На відміну від підходів, за яких технологічні, інформаційні та управлінські процеси розглядаються окремо, запропонований підхід передбачає їх об'єднання в єдиному інформаційному просторі на основі інформаційного принципу Пампуро. Авторським результатом є узагальнена структурно-функціональна модель системи безпеки, у якій забезпечено функціональну наступність між модулями моніторингу, підтримки прийняття рішень і реалізації керувальних впливів, а зміна стану об'єкта формує зворотний інформаційний потік для подальшого коригування управління. Така структура може бути застосована до енергетичних об'єктів різного типу незалежно від фізичної природи процесів генерації енергії.

Виклад основного матеріалу

Процеси виробництва електричної енергії на енергетичних об'єктах різного типу ґрунтуються на різних фізичних принципах і характеризуються різними послідовностями перетворення первинної енергії. На теплових електростанціях і теплоелектроцентралях хімічна енергія палива перетворюється на теплову енергію робочого тіла, далі — на механічну енергію обертання турбіни і, зрештою, на електричну енергію генератора. На атомних електростанціях первинним джерелом теплової енергії є енергія поділу атомних ядер, після чого теплова енергія перетворюється на механічну та електричну. На гідроелектростанціях і гідроакумулювальних електростанціях потенціальна та кінетична енергія води перетворюється на механічну енергію гідротурбіни, а потім — на електричну. На вітрових електростанціях кінетична енергія повітряного потоку перетворюється на механічну та електричну енергію, тоді як на сонячних електростанціях перетворення енергії сонячного випромінювання в електричну відбувається фотоелектричним способом без проміжної механічної стадії. Таким чином, для різних типів енергетичних об'єктів характерними є різні фізичні ланцюги перетворення енергії, які водночас можуть бути об'єднані спільними принципами інформаційного контролю, моніторингу та управління.

Незважаючи на різноманітність фізичних процесів, функціонування електростанції забезпечується єдиним контуром управління, який включає об'єкт управління та сукупність технічних і організаційних засобів, призначених для контролю, аналізу й регулювання його стану. У загальному випадку такий контур управління можна поділити на три функціонально взаємопов'язані підсистеми: підсистему моніторингу, підсистему підтримки прийняття рішень

та підсистему виконання керувальних впливів.

Підсистема моніторингу здійснює безперервне збирання інформації про всі технологічні процеси, що відбуваються на об'єкті. Первинні датчики перетворюють аналогові фізичні величини, які характеризують стан об'єкта управління, у цифрову форму, придатну для подальшого оброблення. До таких величин належать витрата палива, температура процесів горіння, рівень води, тиск і температура пари, швидкість обертання турбогенератора, параметри електричної мережі, стан обладнання, а також багато інших технологічних характеристик. Після перетворення вимірювальна інформація проходить етапи фільтрації, оброблення, класифікації, накопичення та зберігання, формуючи інформаційну основу для аналізу поточного стану об'єкта й прогнозування його подальшого функціонування.

На погляд досвідчених фахівців в галузі державної безпеки [1, 2], в основі будь-якої безпекової діяльності лежить використання системи моніторингу (СМ) і системи підтримки прийняття рішень (СППР), принципові структурні схеми яких подано на рис. 1, як складові частини системи управління безпекою об'єкта.

Система моніторингу структурно складається із семи основних модулів. Перший - модуль «джерела первинних даних» (позначений як 1м). Вони в найпростішому випадку поділяються за контрольованими параметрами, 1, 2,…, G; за інструментальним виконанням 1, 2,…, i; і, наприклад, виду зв'язку (передавання даних) 1, 2,…, j. Іншими словами в цьому випадку Gi,j джерел первинних даних. У низці випадків, їх називаю датчиками.

Другий модуль «збір даних» (2м). Цей модуль відповідає за збір даних, що надходять від різних джерел первинних даних про поточні значення відповідного параметра, що характеризують той чи інший показник стану спостережуваного об'єкта управління.

Третій модуль «обробка даних» (3м). Тут відбувається опрацювання даних, наприклад приведення їх до єдиної системи метрологічних вимірювань, а потім до системи кодів, які використовують сервери даної системи моніторингу.

Четвертий модуль «систематизація даних» (4м). У цьому модулі відбувається машинна (електронна) систематизація даних, яка здійснюється на підставі зміни контрольованих параметрів на спостережуваному об'єкті.

П'ятий модуль «база даних і знань» (5м). Цей модуль відповідає за накопичення систематизованих даних про зміну стану спостережуваного об'єкта. Крім цього тут зберігаються знання про різні ситуації, що мали місце на інших таких самих об'єктах, або об'єктах, що мають схожі характеристики.

Шостий модуль «моделювання варіантів розвитку ситуації» (6м). Тут відбувається моделювання розвитку ситуацій на спостережуваному об'єкті, залежно від виявлених або передбачуваних тенденцій їхнього розвитку.

Сьомий модуль «варіанти розвитку ситуацій» (7м), які можуть статися на спостережуваному об'єкті (або об'єкті управління). Вони включають як найоптимістичніший або найсприятливіший варіант 1, так і найпесимістичніший або найгірший варіант К.

У підсистемі підтримки прийняття рішень практично всі процеси мають інформаційну природу. Тут здійснюється оброблення отриманих даних, їх зіставлення з нормативними значеннями, аналіз можливих відхилень, оцінювання ризику виникнення аварійних ситуацій, прогнозування розвитку подій і вибір оптимальних варіантів керувальних впливів. На цьому етапі інформація існує виключно в цифровій формі та використовується інтелектуальними алгоритмами, математичними моделями, експертними системами й програмними засобами аналізу.

Система підтримки прийняття рішень так само структурно складається із семи основних модулів.

Перший модуль «варіанти розвитку ситуацій» (1пр), одночасно є сьомим блоком системи моніторингу.

Другий модуль «відбір результатів моделювання за певними критеріями» (2пр). Цей модуль забезпечує відбір варіантів моделювання за критеріями, що визначаються відповідними методиками, інструкціями, протоколами або задаються безпосередньо особою, яка приймає рішення (ОПР).

Як правило, обирають не менше двох варіантів.

Третій модуль «розробка варіантів управлінських рішень за кожним відібраним варіантом розвитку ситуації» (3пр). Тут відбувається підготовка варіантів управлінських рішень. Як правило, для кожного відібраного варіанта розвитку ситуації розробляється кілька варіантів управлінських рішень. Підсумком цієї роботи є наступний модуль.

Четвертий модуль «варіанти розроблених управлінських рішень» (4пр). Цей модуль включає сукупність усіх варіантів розроблених управлінських рішень. Стосовно розглянутого прикладу, це перша сукупність управлінських рішень від варіанта 1.1 до варіанта 1.M, що відповідають першому варіанту розвитку ситуації. Друга сукупність управлінських рішень від варіанта К.1 до варіанта К.N, що відповідають К-тому варіанту розвитку ситуації.

П'ятий модуль «обґрунтування та вибір управлінських рішень (наприклад, залежно від наявності сил і засобів)» (5пр). Тут відбувається обґрунтування (тобто розрахунок витрат на зміну перебігу розвитку ситуації, наприклад розрахунок необхідної кількості сил і засобів) для кожного з варіантів управлінських рішень. На підставі виконаних розрахунків проводиться вибір. Як правило, обирається кілька варіантів управлінських рішень. Підсумком цієї роботи є наступний модуль.

Шостий модуль «обґрунтовані та обрані управлінські рішення» (6пр). Цей модуль містить сукупність обґрунтованих і обраних управлінських рішень. Стосовно розглянутого прикладу, це сукупність від управлінського рішення 1 до управлінського рішення L.

Сьомий модуль «вибір і прийняття рішення посадовою особою» (7пр). Тут відбувається прийняття рішення ОПР, яке з управлінських рішень реалізовувати в реальному житті і в які терміни.

Сформовані рішення передаються до виконавчої підсистеми, де знову перетворюються на аналогові впливи на об'єкт управління. Такі впливи можуть реалізовуватися як автоматично — шляхом зміни режимів роботи обладнання, регулювання подачі палива, зміни положення виконавчих механізмів,

керування насосними агрегатами, клапанами та регуляторами тиску, — так і у вигляді організаційних рішень, представлених інструкціями, розпорядженнями, командами або наказами для оперативного персоналу. Незалежно від форми реалізації кожен керувальний вплив змінює стан об'єкта управління та впливає на подальший перебіг технологічного процесу.

Система виконання (СВ) структурно складається з трьох основних модулів.

Перший модуль «вибір і ухвалення рішення посадовою особою» (1св) одночасно є сьомим блоком системи підтримки прийняття рішень.

Другий модуль «система виконання керуючого рішення» (2св). Цей модуль забезпечує розроблення керуючих команд, наказів, інструкцій, директив, протоколів та інших видів керуючих впливів на об'єкт управління.

Зміна стану об'єкта управління призводить до зміни його параметрів, які фіксуються джерелами первинних даних (модуль 1м системи моніторингу).

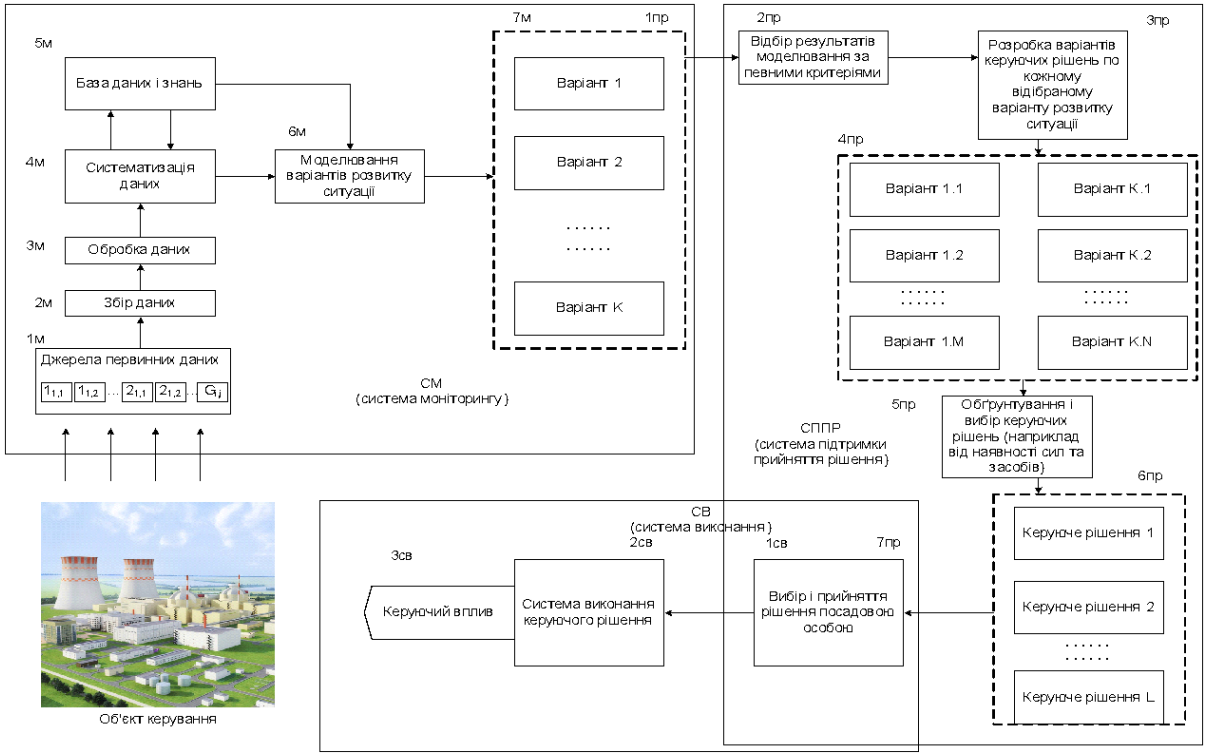

Рис. 1. Система керування безпекою об'єкту

Зібрані, опрацьовані та систематизовані дані дають змогу стежити за розвитком ситуації та коригувати управлінські впливи для збереження або поліпшення стану керованого об'єкта.

Особливістю розглядуваної системи є те, що в ній одночасно функціонують елементи, які принципово відрізняються за своєю фізичною природою. Одні з них здійснюють перетворення енергетичних потоків, інші забезпечують переміщення матеріальних ресурсів, треті виконують функції вимірювання, оброблення інформації, підтримки прийняття рішень або реалізації керувальних впливів. З погляду класичних фізичних уявлень такі елементи складно об'єднати в межах єдиної моделі, оскільки кожен із них описується власними законами та характеристиками.

Для подолання цього методологічного обмеження В.І. Пампуро

запропонував структурно-інформаційний підхід до дослідження складних систем, відповідно до якого різнорідні за фізичною природою елементи можуть бути представлені через процеси формування, перетворення, передавання та використання інформації [3,4]. Сутність цього принципу полягає у відмові від аналізу фізичних відмінностей між елементами системи та переході до їх розгляду як джерел, перетворювачів, накопичувачів, передавачів і споживачів інформації. За такого підходу кожен елемент об'єкта управління, незалежно від його призначення, характеризується насамперед інформацією, яку він сприймає, перетворює, передає або використовує.

Іншими словами, будь-який матеріальний або енергетичний процес розглядається як процес виникнення, зміни та передавання інформації про стан об'єкта. Температура, тиск, витрата палива, швидкість обертання турбіни, електрична напруга, команди оператора та керувальні впливи являють собою різні форми інформаційного опису єдиного технологічного процесу. Завдяки цьому стає можливим побудова універсальної моделі об'єкта управління, у якій усі елементи об'єднані не енергетичними чи матеріальними зв'язками, а системою інформаційних потоків.

Відповідно до принципу Пампуро взаємозв'язок між окремими елементами об'єкта управління є еквівалентним взаємозв'язку інформаційних потоків, що циркулюють між ними. Будь-яка зміна стану одного елемента спричиняє зміну відповідного інформаційного потоку, яка передається іншим елементам системи та ініціює їхню реакцію. Отже, поведінка всієї системи визначається не лише законами перетворення енергії або речовини, а й закономірностями формування, передавання, оброблення та використання інформації.

Аналіз терористичних атак на об'єкти критичної інфраструктури [5-7] показують, що спостереження за навколишнім повітряним простором є одним із ключових методів своєчасного запобігання ударним терористичним впливам на об'єкти енергетики. Крім цього, охоронним структурам і структурам безпеки цих енергетичних об'єктів (де відсутні служби фізичного захисту) необхідне впровадження функцій фізичного захисту, як і на АЕС. При цьому доцільно переходити від забезпечення безпеки одного об'єкта критичної інфраструктури до забезпечення безпеки конгломерації об'єктів критичної інфраструктури [8-10].

Висновки

Запропоновано узагальнену структурно-функціональну модель системи забезпечення безпеки енергетичного об'єкта критичної інфраструктури, представлену як замкнений інформаційно-керувальний контур, що об'єднує систему моніторингу, систему підтримки прийняття рішень та систему виконання керувальних впливів. Взаємозв'язок зазначених підсистем забезпечує безперервний цикл «контроль стану – аналіз і прогнозування – формування рішення – реалізація керувального впливу – контроль результату».

Використання інформаційного принципу Пампуро [9, 10] під час розроблення математичних моделей безпеки дає змогу єдиним чином описувати технологічні, організаційні, інформаційні та управлінські процеси. Це забезпечує можливість об'єднати в межах єдиної моделі процеси технологічного управління, моніторингу небезпек, підтримки прийняття рішень, фізичного захисту, кібербезпеки та протиаварійного управління, розглядаючи їх як взаємопов'язані інформаційні процеси, що забезпечують стале й безпечне функціонування об'єкта.

Література

1. Дивизинюк М.М., Герасимов Б.М., Субач І.Ю. Системи підтримки

прийняття рішень: проєктування, застосування, оцінювання ефективності: монографія. Севастополь : СНУЯЕтаП, 2004. 318 с.

2. Андронов В. А., Дівізінюк М. М., Калугін В. Д., Тютюник В. В. Науково-конструкторські створення комплексної системи моніторингу надзвичайних ситуацій в Україні: Монографія / В. А. Андронов, М. М. Дівізінюк, В. Д. Калугін, В. В. Тютюник. – Х.: НУЦЗУ, 2016. – 319 с. ISBN 978-617-7474-74-5

3. Пампуро В.І. Структурна інформаційна теорія надійності систем / В.І. Пампуро; АН України, Ін-т електродинаміки; відп. ред. Г. Г. Щасливий. - К.: Наукова думка, 1992. - 328 с. - ISBN 5-12-002021-6.

4. Пампуро В.І. Оптимальне управління безпекою екологічно небезпечних об'єктів: монографія / В. І. Пампуро; НАН України, Ін-т геохімії довкілля. - К.: Наукова думка, 2012. - 597 с. - ISBN 978-966-00-1155-7.

5. Дівізінюк М.М. Моделювання загроз та протидії проникнення безпілотних літальних апаратів на об'єкти критичної інфраструктури / М.М. Дівізінюк, О.М. Мирошник, А.В. М'ясоєдова, А.О. Хмирова, О.С. Шевченко, Р.І. Шевченко // Монографія - Черкаси: видавець Вовчок О.Ю., 2023. 122 с. (ISBN 978-617-7508-31-0)

6. Miasoyedova A., Divizinyuk M., Shevchenko R. Mathematical models for detecting the danger of critical infrastructure objects by unmanned aerial vehicles // Challenges and threats to critical infrastructure. Collective monograph - NGO Institute for Cyberspace Research (Detroit, Michigan, USA), 2023. - p. 204 ISBN-10/979-8-218-22315-1

7. Diviziniuk M., Farrakhov O., Shaidetska L., Dement M., Ryzhchenk O. Prevention of Terrorist Effects on Critical Infrastructure Objects Using Motor Vehicle Databases Obtained from External Surveillance Video Systems. In: Ercetin U., Zuievska N., Vovk O. (eds) Critical Infrastructure Protection in Response to Terrorist Attacks. NATO Science for Peace and Security Series - E: Human and Societal Dynamics. 2024. Vol.157. P.86-99. https://doi.org/10.3233/NHSDP240007

8. Азаренко, О., Гончаренко, Ю., Дівізінюк, М., Хмирова, А., Шевченко, Р., Шевченко, О. Характеристика методів захисту критичної інфраструктури держави від терористичного впливу. Науково-технічний збірник «Комунальне господарство міст», 1(182). 2024. С.202–209. https://doi.org/10.33042/2522-1809-2024-1-182-202-209

9. Дівізінюк М.М., Фаррахов О.В., Марцева Л.А., Коцюбинський А.О., Власенко О.В. Аналіз сценаріїв використання безпілотних літальних апаратів проти об'єктів критичної інфраструктури. Науковий журнал «Наука, технології інновації» № 3(31), 2024. С.107-114. http://doi.org/10.35668/2520-6524-2024-3-12

10. Diviziniuk M.M., Farrakhov O.V., Zinovieva I.S., Kutsenko V.O., Shevchuk R. About the methodology to improve concept of maximum security of nuclear facility at minimum costs. IOP Conference Series: Earth and Environmental Science. 2024. Vol.1415. 012123. https://doi.org/10.1088/1755-1315/1415/1/012123

Рукопис опрацьовував незалежний відповідальний редактор; автор не брав участі у процесі рецензування та прийнятті рішення щодо публікації.

Азаренко О.В., Дівізінюк М.М., Лукашенко В.В., Фаррахов О.В.

УЗАГАЛЬНЕНА СИСТЕМА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕНЕРГЕТИЧНОГО ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті розглянуто узагальнену систему забезпечення безпеки енергетичного об'єкта критичної інфраструктури як замкнений інформаційно-керувальний контур, що об'єднує систему

моніторингу, систему підтримки прийняття рішень та систему виконання керувальних впливів. Проаналізовано функціональну структуру кожної з підсистем, їх взаємозв'язки та послідовність циркуляції інформації від первинного контролю стану об'єкта до формування, прийняття й реалізації управлінських рішень із подальшим зворотним контролем результатів впливу. Показано, що енергетичні об'єкти різних типів — атомні, теплові, гідро-, вітрові та сонячні електростанції — істотно відрізняються за фізичною природою процесів перетворення енергії, однак можуть бути описані в межах єдиного підходу через інформаційні потоки, які відображають стан, зміну параметрів і реакцію об'єкта на керувальні дії. Наукова новизна роботи полягає в удосконаленні структурно-функціонального представлення системи безпеки енергетичного об'єкта шляхом інтеграції технологічних, інформаційних, організаційних і управлінських процесів у єдиний інформаційний простір на основі інформаційного принципу Пампуро. Авторським результатом є узагальнена модель, у якій забезпечено функціональну наступність між модулями моніторингу, підтримки прийняття рішень і реалізації керувальних впливів, а зміна стану об'єкта формує зворотний інформаційний потік для коригування управління. Запропонований підхід створює передумови для побудови універсальних моделей безпеки, придатних для аналізу загроз, прогнозування ситуацій, обґрунтування рішень, фізичного захисту, кібербезпеки та протиаварійного управління. Практичне значення результатів полягає у можливості використання моделі для вдосконалення та проєктування систем безпеки об'єктів критичної енергетичної інфраструктури.

Ключові слова: *енергетичний об'єкт, критична інфраструктура, система безпеки, система моніторингу, система підтримки прийняття рішень, інформаційний принцип Пампуро, керувальний вплив.*

Azarenko E.V., Diviziniuk M.M., Lukashenko V.V., Farrakhov O.V.

GENERALIZED SECURITY SYSTEM FOR A CRITICAL ENERGY INFRASTRUCTURE FACILITY

The article considers a generalized security system for a critical energy infrastructure facility as a closed information-and-control loop integrating a monitoring system, a decision support system, and a control-action execution system. The functional structure of each subsystem, their interconnections, and the circulation of information from primary monitoring of the facility state to the formation, adoption, and implementation of management decisions, followed by feedback control of the results, are analyzed. It is shown that different types of energy facilities—nuclear, thermal, hydro, wind, and solar power plants—differ substantially in the physical nature of energy conversion processes, yet they can be described within a unified approach through information flows reflecting the facility state, changes in its parameters, and its response to control actions. The scientific novelty consists in improving the structural and functional representation of an energy facility security system by integrating technological, information, organizational, and management processes into a common information space based on Pampuro's information principle. The authors' result is a generalized model that ensures functional continuity between monitoring, decision support, and control-action implementation modules, while changes in the facility state generate a feedback information flow for control adjustment. The proposed approach provides a basis for developing universal security models suitable for threat analysis, situation forecasting, substantiation of management decisions, physical protection, cybersecurity, and emergency control. The practical significance of the results lies in the possibility of using the model to improve and design security systems for critical energy infrastructure facilities.

Keywords: *energy facility, critical infrastructure, security, monitoring system, information.*

Стаття подана до редакції: 15/09/2026
Стаття прийнята до опублікування:21/09/2026
Стаття опублікована: 10/11/2026

Стаття поширюється на умовах ліцензії CC BY 4.0