УДК 351.861

https://doi.org/10.52058/3041-1254-2024-3(3)-208-220

Помаза-Пономаренко Аліна Леонідівна доктор наук з державного управління, старший дослідник, начальник наукового відділу проблем державної безпеки навчально-науково-виробничого центру, Національний університет цивільного захисту України, вул. Лермонтовська, 28, м. Харків, 61024, https://orcid.org/0000-0001-5666-9350

Тарадуда Дмитро Віталійович кандидат технічних наук, доцент, заступник начальника кафедри організації та технічного забезпечення аварійно-рятувальних робіт факультету цивільного захисту, Національний університет цивільного захисту України, вул. Чернишевська, 94, м. Харків, 61024, https://orcid.org/0000-0001-9167-0058

ОСОБЛИВОСТІ УПРАВЛІННЯ Й ЕКСПЛУАТАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. Визначено особливості побудови й управління критичної інфраструктури, а також її взаємозалежностей, що впливають на властивості експлуатації такої інфраструктури в умовах імпульсної присутності. Акцентовано, що вона може зумовлювати появу ефекту саморуйнування (деструктивізму) об'єктів критичної інфраструктури. Серед засад побудови й управління об'єктами критичної інфраструктури обґрунтовано виокремлення загальних і спеціальних управлінських принципів (результативності, ефективності, науковості, централізованості тощо). Установлено, що зв'язки підсистем критичної інфраструктури можуть призводити до інфраструктурного деструктивізму, тобто мати інфраструктурне походження. При цьому аргументовано співвіднесення суб'єктів й об'єктів критичної інфраструктури. Конкретизовано, що для України найбільш загрозливими є не внутрішні чинники, а зовнішні, як-то повномасштабна агресія рф, що чинить вплив на об'єкти критичної інфраструктури (КІ). Крім того, досліджено аспекти, пов'язані зі значущістю видів зв'язків у процесі функціонування КІ. Доведено, що ці суб'єктно-об'єктні зв'язки формуються та вдосконалюються в межах «інфраструктурного середовища». У цьому контексті запропоновано визначення такого середовища, що представляє собою структуру, яку можна описати з позиції унікальності характеристик, властивих даній структурі як самостійній системі, так і через характеристики інфраструктур, її складових. При цьому наполягається, що між елементами КІ та інфраструктурним

середовищем відсутні чіткі межі (вони доволі розмиті). Окрім секторального підходу, по відношенню до характеристики інфраструктурного середовища рекомендовано застосовувати також інституціональний підхід. Вони дозволяють представити інфраструктурне середовище як сукупність факторів, умов та інститутів, що у підсумку забезпечують належне функціонування об'єктів КІ як у мирний час, так і в період невизначеності, або надзвичайного та воєнного стану. Серед цих інститутів виокремлено правові, соціальні, організаційні та ін.

Ключові слова: публічне управління, національна безпека, інформаційна безпека, соціальна безпека, соціальний захист, надзвичайні ситуації, цивільний захист, об'єкти критичної інфраструктури.

Pomaza-Ponomarenko Alina Leonadivna Doctor in Public Administration, Senior Researcher, Head of the Scientific Department for State Security Problems of the Training Research and Production Centre, National University of Civil Protection of Ukraine, St. Lermontovskaya, 28, Kharkiv, 61024, https://orcid.org/0000-0001-5666-9350

Taraduda Dmytro Vitaliyovych PhD in Technical Science, Associate professor, Deputy Head of Department of organization and technical support of emergency rescue works, National University of Civil Protection of Ukraine, St. Chernyshevskaya, 94, Kharkiv, 61024, https://orcid.org/0000-0001-9167-0058

FEATURES OF MANAGEMENT AND OPERATION OF CRITICAL INFRASTRUCTURE FACILITIES IN THE CONTEXT OF ENSURING INFORMATION SECURITY

Abstract. The peculiarities of the construction and management of critical infrastructure, as well as its interdependencies, which affect the properties of the operation of such infrastructure in the conditions of pulse presence, are determined. It is emphasized that it can lead to the appearance of the effect of self-destruction (destructivism) of critical infrastructure objects. Among the principles of construction and management of critical infrastructure objects, the separation of general and special management principles (effectiveness, efficiency, scientificity, centralization, etc.) is substantiated. It has been established that connections of subsystems of critical infrastructure can lead to infrastructural destructiveness, that is, have an infrastructural origin. At the same time, the correlation of subjects and objects of critical infrastructure is argued. It was specified that the most threatening factors for Ukraine are not internal factors, but external factors, such as the full-scale aggression of the Russian Federation, which affects critical infrastructure (CI). In addition, aspects related to the importance of types of connections in the process of CI functioning were investigated. It is proved that these subject-object relations are formed and improved

within the "infrastructural environment". In this context, a definition of such an environment is proposed, which is a structure that can be described from the standpoint of the uniqueness of the characteristics characteristic of this structure as an independent system, and through the characteristics of infrastructures, its components. At the same time, it is insisted that there are no clear boundaries between CI elements and the infrastructural environment (they are quite blurred). In addition to the sectoral approach, in relation to the characteristics of the infrastructure environment, it is also recommended to use an institutional approach. They allow us to present the infrastructural environment as a set of factors, conditions and institutions, which ultimately ensure the proper functioning of CI facilities both in peacetime and in periods of uncertainty, or in states of emergency and war. Among these institutions, legal, social, organizational, etc. institutions are distinguished.

Keywords: public administration, national security, information security, social security, social protection, emergency situations, civil protection, critical infrastructure facilities.

Постановка проблеми. Через повномасштабну агресію рф проти України ускладнилася ситуація із забезпеченням її цивільної та соціальної безпеки. Зовнішня агресія рф знижує рівень такої безпеки, свідченням чого є зруйнована вітчизняна критична інфраструктура й об'єкти підвищеної небезпеки [1-4; 9; 10]. Складності ситуації додає те, що деструктивний вплив на критичну інфраструктуру також спрямований на зниження інформаційної безпеки такої інфраструктури. У цьому контексті важливою є розробка та здійснення державних заходів, покликаних попередити вчасно виникнення надзвичайних ситуацій, забезпечити трансформацію загроз у сфері безпеки у прогнозовані та регульовані. При цьому особливої актуальності набуває дослідження стану забезпечення цивільної безпеки з позиції попередження надзвичайних ситуацій на об'єктах підвищеної небезпеки та критичної інфраструктури в Україні. Усе це визначає важливість обраної проблематики дослідження.

Аналіз останніх досліджень і публікацій. Особливості публічного управління у сфері цивільної безпеки досліджені в працях Т. Адамса, В. Андронова, К. Бєлікова, Л. Берга, О. Бойко, А. Воденичарова, Т. Гундерсена, С. Калояннідіса, Е.Дж. Кіршнера, Н. Клименко, Ю. Ключки, О. Крюкова, Р.Дж. Леклер, О. Лещенко, П. Махортова, С. Перроу, О. Подскальної, С. Потерійка, М. Стівена, А. Субраманян, В. Терент'євєвої, О. Твердохліба, В. Чжу, М. Хойтинк та ін. [6-8; 11-13].

Постановка завдання. Метою наукового дослідження є визначення особливості управління й експлуатації об'єктів критичної інфраструктури з позиції забезпечення інформаційної безпеки.

Виклад основного матеріалу. Аналіз міжнародного досвіду побудови та функціонування об’єктів КІ [2; 5; 6; 7; 8; 11; 12] показав, що під час реалізації означених процесів поширеним є використання системного та секторального підходів. Вони відзначаються характеристикою КІ:

1) на структурному рівні (через визначення елементів системи та зв'язків між ними);

2) на функціональному рівні (через чітке формулювання функцій КІ та її компонентів);

3) на макро рівні (через представлення КІ у вигляді єдиного цілого, що взаємодіє із зовнішнім середовищем, зокрема, інституційним);

4) на мікро рівні (через представлення КІ у вигляді сукупності взаємозалежних елементів) (рис. 1).

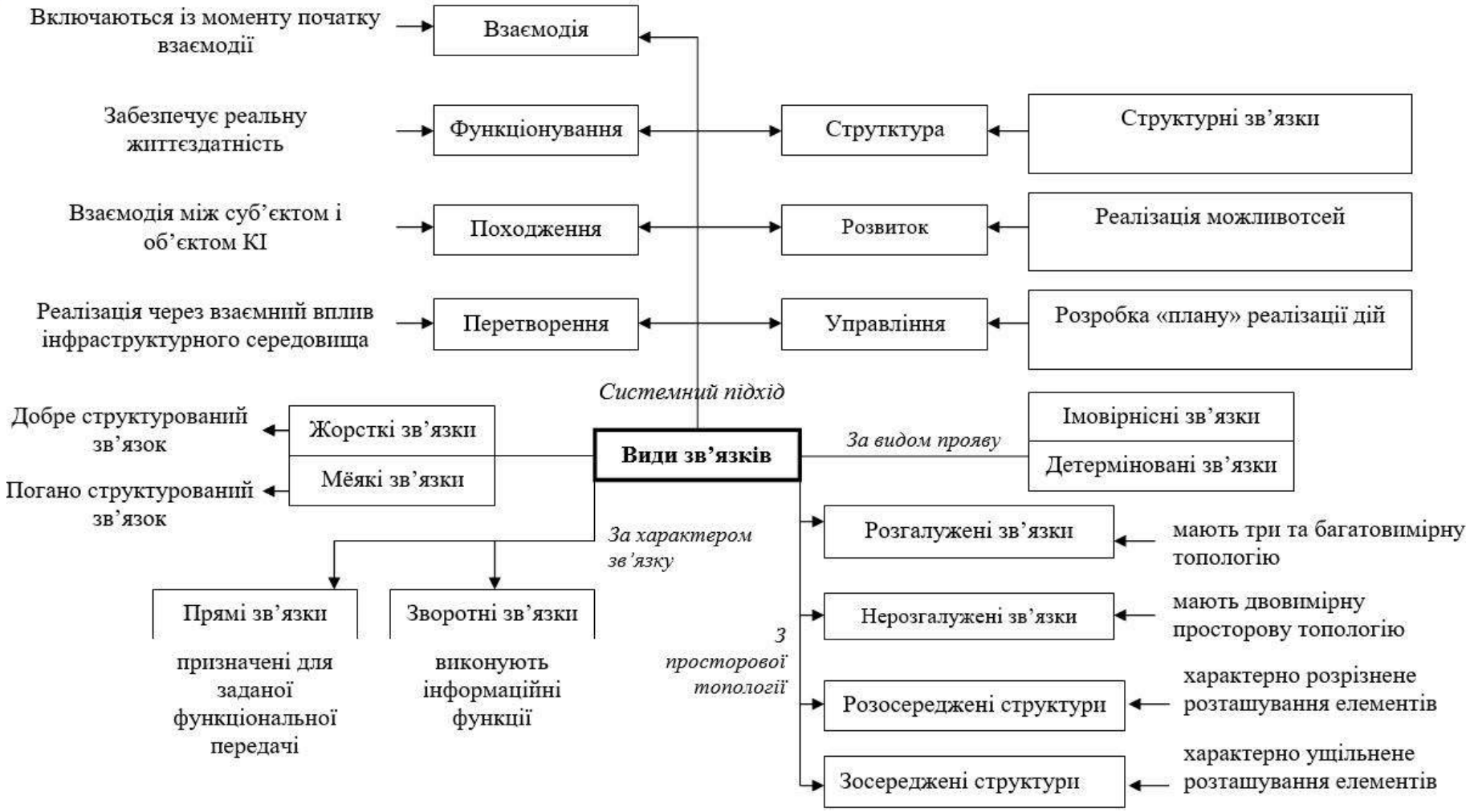

Рис. 1. Класифікація зв'язків у межах критичної інфраструктури
Джерело: авторська розробка

Під час проведення дослідження щодо особливостей побудови КІ виявлено, що структура будь-якої КІ як системи описується крізь призму визначення її: 1) складності через кількість зв'язків; 2) внутрішньої структури – через кількість внутрішніх зв'язків; 3) відкритості (взаємодія із середовищем) – через число зовнішніх зв'язків; 4) стійкості – через загальне число взаємодій та інтенсивність взаємодії елементів (кількість зв'язків, що припадають однією елемент) [6; 7; 11-13].

Варто зазначити, що основні засади побудови системи задаються етапи проектування КІ. У міру дослідження КІ як системи, нами з'ясовано, що її структура може змінюватися. При цьому система може отримати новий функціонал або нові властивості, якщо при постійному кількісному її складі варіювати міжелементними зв'язками, які будуть якісними характеристиками системи. Щодо взаємодії із зовнішнім середовищем виділяють системи: 1) із постійною (статичною) структурою, що характеризуються незмінністю станів системи при зміні параметрів зовнішнього середовища; 2) із гнучкою структурою, що характеризуються здатністю пристосовуватися до зовнішніх умов за рахунок коригування властивостей елементів за сталості складу та структури системи; 3) адаптивні, що функціонують за можливості зміни параметрів і структури на тлі умов зовнішнього середовища, що трансформуються.

Таким чином, дослідження структури системи є одним із найважливіших етапів у дослідженні побудови структури КІ. Оскільки для системи структура є тим системоутворюючим і системозберігаючим фактором, що передбачає збереження стійкості системи. Урахування положень фундаментальної науки дозволило визначити особливості побудови КІ як системи. Розвиток її структури найчастіше супроводжується її зміною, появою нових властивостей та ін. Це необхідно враховувати при виборі рішень щодо управління розвитком систем КІ. При цьому залежно від типу структури системи ті чи інші її властивості можуть проявлятися по-різному.

За результатами дослідження поняття «критична інфраструктура» можна позначити такі властиві їй ознаки: захист прав та послуг; підтримка у сфері послуг; наявність партнерських відносин; облік особливостей сегмента; взаємозалежність елементів; інтерактивність; взаємозв'язок елементів.

Проблема моніторингу взаємозалежностей кількох інфраструктур під час вирішення завдань забезпечення інформаційної безпеки наразі лише починає досліджуватися. Складності пов'язані зі значними класами моделей, що використовуються при описі інфраструктур. Проте сьогодні існують підходи в різних сферах діяльності, спрямовані на оптимізацію функціонування складних систем з урахуванням інфраструктурних особливостей, наприклад, програми підвищення ефективності функціонування електричних мереж, дослідження та аналізу водопровідних мереж міста, оптимізації руху

для транспортних мереж та ін. Крім того, розробляються розширювані програмні рішення на основі акторів для моделювання, симуляції та аналізу взаємозалежних інфраструктур [5; 6].

У наукових роботах [7; 12] розглядаються питання щодо синтезу моделей інтегрованих інфраструктур. Результати досліджень свідчать про загальні підходи до дослідження структури взаємозалежностей усередині КІ. При цьому говорити про універсальність в інтегративному сенсі не варто, оскільки, по-перше, кожна модель є унікальною на кількісному й якісному рівнях. По-друге, у розглянутих підходах не розглядається поведінковий аспект системи. На наш погляд, саме він є основним показником результативності міжагентної взаємозалежності у CAS [2; 4; 5].

Питання безпеки КІ з погляду інфраструктурного аналізу з урахуванням системи взаємозв'язків між елементами КВІ під час інфраструктурної деталізації розглядалися у роботі [13].

Питання залежності безпеки інфраструктури від топології розглянуті у [6; 13]. Обґрунтовано це тим, що знання поточної топології мережі має вирішальне значення для інтерпретації вимірів, що виконуються під час моніторингу оцінки стану захищеності систем. З огляду на те, що і випадкові помилки, і навмисні дії можуть змінити топологію, важливим кроком будь-якої оцінки стану системи є аналіз топології для отримання точних вихідних даних для заданого набору вимірювань. Причому дані дії переважно виконуються до оцінки станів системи. Це дозволяє зловмисникам непомітно індукувати та, можливо, повертати зміни топології протягом одного циклу сканування. Авторами розглядаються формальні моделі атаки та завдання оптимізації для мінімізації витрат зловмисників та визначення наслідків індукованих збоїв топології, що призводять до атак типу «відмова в обслуговуванні».

Практично всі досліджувані проблеми у зазначеній сфері супроводжуються відсутністю метрик, що характеризують стан взаємозалежних інфраструктур та ризики інформаційної безпеки (далі – ІБ), пов'язані із взаємозалежностями. Метрики в даному випадку мають дозволяти: 1) виміряти рівень виникаючих у результаті взаємозалежностей ефективів; 2) формувати набір даних; 3) виконувати перевірку моделей; 4) оцінювати ризики ІБ; 5) формувати систему альтернатив на взаємозалежності.

В аналізі взаємозалежностей виділимо ключові характеристики інфраструктури:

– просторові (географічні) масштаби. Можуть варіюються від окремих частин до метаструктури, що складається із взаємозалежних інфраструктур та навколишнього середовища;

– тимчасові масштаби, що дозволяють визначити релевантність взаємозалежності для аналізу;

– операційні фактори, що впливають на реакцію інфраструктури на імпульси;

– організаційні характеристики, що визначають поведінку інфраструктури.

Крім того, згідно з [5; 11] можна розглядати такі характеристики КІ:

1) інфраструктурна стійкість. Ця характеристика визначає поліпшення зв'язку та мобільності, збільшення суспільних вигод та врівноваження соціальних, економічних та екологічних потреб. Також включає відновлення та повторне використання існуючої інфраструктури;

2) критична стійкість інфраструктури. Належить до здатності міста або країни прогнозувати, запобігати та захищати за допомогою скоординованого плану для мережі, оперативних та своєчасних дій щодо відновлення системи, тоді як обхідні загрози забезпечують мінімальний рівень послуг.

Деталізувати роботу із зазначеними характеристиками інфраструктур можна за допомогою ієрархії елементів, що розширює таксономію С. Перроу [8] (рис. 2).

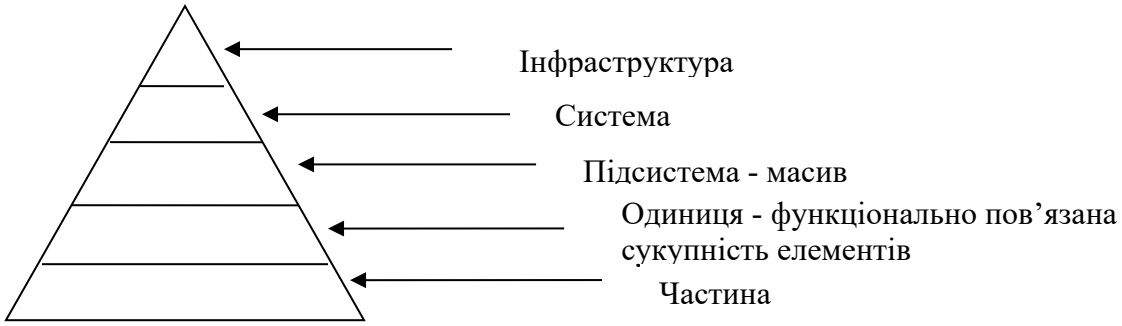

Рис. 2 Ієрархія елементів таксономії інфраструктур (у т.ч. КІ)
Джерело: авторська розробка

Таким чином, у загальному вигляді, безліч станів інфраструктури (у т.ч. КІ) у різних умовах її експлуатації можна розглядати на континуумі, в будь-якій точці якого є залежність між характеристиками елементів таксономії інфраструктур різного рівня і станами інфраструктури. Крім того, у континуумі можна побудувати систему зв'язків між точками значень елементів таксономії та точками наявності збоїв в інфраструктурі в часі.

При побудові континууму особливу увагу варто приділити значенню оптимального проектного стану інфраструктури як самостійної чи інтегративної одиниці. Це значення є важливим в оцінці працездатності та безпеки досліджуваної структури. Крім того, при побудові континууму на «вході» виконується оцінка структури щодо наявності взаємозалежних компонентів у статичному режимі функціонування інфраструктури та при

виникненні імпульсних навантажень. Останнє, своєю чергою, визначає як поведінка системи загалом, а й склад заходів із нейтралізації чи зменшенні можливого результуючого ефекту. Такі складності та невизначеності мають бути виявлені та включені до структури аналізу для вибудовування системи характеристик та вимірювань таксономії інфраструктур.

КІ – це клас інфраструктур, елементи класу якого, структурна організація, підходи до безпеки – відрізняються. Наприклад, поняття «суб'єкт та об'єкт КІ» не є універсальним для міжнародної практики. Воно визначено лише у низці країн. Особливістю європейського підходу є те, що у ньому виділяються дві категорії суб'єктів: оператори життєво важливих послуг та провайдер цифрових послуг. Крім того, при побудові КІ країни, переважно, дотримуються або регулятивного або суб'єктно-діяльнісного підходу [там само].

В Україні об'єктна побудова та розвиток КІ реалізується на секторальній основі. Відповідно до вітчизняного законодавства під суб'єктом КІ розуміється юридична особа – власник об'єктів КІ. Об'єкт КІ – інформаційні системи, телекомунікаційні системи, автоматизовані системи керування. У даному випадку, секторальний підхід, на наш погляд, з одного боку, створює необхідні умови для розвитку КІ, а з другого боку, має суттєвий недолік, який визначається на методологічному рівні. Цей недолік можна усунути за рахунок введення системного підходу до побудови КІ.

Дослідження питань безпеки КІ неможливе без розгляду загальної якості будь-якої матерії – системність. Якщо розглядати КІ як організаційну структуру, то з погляду системного аналізу як основні можна позначити такі структурні показники:

1) оперативність, як здатність КІ швидко реагувати на імпульсні зміни в системі КІ в різних режимах функціонування;

2) централізація, як можливість ефективного виконання керуючих функцій;

3) периферійність як показник топологічної спроможності КІ;

4) життєздатність як здатність зберігати значення основних показників при руйнуванні частини структури;

5) обсяг, як кількість елементів КІ.

При дослідженні структури КІ як системи оцінюють таке: ступінь цілісності, що показує рівень взаємозалежності елементів, стійкості, керованості, а також структурну автономність чи стійкість системи за такою формулою:

$$Сс = З + Св \qquad (1.1)$$

де *Сс* – системна складність, тобто контентне представлення системи у розрізі її використання;

З – власна складність, що представляє собою адитивну оцінку складності елементів у локальному представленні при реалізації поставлених перед системою завдань;

Св – взаємна складність, що визначає рівень взаємозв'язку елементів системи. Важливо, що Св є показником працездатності системи без урахування досягнення поставленої мети.

Із формули (1.1) можна отримати оцінки: α – ступінь цілісності та β – коефіцієнт використання компонентів системи (це формула 1.2):

$$\propto = -\frac{C_в}{C_o}, \beta = \frac{C_c}{C_o},\ \beta = 1 - \alpha \tag{1.2}$$

Оскільки система КІ має ієрархічний характер, можна говорити про заходи, які визначають таке:

1) поділ міжрівневих повноважень (для суміжних рівнів), що визначається за формулою 1.3:

$$\propto_i = \frac{\mu_i}{\mu_{i-1}} \tag{1.3}$$

де μ_i - обсяг завдань (кількість перероблюваної інформації), що розв'язуються на і-м рівні.

Отже, ступінь централізації КІ як системи має такий вигляд:

$$\propto = \sum_{i=1}^{N} q_i \cdot \alpha_i, \sum_{i=1}^{N} q_i = 1 \tag{1.4}$$

де q_i - ваговий коефіцієнт відповідного рівня системи.

Варто відзначити, що чим вище ступінь централізації, тим вище є рівень керованості підсистем й якість управлінських рішень, а також більшою є кількість інформації, з якою виконується робота на верхньому рівні системи. Інакше, якщо підвищується рівень децентралізації, то спостерігається зростання самостійності підсистем і збільшення інформації, з якою виконується робота на нижчих рівнях;

Обсяг завдань, що ефективно виконуються особою, яка приймає рішення – це норма керованості. Такий показник є одним із вирішальних під час виборів структури.

Значення цих показників, у тому числі будуть визначатися рівнем системи та наявністю автоматизованої системи управління. В інтеграційному аналізі КІ як системи вони мають важливе значення. Крім зазначених показників, під час аналізу системи необхідно оцінити її потенціал (можливості). Для вирішення завдань оптимізації цей показник можна розглядати як цільовий.

Для оцінювання потенціалу КІ як системи враховуються її ресурси, які щодо поставленої мети можуть бути як актуалізованими, так і не актуалізованими. Їх характеристика можлива як на кількісному, так і на якісному рівнях. Тобто потенціал КІ, таким чином, можна уявити через актуалізовану та не актуалізовану частини. Виходячи із міри потенціалу, можна буде говорити про складність проблеми управління. Чи не актуалізована частина потенціалу при цьому може розглядатися як додатковий ресурс при реалізації поставленої мети.

У залежності від рівня організованості системи її потенціал $P(S)$, у залежно від потенціалів підсистем $P(S_i)$:

$$\begin{aligned}&((S - \text{добре організована система}) \Rightarrow P(S) > \sum_{i=1}^{N} P(S_i)) \vee \\ &\vee ((S - \text{нейтральна система}) \Rightarrow P(S) = \sum_{i=1}^{N} P(S_i)) \vee \\ &\vee ((S - \text{погано організована система}) \Rightarrow P(S) = \frac{\sum_{i=1}^{N} P(S_i)}{N}) \vee \end{aligned} \quad (1.5)$$

При цьому за інтегративними якостями, системним вимогам найменше відповідають погано організовані системи. Якщо розглядати суб'єкта КІ як організаційну структуру, як суб'єкт управління, то з погляду системного аналізу до суб'єкта КІ представлені структурні показники можна застосувати при виробленні рішень щодо забезпечення безпеки КІ.

Висновки. Таким чином, характеристика складових і принципів побудови КІ, а також її взаємозалежностей впливають на властивості експлуатації такої інфраструктури в умовах імпульсної присутності й здатні призвести до ефекту саморуйнування (деструктивізму) КІ. Серед засад побудови критичної інфраструктури визначені загальні та спеціальні управлінські принципи (результативності, ефективності, науковості, централізованості тощо). Установлено, що зв'язки підсистем КІ можуть призводити до інфраструктурного деструктивізму, тобто мати інфраструктурне походження. У той же час, наполягається, що для України найбільш загрозливими є не внутрішні чинники, а зовнішні, як-то повномасштабна агресія рф. Дії держави-агресора спрямовані на руйнування об’єктів енергетичної, соціальної, транспортної та іншої інфраструктури, значна частина яких входить до складу КІ. Чинники впливу або сприяють адаптованості функціонування об’єктів КІ, або роблять інфраструктуру не гнучкою. Сукупність гнучких структур у складі КІ, на наш погляд, має добре реагувати на зміни в поведінці як факторів, що впливають, так на саму КІ або її складових, і продовжувати надавати необхідні послуги, ніж негнучка, жорстка система. Однак, питання про значущість видів зв'язків у цьому процесі функціонування КІ (у межах «інфраструктурного середовища») вимагає ретельного вивчення та створення нового методологічного підходу. У цьому контексті запропоновано визначення терміноконструкції

інфраструктурного середовище, що представляє собою структуру, яку можна описати з позиції унікальності характеристик, властивих даній структурі як самостійній системі, так і через характеристики інфраструктур, її складових. При цьому наполягається, що між елементами КІ та інфраструктурним середовищем відсутні чіткі межі. Таке середовище слід розглядати також з урахуванням положень теорії інституціоналізму. Вони дозволяють представити інфраструктурне середовище як сукупність факторів, умов та інститутів, що у підсумку забезпечують належне функціонування об'єктів КІ як у мирний час, так і в період невизначеності, або надзвичайного та воєнного стану. Серед цих інститутів можна виокремити правові, соціальні, організаційні та ін.

Література:

1. Помаза-Пономаренко А.Л., Тарадуда Д.В. Забезпечення стійкості системи державного регулювання об'єктів підвищеної небезпеки й об'єктів критичної інфраструктури // Державне управління: удосконалення та розвиток. 2024. № 4. URL: https://www.nayka.com.ua/index.php/dy/article/view/3461. (дата звернення: 12.05.2024).

2. Помаза-Пономаренко А.Л., Тарадуда Д.В. Закордонний досвід забезпечення соціальної безпеки шляхом стійкого функціонування об'єктів критичної інфраструктури та підвищеної небезпеки // Наука і техніка сьогодні. 2024. № 4 (32). С. 371-384.

3. Помаза-Пономаренко А.Л., Тарадуда Д.В. Механізми забезпечення цивільної безпеки України: аспекти попередження НС на об'єктах військово-промислового комплексу // Публічне адміністрування та національна безпека. 2024. № 3 (44). https://www.inter-nauka.com/issues/administration2024/3/9732. (дата звернення: 16.05.2024).

4. Помаза-Пономаренко А.Л., Тарадуда Д.В. Щодо забезпечення цивільної безпеки об'єктів військово-промислового комплексу України в умовах військових конфліктів // Матеріали IV Міжнародної наукової конференції «Воєнні конфлікти та техногенні катастрофи: історичні та психологічні наслідки» (18-19.04.2024 р., м. Тернопіль). С. 123–126.

5. Identifying, Understanding and Analyzing. Retrieved from http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.

6. Leclaire, R.J. (2014). Infrastructure Modeling: Status and Applications. *In: Sustainable Cities and Military Installations. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht*. 391–427.

7. Lei, Yu., Peer-Ola, S. & Aickelin, U. (2012). Modelling Electrical Car Diffusion Based on Agent. *International Journal of Digital Content Technologyand its Applications*. 6. 424–431.

8. Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.

9. Pomaza-Ponomarenko, A., Taraduda, D., Leonenko, N., Poroka, S. & Sukhachov, M. (2024). Ensuring the safety of citizens in times of war: aspects of the organization of civil defense. *AD ALTA: Journal of Interdisciplinary Research.* 14. 216–220.

10. Popov, O., Taraduda, D., Sobyna, V., Dement, M. & Pomaza-Ponomarenko, A. (2020). Emergencies at Potentially Dangerous Objects Causing Atmosphere Pollution: Peculiarities of Chemically Hazardous Substances Migration. Systems, Decisions and Control in Energy I. *Studies in Systems, Decision and Control. Switzerland: Springer International Publishing AG.* 298. 151–163.

11. Steven M., Peerenbom, J.P. & Kelly, T.K. (2001). Critical Infrastructure Interdependencies. Retrieved from https://ru.scribd.com/document/330799700/CII-Rinaldi-pdf.

12. Subramanian, A.S.R., Gundersen, T. & Adams, T.A. (2018). Modeling and Simulation of Energy Systems: A Review. *Processes*. 2018. 6 (12). 238.

13. Jalaliniya, S. & Fakhredin, F. (2011). Enterprise Architecture & Security Architecture. Retrieved from https://www.researchgate.net/publication/257934615_Enterprise_Architecture_Security_Architecture_Development.

References:

1. Pomaza-Ponomarenko, A.L. & Taraduda, D.V. (2024). Zabezpechennya stiykosti systemy derzhavnoho rehulyuvannya ob″yektiv pidvyshchenoyi nebezpeky y ob″yektiv krytychnoyi infrastruktury [Ensuring the stability of the system of state regulation of objects of increased danger and objects of critical infrastructure]. *Derzhavne upravlinnya: udoskonalennya ta rozvytok – State management: improvement and development.* 4. Retrieved from https://www.nayka.com.ua/index.php/dy/article/view/3461. [in Ukrainian].

2. Pomaza-Ponomarenko, A.L. & Taraduda, D.V. (2024). Zakordonnyy dosvid zabezpechennya sotsial′noyi bezpeky shlyakhom stiykoho funktsionuvannya ob″yektiv krytychnoyi infrastruktury ta pidvyshchenoyi nebezpeky [Foreign experience of ensuring social security through the sustainable functioning of critical infrastructure objects and increased danger]. *Science and technology today.* 4. 371–384. [in Ukrainian].

3. Pomaza-Ponomarenko, A.L. & Taraduda, D.V. (2024). Mekhanizmy zabezpechennya tsyvil′noyi bezpeky Ukrayiny: aspekty poperedzhennya NS na ob″yektakh viys′kovo-promyslovoho kompleksu [Mechanisms for ensuring civil security of Ukraine: aspects of emergency prevention at the facilities of the military-industrial complex]. *Publichne administruvannya ta natsional'na bezpeka – Public administration and national security*. 3 (44). Retrieved from https://www.inter-nauka.com/issues/administration2024/3/9732. [in Ukrainian].

4. Pomaza-Ponomarenko, A.L. & Taraduda, D.V. (2024). Shchodo zabezpechennya tsyvil′noyi bezpeky ob″yektiv viys′kovo-promyslovoho kompleksu Ukrayiny v umovakh viys′kovykh konfliktiv [Regarding the provision of civilian security of the objects of the military-industrial complex of Ukraine in the conditions of military conflicts]. Proceedings from MIIM '12: IV Mizhnarodnaya naukova konferentsiya «Voyenni konflikty ta tekhnohenni katastrofy: istorychni ta psykholohichni naslidky» – The 4th International Scientific Conference «Military conflicts and man-made disasters: historical and psychological consequences». (pp. 123–126). Ternopil: TNTU. [in Ukrainian].

5. Identifying, Understanding and Analyzing. Retrieved from http://www.ce.cmu.edu/~ hsm/ im2004/readings/CII-Rinaldi.pdf.

6. Leclaire, R.J. (2014). Infrastructure Modeling: Status and Applications. *In: Sustainable Cities and Military Installations. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht*. 391–427.

7. Lei, Yu., Peer-Ola, S. & Aickelin, U. (2012). Modelling Electrical Car Diffusion Based on Agent. *International Journal of Digital Content Technologyand its Applications*. 6. 424–431.

8. Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.

9. Pomaza-Ponomarenko, A., Taraduda, D., Leonenko, N., Poroka, S. & Sukhachov, M. (2024). Ensuring the safety of citizens in times of war: aspects of the organization of civil defense. *AD ALTA: Journal of Interdisciplinary Research.* 14. 216–220.

10. Popov, O., Taraduda, D., Sobyna, V., Dement, M. & Pomaza-Ponomarenko, A. (2020). Emergencies at Potentially Dangerous Objects Causing Atmosphere Pollution: Peculiarities of Chemically Hazardous Substances Migration. Systems, Decisions and Control in Energy I. *Studies in Systems, Decision and Control. Switzerland: Springer International Publishing AG.* 298. 151–163.

11. Steven M., Peerenbom, J.P. & Kelly, T.K. (2001). Critical Infrastructure Interdependencies. Retrieved from https://ru.scribd.com/document/330799700/CII-Rinaldi-pdf.

12. Subramanian, A.S.R., Gundersen, T. & Adams, T.A. (2018). Modeling and Simulation of Energy Systems: A Review. *Processes*. 2018. 6 (12). 238.

13. Jalaliniya, S. & Fakhredin, F. (2011). Enterprise Architecture & Security Architecture. Retrieved from https://www.researchgate.net/publication/257934615_Enterprise_Architecture_Security_Architecture_Development.