УДК 351.863+338.246.87
DOI: 10.30838/UJCEA.2312.301024.92.1097

ОЦІНКА РИЗИКІВ ВИНИКНЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ В ЕНЕРГЕТИЧНОМУ СЕКТОРІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

КІЧАТА Н. М.[1*], *ас.*,
ТРЕТЬЯКОВ О. В.[2], *докт. техн. наук, проф.*

[1*] Кафедра цивільної та промислової безпеки ім. Героя України Олександра Сергійовича Чуба, Національний авіаційний університет, пр. Любомира Гузара 1, 03058, Київ, Україна, тел. +38 (066) 185-05-05, e-mail: naturly@ukr.net, ORCID ID: 0000-0002-6991-3970
[2] Кафедра цивільної та промислової безпеки ім. Героя України Олександра Сергійовича Чуба, Національний авіаційний університет, пр. Любомира Гузара 1, 03058, Київ, Україна, тел. +38 (097) 342-31-80, e-mail: mega_ovtr@ukr.net, ORCID ID: 0000-0002-0457-9553

Анотація. ***Постановка проблеми.*** Для ефективного підвищення безпеки об'єктів критичної інфраструктури в енергетичному секторі потрібно оцінити всі загрози та проаналізувати сценарії загроз для самого об'єкта. Загрози енергетичній безпеці – це можливість виникнення короткочасних або тривалих ситуацій, реальних або потенційних факторів, явищ та подій, які можуть порушити стабільність та безпеку енергетичного сектора країни. Ці загрози можуть спричинити обмеження або порушення енергозабезпечення споживачів, аварії та інші негативні наслідки. У багатьох випадках вихід із ладу одного об'єкта або системи вплине на здатність взаємопов'язаних об'єктів або систем у тому чи іншому секторі виконувати свої функції. Для відносно стаціонарної системи важливо визначити ті компоненти або критичні вузли, де потенційні наслідки будуть найвищими і де потрібно зосередити заходи із безпеки та стійкості. ***Мета статті*** – розроблення і впровадження підходу до визначення ризиків надзвичайної ситуації на об'єктах критичної інфраструктури на прикладі Долинського газопереробного заводу (ГПЗ). ***Висновки.*** Розроблено і впроваджено підхід до визначення та оцінювання ризиків критичної інфраструктури енергетичного сектора, за допомогою якого виявляються потенційні вразливості об'єкта перед різними загрозами. Побудовано імітаційну модель для каскадних ефектів, яка дозволяє отримати ймовірнісні оцінки розвитку подій за визначеними сценаріями для об'єкта критичної інфраструктури.

Ключові слова: *критична інфраструктура; ризики; загроза; енергетичний сектор; стійкість*

ASSESSMENT OF THE RISKS OF EMERGENCY SITUATIONS IN THE ENERGY SECTOR OF CRITICAL INFRASTRUCTURE

KICHATA N.M.[1*], *Ass.*,
TRETYAKOV O.V[2], *Dr. Sc. (Tech.)., Prof.*

[1*] Department of Civil and Industrial Security named after the Hero of Ukraine Oleksandr Serhiyovych Chub, National Aviation University, 1, Lubomyra Huzar Ave., Kyiv, 03058, Ukraine, tel. +38 (066) 185-05-05, e-mail: naturly@ukr.net, ORCID ID: 0000-0002-6991-3970
[2] Department of Civil and Industrial Security named after the Hero of Ukraine Oleksandr Serhiyovych Chub, National Aviation University, 1, Lubomyra Huzar Ave., Kyiv, 03058, Ukraine, tel. +38 (097) 342-31-80, e-mail: mega_ovtr@ukr.net, ORCID ID: 0000-0002-0457-9553

Abstract. ***Problem statement.*** In order to effectively increase the security of critical infrastructure in the energy sector, it is necessary to assess all threats and analyze threat scenarios for the facility itself. Threats to energy security are the possibility of short-term or long-term situations, real or potential factors, phenomena or events that may disrupt the stability and security of the country's energy sector. These threats can lead to restriction or disruption of energy supply to consumers, accidents and other negative consequences. In many cases, the failure of one facility or system will affect the ability of interconnected facilities or systems in the same or another sector to perform their functions. For a relatively stationary system, it is important to identify those components or critical nodes where the potential consequences will be highest and where security and resilience efforts need to be focused. The purpose of the article is to develop and implement an approach to determining the risks of an emergency situation at critical infrastructure facilities using the example of the Dolyna Gas Processing Plant (GPP). Conclusions. An approach to identifying and assessing the risks of the critical infrastructure of the energy sector was developed and implemented, with the help of

which potential vulnerabilities of the object to various threats are revealed. A simulation model for cascading effects has been built, which allows obtaining probabilistic estimates of the development of events under defined scenarios for a critical infrastructure object.

Keywords: *critical infrastructure; risks; threats; energy sector; sustainability*

Постановка проблеми. Забезпечення безпеки енергетики країни – це один із важливих, але складних аспектів системи управління державою у контексті національної безпеки. Об'єкти енергетики – ключові у забезпеченні функціонування підприємств усіх галузей економіки та задоволенні потреб в енергоресурсах для населення і соціально значущих установ.

Часто неможливо точно визначити збиток об'єктів критичної інфраструктури, який може виникнути внаслідок певної події, оскільки потенційних загроз та ризиків є величезна кількість. Крім того, збиток часто не обмежується лише матеріальними втратами, які можна виразити у грошовому еквіваленті, а й включає нематеріальні аспекти, що ускладнюють точну оцінку. Також досить складно точно визначити ймовірність виникнення небезпечної події, тому можна розглядати лише оцінки цих значень замість точних даних. Для досягнення надійних результатів важливо правильно визначити параметри та вхідні дані для проведення моделювання. Саме через це відсутність однієї загальновизнаної методики визначення ризиків надзвичайних ситуацій на критичних інфраструктурних об'єктах постає важливою проблемою.

Тому застосування імітаційної моделі для каскадних ефектів дозволяє отримати ймовірнісні оцінки розвитку подій за визначеними сценаріями та провести оцінення загроз для об'єктів критичної інфраструктури, враховуючи імовірність настання подій і переходів між ними.

Аналіз останніх досліджень. Дослідження питань, пов'язаних з оцінкою ризиків виникнення надзвичайних ситуацій в енергетичному секторі критичної інфраструктури, наразі дуже актуальне. В сучасних умовах війни і загроз національній безпеці України в енергетичній сфері необхідно забезпечити технологічну, технічну та економічну стійкість кожної державної системи. Вчасне виявлення та запобігання загрозам об'єктам критичної інфраструктури становить важливу частину державної політики щодо їх захисту.

Злагоджені дії державних органів у сфері прогнозування ризиків та протидія загрозам забезпечують надійний захист критичних об'єктів. Потребу інтеграції цих процедур у державну політику захисту критичної інфраструктури розглядали науковці Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов, О. М. Суходоля [1]. Вони наголошують на важливості раннього виявлення та управління ризиками як ключових елементів безпеки критичної інфраструктури.

Комплексна оцінка ризиків може бути виправдана для всіх або більшості критично важливих елементів інфраструктури в певних районах, де можливі наслідки від порушень, руйнування або неправильної експлуатації особливо серйозні. Процедуру перевірки слід застосовувати до всіх інших складових інфраструктури, щоб зменшити навантаження на ті елементи, які можуть не потребувати повного аналізу ризиків.

Надзвичайні ситуації різного характеру суттєво впливають на соціальні, економічні, політичні та інші процеси в суспільстві. Тому управління ризиками в умовах різних надзвичайних ситуацій стає ключовим для об'єктів критичної інфраструктури з метою забезпечення стабільного розвитку та національної безпеки країни. Сучасний стан справ, упровадження новітніх технологій (особливо інформаційних), а також поява нових ризиків і загроз (зокрема, воєнних дій) вказують, що роль держави та її органів управління в цій сфері буде зростати в майбутньому.

Енергетичні системи організовані по-різному в кожній країні, але електромережа зазвичай складається з мережі окремих і фізично відокремлених об'єктів

інфраструктури, які є ключовими для виробництва, передачі, розподілу та контролю енергії. Часто вихід із ладу одного з компонентів (наприклад, електростанцій) спричинює збій усіх наступних компонентів, що в результаті викликає перебої в наданні цих послуг і всіх пов'язаних із ними послуг, що залежать від енергопостачання.

Наразі зростання загрози щодо зниження рівня безпеки важливих об'єктів критичної інфраструктури в Україні стало наслідком надмірної експлуатації споруд, конструкцій, обладнання та інженерних мереж, які вже досягли або перевищили свій проектний термін використання. Це створює серйозні ризики виникнення надзвичайних ситуацій природного або техногенного походження, що загрожують безпеці функціонування об'єктів критичної інфраструктури.

Мета статті – розроблення і впровадження підходу до визначення ризиків надзвичайної ситуації на об'єктах критичної інфраструктури на прикладі Долинського газопереробного заводу (ГПЗ).

Результати досліджень. Розроблено імітаційну модель для каскадних ефектів Долинського ГПЗ, яка дозволяє отримати ймовірнісні оцінки розвитку небезпечних подій за визначеними сценаріями.

Математична модель будується шляхом проведення таких процедур:

− визначення подій у сценарії розвитку ситуації (компоненти сценарію, що можуть мати потенційний вплив на реалізацію загрози);

− визначення множини можливих станів подій, що впливають на рівень загрози;

− формування сценаріїв розвитку загрози (визначення послідовних кроків, які ведуть до виникнення загрози) через індивідуальні елементи, що формують ланцюжки подій та їх переходи до заданих станів, це представлено у структурно-логічній моделі розвитку кризової ситуації з різними варіантами розвитку сценарію на прикладі об'єктів критичної інфраструктури;

− формування оргграфа сценаріїв загроз (структурно-логічна модель, що охоплює всі можливі сценарії реалізації загрози);

− оцінення ймовірностей різних подій і переходів між ними;

− оцінення ймовірності реалізації сценаріїв загроз.

Алгоритм реалізації цього підходу можна відобразити таким чином:

1. Індентифікація небезпечних подій у сценарії розвитку ситуації (аспекти сценарію, які можуть вплинути на здійснення загрози).

Визначення подій у сценарії розвитку ситуації передбачає аналіз різних складових елементів, які можуть впливати на реалізацію загрози. Ці події можуть включати в себе такі явища як кібератаки, природні катастрофи, технічні збої, терористичні акти тощо. Позначимо множину таких елементів:

$$I = \{1, 2, \dots, n\}.$$

Паливно-енергетичний комплекс Долинський газопереробний завод публічного акціонерного товариства «Укрнафта» піддається багатьом ризикам.

Загрози для цього об'єкта такі: неконтрольована вирубка лісів у даному регіоні, яка спричинює повені, зсуви; для Долинського району характерні землетруси; застаріле устаткування у системі виробництва, яке може викликати збої апаратного забезпечення; кібератаки; пожежі; теракти; зменшення обсягів видобутку стає приводом до скорочення робочих місць; загроза від воєнних дій; фінансово-економічна скрута; соціальне напруження через не завжди лояльне ставлення місцевої влади до виробничників.

Ідентифікація ризиків в енергетичному секторі – неперервний процес, оскільки зовнішнє та внутрішнє середовище постійно зазнають змін. Ці зміни можуть створювати нові ризики або змінювати вже відомі.

2. На основі цих подій визначаються множини можливих станів подій на Долинському газопереробному заводі S_i – фактор небезпечної події, $S_{j,k}$ – індекси, які відповідають станам безпеки або небезпеки

об’єкта критичної інфраструктури для даної події.

До головних підрозділів Долинського виробництва належать дільниці компресування газу, переробки газу, зберігання сировини і готової продукції, відвантаження готової продукції, автогазонаповнювальна станція для реалізації газу на теренах Західної України. Основні технологічні об’єкти Долинського ГПЗ: компресорна станція, маслоабсорбційна та газофракційна установки.

Для забезпечення безперервного циклу Долинського ГПЗ на всіх його етапах виділено низку пріоритетних проектів у рамках напрямів: будівництва та капітального ремонту наземної інфраструктури, сервісного обслуговування, виробництва та ремонту газового обладнання, проведення робіт зі збільшення продуктивності свердловин, пошуку і розвідки родовищ газу. Окремим важливим напрямом діяльності компанії залишається реалізація газу та продуктів його переробки.

3. Наступним етапом створюється структурно-логічна модель розвитку кризової ситуації з можливими сценаріями на об’єкті. Це може бути представлено у вигляді графа, де вузли відповідають різним станам системи, а ребра – переходам між ними (рис. 1).

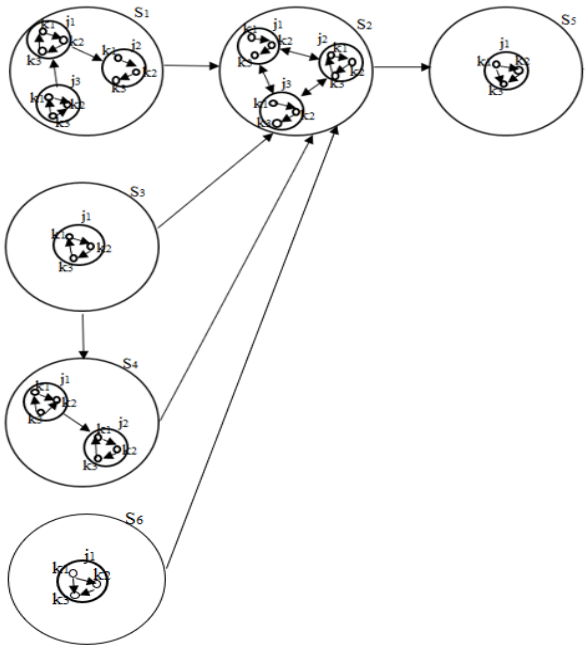

Рис. 1. Модель розвитку кризової ситуації унаслідок впливу небезпек на газопереробному заводі у вигляді оргграфа

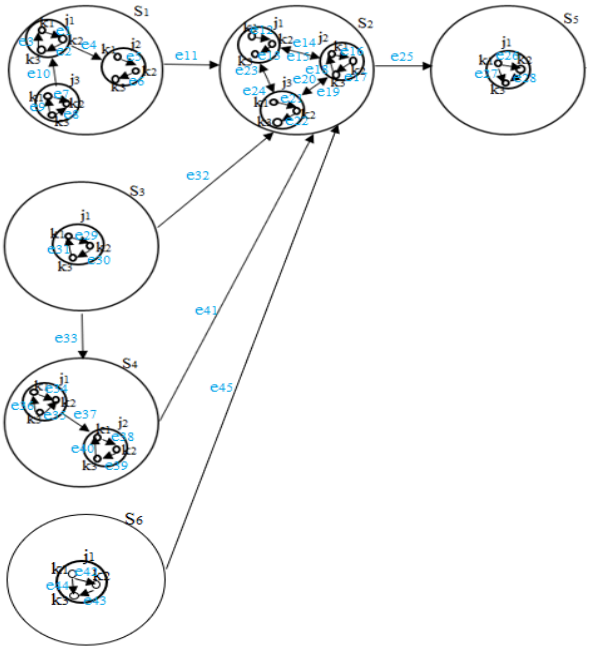

Рис. 2. Оргграф сценаріїв розвитку надзвичайних ситуацій на Долинському ГПЗ із визначенням імовірностей переходів подій

На рисунку 1 визначена $S = \{S_i\}$ – множина загальних небезпек різних факторів, де i – кількість елементів факторів (S_1 – природні, S_2 – техногенні, S_3 – кібератаки, S_4 – терористичні акти, S_5 – соціально-політичні фактори, S_6 – атака БПЛА); $J = \{j_n\}$ – множина небезпек одного фактора, де n – кількість елементів фактора (зсув, повінь, землетрус, пожежа, вибух, збій апаратного забезпечення, хакерська атака, теракт, масовий протест, атака БПЛА); $K = \{K_n\}$ – множина небажаних подій на різних дільницях газопереробного заводу, де n – кількість дільниць газопереробного заводу.

4. Після створення моделі розвитку кризової ситуації можна визначити всі можливі сценарії загроз на Долинському ГПЗ. Будуємо структурно-логічну модель у вигляді орграфа, яка відображає переходи одних подій в інші через їх послідовності та взаємозв’язки.

На рисунку 2 події зображені як вузли з відповідними ребрами (e_1, e_2, e_n). Кожне ребро e_n вказує на можливий шлях або перехід між конкретними станами системи, відображаючи рух від одного стану до іншого згідно з послідовністю подій.

5. Наступним кроком стає оцінення ймовірностей станів подій у сценарії загроз для Долинського ГПЗ. Для розрахунку ймовірнісних оцінок використовуємо статистичні дані щодо нашого об'єкта за певний період.

Припустимо, що стан події $i \in I$ описується дискретною випадковою величиною x_i. Позначимо $p_i(s)$ – ймовірність перебування події , $i \in I$ в стані $s \in S_i$, тобто,

$$p_i(s) = P\{x_{ijk} = s\}, s \in S_i.$$

Кожне ребро орієнтовного графа буде мати відповідне значення P_{jk} де $0 \leq P \leq 1$. Припустимо, що величини x_i, $i \in I$ стохастично незалежні, а ймовірності $p_i(s) = P\{x_{ijk} = s\}, s \in S_i$ задані на основі статистичних даних. Тоді ймовірності переходів від однієї події до іншої подамо у вигляді значень, наведених у таблиці 1.

Таблиця 1

Матриця характеристики небезпечних подій

$Ps_1j_1k_1k_2$ (e_1)	$Ps_1j_1k_2k_3$ (e_2)	$Ps_1j_1k_3k_1$(e_3)	$Ps_1j_1j_2$ (e_4)	$Ps_1j_2k_1k_2$ (e_5)	$Ps_1j_2k_2k_3$ (e_6)	$Ps_1j_3k_1k_2$ (e_7)
0,25	0,25	0,25	0,2	0,6	0,6	0,1
$Ps_1j_3k_3k_2$ (e_8)	$Ps_1j_3k_3k_1$ (e_9)	$Ps_1j_3j_1$ (e_{10})	Ps_1s_2 (e_{11})	$Ps_2j_1k_1k_2$ (e_{12})	$Ps_2j_1k_2k_3$ (e_{13})	$Ps_2j_1j_2$ (e_{14})
0,1	0,1	0,1	0,6	0,2	0,2	0,1
$Ps_2j_2j_1$ (e_{15})	$Ps_2j_2k_1k_2$ (e_{16})	$Ps_2j_2k_2k_3$ (e_{17})	$Ps_2j_2k_3k_1$ (e_{18})	$Ps_2j_2j_3$ (e_{19})	$Ps_2j_3j_2$ (e_{20})	$Ps_2j_3k_1k_2$ (e_{21})
0,1	0,2	0,2	0,1	0,2	0,1	0,01
$Ps_2j_3k_2k_3$ (e_{22})	$Ps_2j_3j_1$ (e_{23})	$Ps_2j_1j_3$ (e_{24})	Ps_2s_5 (e_{25})	$Ps_5j_1k_1k_2$ (e_{26})	$Ps_5j_1k_1k_3$ (e_{27})	$Ps_5j_1k_2k_3$ (e_{28})
0,01	0,1	0,2	0,2	0,2	0,1	0,1
$Ps_3j_1k_1k_2$ (e_{29})	$Ps_3j_1k_2k_3$ (e_{30})	$Ps_3j_1k_3k_1$ (e_{31})	Ps_3s_2(e_{32})	Ps_3s_4(e_{33})	$Ps_4j_1k_1k_2$ (e_{34})	$Ps_4j_1k_3k_2$ (e_{35})
0,18	0,18	0,18	0,1	0,5	0,35	0,35
$Ps_4j_1k_3k_1$ (e_{36})	$Ps_4j_1j_2$ (e_{37})	$Ps_4j_2k_1k_2$ (e_{38})	$Ps_4j_2k_2k_3$ (e_{39})	$Ps_4j_2k_3k_1$ (e_{40})	Ps_4s_2(e_{41})	
0,35	0,35	0,6	0,6	0,6	0,6	
$Ps_6j_1k_1k_2$ (e_{42})	$Ps_6j_1k_2k_3$ (e_{43})	$Ps_6j_1k_1k_3$ (e_{44})	Ps_6s_2(e_{45})			
0,6	0,6	0,6	0,6			

На основі аналізу даних визначаються числові значення ймовірностей для кожного стану події та кожного можливого переходу між станами. Ймовірності можуть бути виражені у відсотках, дробах або інших формах, залежно від потреб моделювання. Аналіз даних відбувається на основі статистичних даних.

Звичайно природні фактори тісно пов'язані з техногенними. Ймовірність переходу природної надзвичайної ситуації в техногенну на Прикарпатті може бути визначена шляхом аналізу різноманітних факторів, таких як географічне положення, природні умови, техногенна інфраструктура.

Долина розташована в гірському регіоні, це збільшує ризик природних небезпек (як зсуви, повені) на інфраструктуру промислових підприємств. Згідно з інформаційно-аналітичною довідкою про надзвичайні ситуації в Україні у 2023 році на Прикарпатті за рік було

зафіксовано сім надзвичайних ситуацій природного характеру [2].

Наприклад, у 2017 році в с. Витвиця відбулися зсуви середньої швидкості, сам завод не зачепило. Останній зсув у Долинському регіоні був у 2021 р. на дорозі Р-21 Долина–Хуст.

Паводки на карпатських річках повторюються 4–5 разів на рік [3]. За останні чотири роки найбільші повені на території Івано-Франківської області відбувалися в 2020 р. (в таких районах як Надвірнянський, Калуський, Коломийський були зафіксовані значні паводки, які призвели до руйнувань і затоплень населених пунктів, доріг та інфраструктури). У травні 2021 р., через значні опади у вигляді дощу та місцями граду, на території Івано-Франківської області відбулися різкі підйоми рівнів води в басейнах річок Дністер та Прут. Внаслідок негоди в м. Калуш підтоплено та пошкоджено житлові будинки; затоплено понад 6,3 тис. присадибних ділянок, пошкоджено с/г угіддя, розмито береги. У червні 2023 р., внаслідок інтенсивних дощів із штормовим вітром у Івано-Франківському, Коломийському, Косівському, Калуському районах відбувся різкий підйом рівнів води в потічках і гірських ріках басейну Прута та Дністра [4].

Сейсмічна активність фіксується постійно, але більшість землетрусів не відчутна. Останній раз сейсмічні поштовхи в м. Долина відчувались у 2020 р., потужність склала 3,2 за шкалою Ріхтера [5].

Промислові трубопроводи відіграють ключову роль у газовій промисловості, найчастіше пожежі відбуваються саме на них. Підприємства, які займаються видобуванням, транспортуванням та переробкою нафти, – основні джерела техногенних ризиків. Це пов’язано з викидами шкідливих речовин та виникненням аварійних ситуацій, таких як вибухи та пожежі.

Багатокілометрові промислові трубопроводи на нафтових і газових родовищах створюють потенційні загрози аварій. Щорічно на газопромислових трубопроводах стається одна – дві аварії. Магістральні газопроводи – надзвичайно вибухонебезпечні об’єкти. На Долинському ГПЗ в магістральні газопроводи подається відбензинений осушений газ. Аварійний викид газу на одному магістральному газопроводі може спричинити ураження сусідніх газопроводів через вибух газової хмари [6].

Ймовірність виникнення пожежі на Долинському ГПЗ наразі, досить низька, завод виконує всі функції і відповідає усім вимогам нормативно-технічної документації. У роботі магістральних газопроводів відмови трубопроводів вважаються рідкісними та випадковими подіями. Їх частота та тривалість ліквідації значно залежать від місця розташування та умов експлуатації газопроводу.

Збої апаратного забезпечення на газопереробних заводах можуть виникати з різних причин, таких як технічні несправності, зношення або вік обладнання, неправильна експлуатація, вплив природних факторів чи людські помилки.

На Долинському ГПЗ в 2019 році було виявлено низку технічних неполадок, серед яких простежувалась невисока якість газових продуктів та відбувалось неефективне використання ресурсів, у 2020 році проведено планові ремонтні роботи на підприємстві. У 2021 році на цьому ГПЗ виконано роботи з реконструкції технологічного обладнання системи продувки установки сепарації газу. У 2023 році виконано регенерацію каталізатора, який пропрацював на заводі понад три роки (при терміні безперервної роботи 2–2,5 року) [7]. Тому наразі Долинський ГПЗ перебуває в модернізованому стані.

Серед потенційних небезпек особливе занепокоєння викликають спроби незаконного впливу на автоматизовані системи керування технологічними процесами на підприємствах та об’єктах інфраструктури; російсько-Українська кібервійна почалася з 2014 року. Долинський ГПЗ також зазнав втручання,

були виведені з ладу сервери та мережеві комутатори [7].

У 2020-му хакери атакували дата-центр «Укрнафти», як наслідок добу не працювали вебсайт акціонерного товариства «Укрнафта» (Долинський ГПЗ є структурною одиницею «Укрнафти»), в 2024 р. стався кібернапад на мережі та сервери газопостачальних компаній «Нафтогаз України» та «Газмережі», добу компанії не мали доступу до своєї інформаційної бази [8].

На жаль, загроза вчинення терактів залишається вкрай серйозною для України на сьогодні. Російські терористи продовжують атакувати всі об'єкти критичної інфраструктури по всій Україні, здійснюючи масовані ракетні обстріли по енергетичних об'єктах критичної інфраструктури. Івано-Франківська область також зазнає нападу терористів (жовтень 2022 р., грудень 2022 р., березень 2024 р., квітень 2024 р.) [9]. Оскільки напрямок прильоту ракети не може бути спрогнозованим, ймовірність ризику залишається досить високою.

Безпілотні літальні апарати (БПЛА) 26 лютого 2022 р. пошкодили газопровід на Шебелинському газопереробному заводі, через ризики воєнних дій роботу було зупинено. У лютому 2024 р. знову Шебелинське відділення з переробки газового конденсату і нафти було пошкоджене ворожими дронами.

Атака на газотранспортну систему може призвести до гуманітарної катастрофи серед цивільного населення та повністю паралізувати промислову діяльність. Газотранспортна система – одна з найбільш вразливих енергетичних систем, відновлення роботи якої вимагатиме тривалого часу. Крім того, атаки на газові сховища можуть мати катастрофічні наслідки.

Статистичні дані дозволяють отримати об'єктивне уявлення про розподіл, зв'язки та взаємозалежності між різними явищами.

Оцінення ймовірності реалізації сценаріїв загроз на Долинському ГПЗ стало завершальним етапом у процесі управління ризиками і забезпечення стійкості критичної інфраструктури.

Ймовірність виникнення сценаріїв загроз можна розрахувати, використовуючи теорему повної ймовірності [55]:

$$P_{\text{сценарію}} = 1 - \prod(1 - P_{ijk}), (i \in A_k)\,. \quad (1)$$

Відповідно даних із таблиці 1 та використовуючи формулу 1, отримуємо результати оцінювання ймовірності реалізації сценаріїв загроз для Долинського ГПЗ.

Таблиця 2

Результати розрахунків оцінювання сценаріїв

Сценарії загроз	Ймовірність виникнення
P_1 (S_1, S_2, S_5)	0,998 885
P_2 (S_3, S_2, S_5)	0,96
P_3 (S_3, S_4 S_2, S_5)	0,99 994
P_4 (S_6, S_2, S_5)	0,9979

Таким чином, можна визначити найбільш критичний сценарій загроз для заводу та виявити ключові події, які можуть спричинити інші каскадні ефекти. Аналізуючи отримані дані для Долинського ГПЗ, можна дійти висновку, що ймовірність реалізації будь-якого з цих сценаріїв досить висока.

Висновки.

Розроблена модель дозволяє оцінити значущість ризиків для Долинського ГПЗ та визначити потенційні загрози каскадних ефектів у різних можливих сценаріях подій на об'єкті критичної інфраструктури.

Для аналізу можливих наслідків загрози слід опиратися на інформацію про минулі інциденти, а також використовувати результати прогнозування негативних наслідків або моделювання кризових сценаріїв, які можуть виникнути в разі реалізації потенційних загроз.

Потенційні загрози каскадних ефектів можуть спровокувати ситуації, коли одна подія запускає послідовні ланцюгові реакції, що підсилюють її вплив і наслідки на об'єкт критичної інфраструктури. Це виявлення дозволить розробити управлінські заходи для запобігання та усунення таких небезпек у майбутньому.

Наприклад, упровадження системи моніторингу раннього виявлення потенційних небезпек (автоматизовані системи управління для виявлення аномалій); забезпечення охорони об’єктів, включаючи охоронні системи, відеоспостереження та контроль доступу, укріплення конструкцій та встановлення захисних бар’єрів для захисту від фізичних атак; упровадження сучасних засобів кіберзахисту, регулярне оновлення програмного забезпечення та проведення тестувань на вразливість об’єкта; розроблення та впровадження планів реагування на надзвичайні ситуації; встановлення резервних джерел електроживлення; підтримка запасів важливих матеріалів та запасних частин для швидкого ремонту обладнання; регулярне технічне обслуговування та перевірка обладнання для запобігання несправностям.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. Київ : НІСД, 2019. 224 с.

2. Іванець Г. В. Аналіз стану техногенної, природної та соціальної небезпеки адміністративно-територіальних одиниць України на основі даних моніторингу. *Збірник наукових праць Харківського університету Повітряних Сил*. 2016. Вип. 3 (48). С. 142–145.

3. Звіт про оцінку можливих наслідків для довкілля від реалізації Стратегії розвитку Долинського субрегіону на період до 2027 року. Київ, 2017. URL: http://pleddg.org.ua/wp-content/uploads/2020/12/Skrining_Dol.pdf (дата звернення : 19.04.2024).

4. Інформаційно-аналітична довідка про надзвичайні ситуації в Україні у 2023 році. URL: https://dsns.gov.ua/upload/2/0/2/2/3/1/4/2023-rik.pdf (дата звернення : 19.04.2024).

5. Головний центр спеціального контролю. URL: https://gcsk.gov.ua/ya-vidchuv-zemletrus/ (дата звернення: 19.04.2024).

6. Енергетика. Івано-Франківська обласна державна адміністрація : офіційний веб-сайт Івано-Франківської обласної державної адміністрації. URL: http://www.if.gov.ua/modules.php?name=Content&pa=showpage& pid=728 (дата звернення : 19.04.2024).

7. Лазоришин І. Долинський газопереробний завод продовжує надійно працювати. 17.08.2020. *Агенція новин.* URL: https://firtka.if.ua/blog/view/bogdan-deputat-nezvazhaiuchi-na-covid-19-ta-ekonomichnu-krizu-dolinskii-gazopererobnii-zavod-prodovzhuie-nadiino-pratsiuvati (дата звернення : 19.04.2024).

8. Об'єкти «Нафтогазу» на заході України пошкоджено внаслідок ранкової атаки рф. *Інтерфакс.* URL: https://interfax.com.ua/news/economic/975650.html (дата звернення : 19.04.2024).

9. Вікіпедія. Удари по об'єктах критичної інфраструктури України під час російсько-української війни. URL: https://uk.wikipedia.org (дата звернення : 19.04.2024).

10. Іванюта С. П., Качинський А. Б. Екологічна та природно-техногенна безпека України : регіональний вимір загроз і ризиків : монографія. Київ : НІСД, 2012. 308 с.

REFERENCES

1. Bobro D.H., Ivaniuta S.P., Kondratov S.I. and Sukhodolia O.M. *Orhanizatsiini ta pravovi aspekty zabezpechennia bezpeky i stiikosti kry-tychnoi infrastruktury Ukrainy : analit. dop.* [Organizational and legal aspects of ensuring the safety and stability of critical infrastructure of Ukraine: analyst. add.]. Kyiv : NISD Publ., 2019, 224 p. (in Ukrainian).

2. Ivanets H.V. *Analiz stanu tekhnohennoi, pryrodnoi ta sotsialnoi nebezpeky administratyvno-terytorialnykh odynyts Ukrainy na osnovi danykh monitorynhu* [Analysis of the state of man-made, natural and social hazards of administrative-territorial units of Ukraine based on monitoring data]. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl* [Collection of Scientific Works of Kharkiv Air Force University]. 2016, no. 3 (48), pp. 142–145. (in Ukrainian).

3. *Zvit pro otsinku mozhlyvykh naslidkiv dlia dovkillia vid realizatsii Stratehii rozvytku Dolynskoho subrehionu na period do 2027 roku* [Report on the assessment of possible consequences for the environment from the implementation of the Strategy for the Development of the Dolyna Subregion for the period until 2027]. Kyiv, 2017. URL: http://pleddg.org.ua/wp-content/uploads/2020/12/Skrining_Dol.pdf (date of application : 19.04.2024). (in Ukrainian).

4. *Informatsiino-analitychna dovidka pro nadzvychaini sytuatsii v Ukraini u 2023 rotsi* [Informational and analytical report on emergency situations in Ukraine in 2023]. URL: https://dsns.gov.ua/upload/2/0/2/2/3/1/4/2023-rik.pdf (date of application : 19.04.2024). (in Ukrainian).

5. *Holovnyi tsentr spetsialnoho kontroliu* [The main center of special control]. URL: https://gcsk.gov.ua/ya-

vidchuv-zemletrus/ (date of application : 19.04.2024). (in Ukrainian).

6. *Enerhetyka. Ivano-Frankivska oblasna derzhavna administratsiia : ofitsiinyi veb-sait Ivano-Frankivskoi oblasnoi derzhavnoi administratsii* [Energy. Ivano-Frankivsk Regional State Administration : the official website of the Ivano-Frankivsk Regional State Administration]. URL: http://www.if.gov.ua/modules.php?name=Content&pa=showpage&pid=728 (date of application : 19.04.2024). (in Ukrainian).

7. Lazoryshyn I. *Dolynskyi hazopererobnyi zavod prodovzhuie nadiino pratsiuvaty. 17.08.2020* [The Dolyna gas processing plant continues to operate reliably. 17.08.2020]. *Ahentsiia novyn* [News Agency]. URL: https://firtka.if.ua/blog/view/bogdan-deputat-nezvazhaiuchi-na-covid-19-ta-ekonomichnu-krizu-dolinskii-gazopererobnii-zavod-prodovzhuie-nadiino-pratsiuvati (date of application : 19.04.2024). (in Ukrainian).

8. *Obiekty «Naftohazu» na zakhodi Ukrainy poshkodzheno vnaslidok rankovoi ataky RF* [Naftogaz facilities in the west of Ukraine were damaged as a result of the Russian attack in the morning]. *Interfaks* [Interfax]. URL: https://interfax.com.ua/news/economic/975650.html (date of application : 19.04.2024). (in Ukrainian).

9. *Wikipediia. Udary po obiektakh krytychnoi infrastruktury Ukrainy pid chas rosiisko-ukrainskoi viiny* [Wikipedia. Strikes on critical infrastructure facilities of Ukraine during the Russian-Ukrainian war]. URL: https://uk.wikipedia.org (date of application : 19.04.2024). (in Ukrainian).

10. Ivaniuta S.P. and Kachynskyi A.B. *Ekolohichna ta pryrodno-tekhnohenna bezpeka Ukrainy : rehionalnyi vymir zahroz i ryzykiv : monohrafiia* [Ecological and natural and man-made security of Ukraine : regional dimension of threats and risks : monograph]. Kyiv : NISD Publ., 2012, 308 p. (in Ukrainian).

Надійшла до редакції: 13.09.2024.